UNIVERSIDADE
LUSÓFONA

Diogo de Castro Oliveira

Prova Digital – A Apreensão de Correio Eletrónico e Registos de Comunicações de Natureza Semelhante no Decurso da Pesquisa de Dados Informáticos

Trabalho Realizado sob orientação da
Professora Doutora Inês Fernandes Godinho

fevereiro de 2023

UNIVERSIDADE
LUSÓFONA

Diogo de Castro Oliveira

Prova Digital – A Apreensão de Correio Eletrónico e Registos de Comunicações de Natureza Semelhante no Decurso da Pesquisa de Dados Informáticos

Dissertação de Mestrado

Mestrado em Ciências Jurídico-Criminais

Dissertação defendida em provas públicas na Universidade Lusófona do Porto no dia 13/02/2023, perante o júri seguinte:

Presidente: Profª. Doutora Alexandra Maria dos Santos Esteves Vilela
(Professora Associada da Universidade Lusófona do Porto)

Arguente: Profª. Doutora Ana Raquel Conceição
(Professora Auxiliar da Escola de Direito da Universidade do Minho)

Orientadora: Profª. Doutora Inês Fernandes Godinho
(Professora Associada da Universidade Lusófona do Porto

fevereiro de 2023

AGRADECIMENTOS

Diz-nos as regras de experiência comum que o crescimento pessoal, social, profissional, emocional e académico de cada pessoa humana, acontece ou evolui juntamente com os alicerces das mesmas características que cada ser transparece às pessoas que estão ao seu redor.

Na minha pessoa, com toda a genuinidade caracteristicamente revestida nestas palavras, agradeço profundamente à minha companheira de vida Zita Avelar pelos minutos, horas, dias, meses e anos que teve necessidade de assumir funções que não eram suas para serem assumidas, em prol de auxiliar o meu estudo, a minha evolução académica, acabando por ser prejudicada nas suas lides diárias.

Não posso deixar de referir o meu sincero agradecimento à minha colega de estudo e de sacrifício académico, Sandra Rodrigues, que num laço mútuo de dedicação, juntos percorremos todo este caminho, à procura da evolução académica que por sua vez resulta numa evolução profissional.

Por último, com um toque especial de gratidão, agradeço à minha orientadora Senhora Professora Inês Fernandes Godinho e ainda à Senhora Professora Alexandra Vilela, por me terem feito evoluir academicamente, abrindo os meus horizontes até a um percurso de excelência, não só como jurista, mas também como ser humano.

Estes últimos seis anos da minha vida com resiliência e dedicação foram passados com alegria na Universidade Lusófona do Porto.

Paz não é a ausência de guerra; é uma virtude, um estado mental, uma disposição para a benevolência, confiança e justiça.

Baruch Spinoza

RESUMO

A prova digital resulta numa subordinação da própria essência da prova geral. As características específicas da prova digital são a instabilidade, efemeridade, fragilidade, dispersão, complexidade bem como a imaterialidade. Estas características não podem ser definidas como únicas, porque o universo digital está em constante evolução, em que irão certamente surgir outras características relevantes. Dos meios de obtenção de prova da Lei do Cibercrime, bem como na Lei dos Metadados, surgem alguns problemas. Da primeira Lei, verificamos alguma falta de esclarecimento por parte do legislador, sendo esses conflitos dirimidos pela jurisprudência e pela doutrina, não resultando sempre num entendimento firme. A Lei dos Metadados foi recentemente alvo de uma fiscalização por parte do Tribunal Constitucional, em que o art. 4.º conjugado com o art. 6.º, foi considerado inconstitucional no que diz respeito ao prazo de conservação dos dados informáticos de um ano. Também o art. 9.º foi considerado inconstitucional por os visados não serem notificados que os seus dados foram utilizados pelo sistema de justiça. A pesquisa de dados informáticos é um meio de obtenção de prova fundamental nos crimes que envolva algum sistema informático. A par das escutas telefónicas, também podem ser adquiridos conhecimentos fortuitos na pesquisa de dados informáticos. No seguimento da pesquisa, se for necessário a apreender correio eletrónico e registos de comunicações de natureza semelhante, essa apreensão deverá ser ordenada ou autorizada por um juiz, como fiscalizador das liberdades, direitos e garantias, tenha ou não sido lido pelo seu destinatário.

Palavras-chave: Prova Digital; Metadados; Pesquisa de Dados Informáticos; Apreensão de Correio Eletrónico; Conhecimentos Fortuitos.

ABSTRACT

The digital proof results in a subordination of the very essence of the general proof. The specific characteristics of digital proof are instability, ephemerality, fragility, dispersion, complexity as well as immateriality. These characteristics cannot be defined as unique, because the digital universe is constantly evolving, in which other relevant characteristics will certainly emerge. From the means of obtaining evidence from the Cybercrime Law, as well as from the Metadata Law, some problems arise. Regarding the first Law, we found some lack of clarification on the part of the legislator, and these conflicts were settled by jurisprudence and doctrine, not always leading to a firm understanding. The Metadata Law was recently subject to a constitutional review, in which article 4 in conjunction with article 6, was considered unconstitutional with regard to the one-year retention period for computer data. Also article 9.º was considered unconstitutional because the targets were not notified that their data were used by the justice system. Researching computer data is a means of obtaining fundamental evidence in crimes involving a computer system. In addition to wiretapping, fortuitous knowledge can also be acquired in the search for computer data. Following the search, if it is necessary to seize e-mails or communications of a similar nature, this seizure must be ordered or authorized by a judge, as a supervisor of freedoms, rights and guarantees, whether or not it has been read by the receiver.

Keywords: Digital Evidence; Metadata; Computer Data Research; Seizure of Electronic Mail; Fortuitous Knowledge.

Índice

AGRADECIMENTOS iv

RESUMO v

ABSTRACT vi

SIGLAS E ABREVIATURAS ix

1- Enquadramento 1

2- Prova Digital 1

2.1- Breves Referências sobre a Teoria Geral da Prova 3

2.1.1- Distinção entre Meios de Prova e Meios de Obtenção de Prova 5

2.2- Prova Eletrónica-Digital 6

2.2.1- Características da Prova Digital 9

3- Meios de Obtenção de (prova) Dados Informáticos 12

3.1- Preservação Expedita de Dados – Art. 12.º da Lei do Cibercrime 13

3.1.1- A Semelhança Processual entre Preservação e a Conservação de Dados 16

3.1.2- Breve análise ao Acórdão n.º 268/2022 do Tribunal Constitucional 17

3.1.2.1- Previsível Resposta Legislativa ao Acórdão do TC 20

3.1.3- Acórdão do TJUE Relativamente à Conservação Generalizada e Indiferenciada de Dados 22

3.2 Pesquisa de Dados Informáticos 24

3.2.1 Busca Informática ou Pesquisa de Dados Informáticos? 25

3.2.2. Grau de Subsidiariedade 31

3.2.3- Autorização da Pesquisa 32

3.2.4- Consentimento por Quem Tiver a Disponibilidade ou Controlo dos Dados Informáticos 35

3.2.5- Direitos Fundamentais Restringidos 38

3.2.6- Apreensão de dados informáticos 40

3.2.7- Conhecimentos Fortuitos e a Pesquisa de Dados Informáticos 42

4- Apreensão de Correio Eletrónico e de Registos de Comunicação de Natureza Semelhante 48

4.1- Acórdão do Tribunal Constitucional n.º 687/2021 48

4.2- Apreensão de Correspondência 50

4.3- Correio Eletrónico e Registos de Comunicações de Natureza Semelhante 51

4.3.1- Apreensão do Correio Eletrónico Lido e não Lido 52

4.3.2- Conhecimento do Conteúdo 55

4.4- Procedimentos a Adotar Após a Pesquisa 57

5- Conclusões 58

Bibliografia 62

Jurisprudência 66

SIGLAS E ABREVIATURAS

Ac.	Acórdão
Al.	Alínea
Art.	Artigo
CP	Código Penal
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
MP	Ministério Público
P.	Página
SS	Seguintes
TC	Tribunal Constitucional
TJUE	Tribunal de Justiça da União Europeia
TRL	Tribunal da Relação de Lisboa
TRP	Tribunal da Relação do Porto

1- Enquadramento

O mundo digital surgiu em tempos pós-guerra, numa procura de melhorar a qualidade de vida dos usufruidores, e, principalmente, por muito que nos custe a admitir, para facilitar os fenómenos terroríficos que a guerra conduz, numa clara evolução bélica[1]. Algum tempo depois, quando o mundo digital ganhou um considerável reconhecimento, foi utilizado para a evolução, nomeadamente nas situações de desenvolvimento industrial, social, económico, saúde, bem como tantos outros.

Parece-nos unânime que, nos tempos atuais, a falha dos sistemas informáticos que dão *vida* ao mundo digital, poderá resultar em danos imensuráveis, perigosos, e no limite, poderá até resultar em extinção da vida humana tal e qual como a definimos atualmente.

Por isso, é necessário reforçar a proteção desse mundo digital ou virtual, adotando medidas preventivas de salvaguarda dos sistemas informáticos, como também medidas repressivas que auxiliem o combate ao delito já preenchido, e ainda criar mecanismos de ressurgimento dos elementos digitais considerados essenciais para a própria natureza humana.

Assim, o princípio fundamental explicitamente exposto no art. 1.º da Constituição da República Portuguesa, o princípio da dignidade da pessoa humana, juntamente com a construção da sociedade livre, justa e solidária, devendo ser garantido aos cidadãos de cada estado, o acesso ao mundo virtual.

2- Prova Digital

Dada a proximidade evidente entre a prova digital e o cibercrime, consideramos apropriado estabelecer, numa primeira fase, a ligação teórica entre a prova digital e a teoria geral da prova, começando pela sua definição, avançando para os meios de obtenção de prova mais relevantes para o presente estudo previstos na Lei n.º 109/2009, de 15 de setembro, doravante designada por Lei do Cibercrime, procurando adotar uma perspetiva crítica à sua tese problemática, bem como as soluções que aí poderiam ter sido consagradas.

[1] ABREU, Karen Cristina Kraemer, História e Usos da Internet, p. 1 e 2. Disponível em: http://bocc.ufp.pt/pag/abreu-karen-historia-e-usos-da-internet.pdf. Acesso em: 10-02-2023.

A Lei do Cibercrime veio transpor para a ordem jurídica interna a decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativo a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa[2].

A Lei do Cibercrime teve os fins de compilar num único diploma legislativo, todas as normas que envolvam a criminalidade informática, abrangendo o direito substantivo, processual penal e ainda de cooperação judiciária internacional. Assim, revogou a anterior Lei da Criminalidade Informática, Lei n.º 109/91, de 17 de agosto[3].

A Lei n.º 79/2021, de 24 de novembro, veio a introduzir novas mudanças na Lei do Cibercrime, bem como em outras leis conexas, transpondo a Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, sendo que as alterações mais significativas dizem respeito à Lei do Cibercrime, ao Código Penal, doravante designado por CP, e ainda ao Código de Processo Penal[4], doravante designado por CPP, substituindo a Decisão-Quadro 2001/413/JAI[5].

Num ponto de vista ainda introdutório, devemos ter atenção que embora a Lei seja denominada por Lei do Cibercrime, a sua aplicação é geral em todo o sistema processual penal, isto é, não representa uma exclusividade de aplicação nos crimes informáticos, e como tal, as disposições processuais previstas na Lei do Cibercrime deveriam ter sido enquadradas sistematicamente num local de reconhecimento dessa posição, nomeadamente num capítulo do próprio CPP[6].

Na verdade, esta nova lei procurou resolver os problemas existentes na ordem jurídica, atualizando-se em comparação com o quotidiano das novas tecnologias, acompanhando assim a diretiva suprarreferida.

---

[2] Preâmbulo Lei n.º 109/2009, de 15 de setembro.
[3] FIDALGO, Sónia, A Recolha de Prova em Suporte Eletrónico – Em Particular, A Apreensão de Correio Eletrónico *in* Julgar, n.º 38, 2019a, p. 152.
[4] Preâmbulo Lei n.º 79/2021, de 24 de novembro.
[5] Esta decisão procurava combater a fraude e a contrafação de meios de pagamento que não em numerário, tendo a particularidade de definir certos tipos de comportamento considerados fraudulentos, que devem ser considerados como infrações penalmente relevantes puníveis nos países da EU.
[6] CORREIA, João Conde (2016, abril, 08). Prova Digital: Enquadramento legal *in* Prova em Direito Penal, Cibercriminalidade e Prova Digital. Centro de Estudos Judiciários, Lisboa. https://educast.fccn.pt/vod/clips/13vwtviahd/streaming.html?locale=pt

O legislador, optou apenas para aditar novos tipos legais de crime, e aprimorar o direito substantivo, o que não se condena, mas ignorou implicitamente a necessidade de esclarecer as dúvidas processuais que a Lei do Cibercrime traz consigo.

Esta última alteração foi uma excelente oportunidade (perdida) de aproveitar uma reforma legislativa para uniformizar esta matéria, em que deviam ter sido resolvidos os problemas da Lei do Cibercrime, o que, até o momento de elaboração desta dissertação nada ficou resolvido. Ademais, foram necessários doze (12) anos para proceder a uma alteração da Lei do Cibercrime. Esta lei merecia um melhor aproveitamento e dedicação, até porque o percurso jurídico da natureza humana já é essencialmente digital, e chegará muito brevemente a um momento de quase exclusividade digital.

Podemos referir que, é certo que a evolução do sistema jurídico não pode (nem consegue) caminhar à frente da evolução da sociedade e de tudo o que a representa. No entanto, será naturalmente pertinente atingir num momento retrospetivo, a lógica de alcançar a evolução da sociedade, sendo a única forma de minimizar os danos que daí podem advir. É então, o evoluir do próprio sistema jurídico.

Neste sentido, já nos ensina Figueiredo Dias[7], que o Direito Processual Penal para garantir soluções aos seus problemas básicos, depende substancialmente da própria evolução e desenvolvimento cultural e social, sendo os fins a administração da justiça penal, apoiando-se na extensa evolução da escolha dos meios adequados para atingir esses fins.

2.1- Breves Referências sobre a Teoria Geral da Prova

O Direito Processual pretende atingir um resultado adequado para aplicar o Direito, através da descoberta da verdade material[8]. Antes de alcançar este resultado, podemos associar a existência de duas fases distintas que se complementam na decisão final. A primeira fase diz respeito à verificação dos factos que condicionam a aplicação do Direito, já a segunda é a aplicação do Direito propriamente dito. Em conjunto, a prova existente nessas duas fases, servirá um propósito de capacitar a existência ou não dos factos que levem ao preenchimento da previsão abstrata[9]. Neste sentido, nele devem fazer

[7] DIAS, Jorge de Figueiredo, Direito Processual Penal, Clássicos Jurídicos, Coimbra Editora, Impressão 2004, p. 60.
[8] GONÇALVES, Fernando, A Prova do Crime, Meios Legais Para a Sua Obtenção, Almedina, 2009, p. 15.
[9] SILVA, Germano Marques, Processo Penal, Vol. II, Verbo, 2008, p. 109 e 110.

parte, ou pelo menos devem ser verificados, os factos considerados provados para alcançarmos uma certa consequência jurídica[10]. A definição de prova não é unívoca. Manuel Guedes Valente[11], assume que o instituto jurídico do Direito, a qual faz parte a prova, representa uma *conceção de natureza jurídica poliédrica*. Isto é, assume uma vertente multifacetada, em que cada uma das faces representa um conceito próprio. A face essencial representa a descoberta da verdade, que, para todos os efeitos, não é uma verdade real nem absoluta. Desta forma, a verdade não exibe uma convicção cientificamente comprovada, baseando-se apenas numa lógica de probabilidade[12], dada o facto inato que o Direito é uma ciência inexata[13].

Como refere o art. 341.º do Código Civil, *as provas têm por função a demonstração da realidade dos factos,* sendo essa a sua finalidade principal[14]. No entanto, não é exclusiva. Ainda no lado interno representado pela prova, outra face com uma importância significativa é a realização da justiça, que intrinsecamente se encontra conectado à defesa e garantia dos direitos de todos os cidadãos, sejam eles os agentes do crime, as vítimas diretas ou indiretas, bem como o restabelecimento da paz jurídica e social[15]. Esta garantia elimina o juízo que se poderá utilizar meios ilícitos para demonstrar a realidade dos factos, obrigando ainda a que as valorações dessas provas sejam devidamente fundamentadas e fiscalizadas[16].

A prova caracteriza-se em dois sentidos que, numa lógica de complementaridade, representam a prova na sua plenitude. O primeiro sentido diz respeito à prova em sentido objetivo, fazendo nele parte todos os meios de prova fornecidos ao tribunal que servem para retratar a realidade dos factos. Já o segundo sentido é a prova em sentido subjetivo, que representa o peso de cada elemento de prova na formação da convicção do julgador, tendo em conta o seu espírito, verificando a existência (ou não) de factos relevantes adequados para produzir uma decisão final[17].

---

[10] A consequência jurídica representa, como o próprio nome indica, uma consequência à violação da norma. A norma jurídica para ser considerada como *completa,* necessita de uma previsão abstrata e uma estatuição, sendo que a primeira tipifica uma conduta considerada ilegal, e a segunda atribuí uma certa consequência jurídica à adoção dessa conduta. Cfr MACHADO, João Baptista, Introdução ao Direito e ao Discurso Legitimador, Almedina, 2002, p. 79 e 80.
[11] VALENTE, Manuel Monteiro Guedes, Cadeia de Custódia da Prova, Almedina, 2021, p. 20.
[12] GONÇALVES (2009), p. 14.
[13] ALMEIDA, Ivo de, A Prova Digital, Librum Editora, 2018, p. 17.
[14] SILVA (2008), p.110.
[15] VALENTE (2021), p. 20.
[16] SILVA (2008), p.110 e 111.
[17] ALMEIDA (2018), p. 17.

Numa perspetiva de valoração, a prova em processo penal assenta em duas ideias fundamentais. A prova deve ser valorada tendo em conta as *regras da crítica*, ou do critério humano, devendo ser valoradas por um juiz, não podendo ser baseado no seu convencimento psicológico. Assim, o dever de fundamentação da valoração ou não da prova é exigido, conforme já referimos. No entanto, a vertente psicológica é extremamente relevante, até porque na própria essência de certos meios de prova, nomeadamente a prova testemunhal, o juiz deve aplicar alguns conceitos de valoração, o que aliados à experiência, poderá resultar numa convicção de existência ou não do facto que se pretende provar[18].

2.1.1- Distinção entre Meios de Prova e Meios de Obtenção de Prova

Conforme retratamos no capítulo anterior, o objeto da prova não assume uma ética de reconstrução plena dos factos que irão direcionar a aplicação da consequência jurídica. Para nos auxiliar na constituição desse objeto, o art. 124.º do CPP dispõe que *constituem objeto da prova todos os factos juridicamente relevantes para a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou da medida de segurança aplicáveis.*

Ainda no CPP, denota-se uma clara distinção entre os meios de obtenção da prova e os meios de prova, em que o primeiro servirá uma lógica de recolha do segundo, tendo em vista formar uma convicção das autoridades judiciárias. Esta diferenciação está consagrada numa dupla perspetiva, a perspetiva lógica e a técnico-operativa. A lógica dos meios de prova representa uma perspetiva individual de fundamento processual, por si só apto a provar certos e determinados factos, convencendo o julgador. Já os meios de obtenção da prova, servirão um simples propósito de recolha desses meios de prova. Na vertente técnico-operativa, os meios de obtenção da prova normalmente serão utilizados na fase preliminar no processo, nomeadamente na fase de inquérito, e, dessa forma, acarreta uma responsabilidade relevante no âmbito de uma investigação criminal e da recolha dos meios de prova[19].

[18] CABRAL, José António Henriques dos Santos, Código de Processo Penal – Comentado, Comentário ao art. 124.º, 4.º Edição, Almedina, 2022, p. 361.
[19] ANTUNES, Maria João, Direito Processual Penal, Almedina, 2016, p. 110 e 111.

2.2- Prova Eletrónica-Digital

A prova digital está associada a uma lógica de modernização da sociedade, em que numa perspetiva de evolução e de avanço tecnológico, necessariamente permitiu também a incorporação deste tipo de prova, cada vez mais significativa no que concerne à busca da realização dos fins primordiais previstos no direito processual penal, nomeadamente, a descoberta da verdade material que se correlaciona autonomamente com a realização da justiça, igualmente a proteção perante o estado dos direitos fundamentais dos cidadãos e ainda o restabelecimento da paz jurídica[20].

Para definir ou estabelecer a diferença entre prova digital e a prova dita como comum, não há qualquer norma que resolva esse conceito. Neste sentido, torna-se necessário o recurso à jurisprudência e à doutrina para definir o conceito de prova digital. Tal como a prova dita como comum, a sua função essencial será idêntica, ou seja, terá a função de ser suscetível para valoração pelo julgador que aprecie a veracidade ou não dos factos em causa[21], resultando assim que a prova digital poderá ser entendida uma subordinação da prova geral. Assim, a diferença primordial entre ambas, é que a comum insere-se num ambiente real ou físico, já a digital será recolhida numa lógica de *ambiente digital*[22].

Duarte Rodrigues Nunes[23] define a prova digital *como a informação relevante para fins probatórios produzida/obtida a partir de dados em formato digital (na forma binária, em que todas as quantidades se representam pelos números 0 ou 1) armazenados, processados ou transmitidos em/através de/entre sistemas informáticos ou armazenados em suportes informáticos, muitas vezes com utilização de redes de comunicações eletrónicas.*

Já Benjamim Silva Rodrigues[24] procurou definir prova digital como *qualquer fluxo informacional ou comunicacional digital, que, estaticamente, se encontre*

[20] ANTUNES (2016), p. 14 e 15.
[21] ALMEIDA (2018), p. 35.
[22] GONÇALVES, João Gama, A Prova Digital em 2017 – Reflexões Sobre Algumas Insuficiências Processuais e Dificuldades da Investigação, CEDIS Working Papers, outubro 2017, p. 7. Este autor procura distinguir essas provas, assumindo que só assim se tornará compreensível estabelecer as diferenças, existindo assim uma fronteira compreensível no *ambiente digital* ou imaterial (prova digital), *e* o contexto físico ou material (prova comum).
[23] NUNES, Duarte Rodrigues, Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime, Gestlegal, 2021, p. 47
[24] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo IV – Da Prova – Electrónico- Digital e da Criminalidade Informático- Digital, Rei dos Livros, 2011, p. 30.

armazenado, tratado ou processado ou, pelo contrário, dinamicamente, seja transmitido, veiculado ou não por meio das redes informáticas ou de serviços e comunicações eletrónicas, quer ao nível de um ciclo informacional e comunicacional fechado ou aberto, privado ou público.

Embora assumindo que a procura de uma definição como as anteriormente descritas abrangem uma panóplia de situações digitais, concordamos com David Ramalho[25] quando estabelece que a formulação deste conceito oscila entre duas situações, nomeadamente *a inoperatividade em virtude da sua excessiva abstração* bem como *a curta duração por força da rápida evolução tecnológica.* Por isso, a procura de uma definição que não vá contra estas duas posições, afigura-se dedálea, devendo assim reconhecer que a formulação alvo de estudo deverá atingir um patamar de flexibilidade duradoura.

Desde logo, este último autor, reconhece que existem algumas incongruências da procura da definição deste conceito. Isto porque verificámos a existência de uma certa ideia de *sinonímia,* nos conceitos de prova eletrónica e prova digital. Algo que a par de David Ramalho não concordamos.

Note-se que a doutrina muitas vezes nem reconhece a existência de prova eletrónica, abordando o assunto meramente como prova digital. Outros autores já procuram estabelecer uma certa ligação entre prova eletrónica e prova digital[26]. Também a nosso ver, o que nos parece mais lógico é, numa ideia de definição ainda mais específica, a prova eletrónica abrange uma perspetiva geral, enquanto a prova digital abrange algo mais característico, estando esta última inserida nessa primeira. David Ramalho[27], citando George R. S. Weir e Stephen Mason, procura definir a prova eletrónica como um meio de prova que engloba tanto a prova analógica como a prova digital. Isto torna-se significativamente mais importante, porque os procedimentos a adotar nestes dois tipos de prova revelam-se distintos. Assim, os autores em estudo procuram definir prova eletrónica como *dados (compreendendo o resultado de dispositivos analógicos ou dados em formato digital) que são manipulados, armazenados ou comunicados através de qualquer dispositivo, computador ou sistema informático feito pelo Homem, ou transmitidos através de um sistema de comunicação, que tem o potencial de tornar a*

[25] RAMALHO, David Silva, Métodos Ocultos de Investigação Criminal em Ambiente Digital, Almedina, 2017, p. 98 e 99.
[26] Principalmente, RODRIGUES (2011), no título da obra, bem como na p. 30 e ss.
[27] RAMALHO (2017), p. 99 e 100.

explicação factual de qualquer parte mais provável ou menos provável do que seria sem a prova[28].

Partindo desta última definição, aqui enquadrar-se-á qualquer elemento de prova digital, bem como a prova em formato analógico, que se traduz em rolos fotográficos que poderão conter fotografias bem como gravações em fita de vídeo e áudio[29], que embora possam ser digitalizadas, não são oriundas do mundo digital[30].

Em jeito de conclusão, existem certas e determinadas provas que à primeira vista não correspondem a provas digitais. Falamos, naturalmente, dos vestígios biológicos suscetíveis de identificar o(s) agente(s) do crime, que após a sua recolha são inseridos numa base de dados[31], em que, a título de exemplo o ADN[32] é, também, composto por informação em formato digital, podendo ser visto que a sua inserção equivale a uma digitalização de vestígios orgânicos[33], tornando-se assim provas digitais cumprindo as finalidades da sua existência.

Posto isto e tendo em conta que iremos abordar esta parte nos capítulos seguintes, a prova digital não pode ser entendida como um assunto de exclusiva aplicação no ciberespaço[34] – embora neste tipo de criminalidade é certamente o tipo de prova considerada fundamental para a descoberta da verdade material –, sendo certo que este tipo de provas representa uma realidade aplicável em todo o processo penal, nos mais variados tipos legais de crime ou bens jurídicos ofendidos, desde que cumpram os princípios e a legislação que determinam a necessidade de recolha tipo de prova.

---

[28] RAMALHO (2017), p. 99 e 100, citando os autores. Este autor também justifica a sua posição citando o parágrafo 141 do Relatório Explicativo da Convenção sobre o Cibercrime, onde refere que a prova eletrónica abrange *a informação contida em formato digital ou outro formato eletrónico [suscetível de] poder ser utilizada como prova,* explicando assim o âmbito de aplicação do art. 14.º n.º 2 alínea a) da Convenção sobre o Cibercrime.

[29] Partindo do pressuposto das definições de prova digital aqui referidas, não nos parece que haja compatibilidade na inserção destes meios de prova nessas definições, a não ser naquela que David Ramalho nos trouxe.

[30] *Ibidem*

[31] Sobre este assunto em particular, teremos de nos socorrer da Lei n.º 5/2008. de 11 de fevereiro.

[32] Ácido Desoxirribonucleico.

[33] RAMALHO (2017), p.101.

[34] Espaço não físico, virtual, que surge para estabelecer ligações entre vários dispositivos digitais conectados.

2.2.1- Características da Prova Digital

A prova digital acarreta algumas características que se distinguem da prova dita como comum. No entanto, podemos inserir este meio de prova, tendo em consideração ideia sistémica do CPP, no capítulo reservado à prova pericial[35]/[36], até porque para se proceder à sua recolha é necessária a intervenção de um perito/especialista apto para recolher esse tipo de prova. Não obstante, após a sua recolha através da perícia, o conteúdo terá que ser analisado e redigido a escrito, tornando-se documentação.

Estas diferenças revelam uma incompatibilidade natural, podendo assim assumir que a prova digital assume uma meritória autonomia[37] *fragmentária, (…) frágil, volátil, alterável, apagável e manipulável, invisível e espacialmente dispersa*[38].

Já Benjamim Silva Rodrigues[39], assume que as principais características da prova eletrónica-digital são necessariamente importantes para configurar um modelo de investigação criminal forense digital adequado para atingir as finalidades do processo penal.

A primeira característica que este último autor refere é a efemeridade. A prova digital assume um carácter temporário, que consequentemente indica um género de não durabilidade deste meio de prova. O mesmo é dizer que este tipo de prova, dada a sua natureza correspondente a todas as suas características, obriga, tanto no meio legal de obtenção de prova como no sucesso da sua obtenção, que os investigadores forenses digitais atuem com uma certa celeridade e com alguns cuidados acrescidos à prova dita como comum. Se estes dois preceitos não forem cumpridos, poderá resultar numa perda da obtenção da própria prova[40].

Outra característica imanente na prova digital é a sua fragilidade e uma certa simplicidade de ser suscetível a alterações. Com isto, entende-se que este tipo de prova, se não for levado com o cuidado considerado necessário, adequado e proporcional, poderá

---

[35] RAMOS, Armando Dias, O Agente Encoberto Digital - Meios Especiais e Técnicos de Investigação Criminal, Almedina, 2022, p. 119.
[36] Esta ideia poderá ser temerária. Nos termos do art. 163.º, n.º 1 do CPP, a prova pericial assume a presunção da subtração da livre apreciação do julgador (art. 127.º do CPP). Não obstante, essa presunção pode ser dirimida se a convicção do julgador se introduzir no campo da divergência, devendo utilizar a regra ou o dever de fundamentação (art. 163.º, n.º 2 do CPP).
[37] RAMALHO (2017), p. 104.
[38] RAMOS (2022), p. 119.
[39] RODRIGUES (2011), p.41 e 42.
[40] RODRIGUES (2011), p. 42.

prejudicar a sua recolha, resultando numa alteração das suas propriedades que a tornam ineficiente ou mesmo pelo seu desaparecimento. É também necessário acautelar essas duas possibilidades quando o sistema operativo, de forma automática[41], assim o determina – normalmente, como podemos estar a lidar com um cibercriminoso, essa possibilidade poderá ser originada pelo próprio agente do crime, tendo em vista prejudicar a recolha de provas que fundamentem a sua condenação. Nesta última possibilidade, em bom rigor, a prova digital até pode ser alterada por um terceiro que acede ao sistema em causa, via remoto, podendo a alterar ou até mesmo a eliminar. Esta particularidade resultará numa lógica de procurar obter uma especial dedicação por parte do investigador para tentar abordar, logo após o início da intervenção, o vestígio da prova que será eficiente para trazer para objeto do processo[42].

A próxima característica, que se encontra intimamente ligada à anterior, é a volatilidade ou instabilidade dessa prova eletrónica-digital. A sua natureza digital pressupõe a possibilidade de ser instável e mutável, dificultando a sua recolha. Imagine-se que numa lógica de *post-mortem analysis*[43], o investigador forense digital quando aborda o local onde se situa o computador, após verificar que o mesmo se encontra ligado, não deverá simplesmente *desligar a ficha*, apreendê-lo e entregá-lo ao laboratório[44]. Se o fizer, poderão ser perdidas certas ligações a sistemas remotos (por exemplo: máquinas virtuais, às vezes até com um sistema operativo diferente do primário) ou até mesmo poderão ter sido instalados certos programas de autodestruição de dados. Nesta situação em concreto, será adequado proceder a uma *live analysis*[45], onde será pertinente verificar todos os programas que estão em funcionamento no sistema informático bem como outros procedimentos julgados adequados pelos investigadores forenses digitais[46]. Esta

[41] RAMALHO (2017), p. 116.
[42] *Ibidem*
[43] Análise das provas digitais em laboratório especializado, diferente do local de recolha.
[44] No entanto, em algumas situações poderá ser a decisão mais acertada. Isto porque, há certas redes de criminosos que se verificarem que está a ser efetuada uma *live analysis*, poderão, virtualmente, apagar todos os ficheiros contidos no disco rígido. Nessa lógica, será o mais acertado proceder ao *desligar da ficha* do computador para mais tarde clonar o disco rígido e efetuar uma *post-mortem analysis*. Para tomar esta decisão, será pertinente avaliar o tipo de rede criminosa que está a ser investigada, devendo ser adotada a decisão que o investigador digital considerar mais eficiente para garantir a prova.
[45] Análise das provas digitais no próprio local de recolha da busca ou então efetuada de modo remoto.
[46] RAMOS (2022), p. 120.

característica é uma das mais relevantes, principalmente no que toca à própria cadeia de custódia da prova[47].

No entanto, existe pelo menos uma determinada prova digital em que esta particularidade não é preenchida, perdendo assim esta característica. Falamos, naturalmente, dos *dados de tráfego*[48], em que se torna observável a existência de uma certa pegada digital, marcada após essa comunicação, em que se verifica a autonomização da criação de dados relacionados com a comunicação, criados pelo sistema de telecomunicação[49].

Outra dificuldade que se revela importante para inserir nestas características, é a aparente imaterialidade, ou até mesmo, a invisibilidade deste meio de prova[50]. A imaterialidade representa a própria lógica de existência da prova, no meio que não se revela físico ou material. A prova está inserida num formato digital, não acessível pelos meios tradicionais físicos, sendo que até poderá atingir um formato invisível através da instalação de manobras de equívoco, sendo pertinente a existência de um perito com conhecimentos técnicos sobre este tipo de prova.

Também a complexidade ou codificação deste tipo de prova são um problema[51]. O utilizador, numa tentativa de se salvaguardar, poderá aplicar uma codificação de segurança[52], através de acesso a um ficheiro ou vários apenas através da introdução de uma palavra-passe, perguntas de segurança, dupla confirmação através da utilização de outro aparelho eletrónico (normalmente são utilizados os telemóveis), ou até, mais recentemente, qualquer técnica de encriptação biométrica, seja por impressão digital, reconhecimento facial, reconhecimento de íris, reconhecimento de voz, reconhecimento de retina bem como o reconhecimento pela digitação, sendo que esta última acaba por se revelar pouco fiável. Esta codificação poderá resultar numa inutilidade, não podendo ser

[47] RAMALHO (2017), p. 106. Também RAMOS (2022), p. 119.
[48] A Lei 109/2009, de 15 de setembro, concretamente no art. 2.º alínea c) define dados de tráfego como *os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente;*
[49] ANDRADE, Manuel da Costa, Bruscamente no Verão Passado, a Reforma do Código de Processo Penal – Observações Críticas Sobre Uma Lei que Podia e Devia Ter Sido Diferente, Coimbra, Coimbra Editora, 2009, p. 156.
[50] RODRIGUES (2011), p. 43.
[51] *Ibidem*
[52] Embora existam técnicas de desencriptação para todos os meios de codificação, nem sempre se obtém sucesso na utilização.

utilizada como prova em sede de audiência de discussão e julgamento, visto que poderá não ser possível efetuar uma leitura a uma prova cifrada[53].

Outra característica que se revela complexa, num ponto de vista estratega de que a investigação poderá se apoiar, é a própria dispersão deste tipo de prova em específico. Claramente podemos associar que a diferença entre este tipo de prova e a prova física, é a sua dificuldade na própria localização, dado que a prova eletrónico-digital acarretará, frequentemente, um carácter não concentrado, dispersos por todo o tipo de elementos que se enquadrem na complexidade informática-digital[54]. Em algumas situações, normalmente quando o agente do crime possuí alguma inexperiência, a prova poderá estar concentrada numa só pasta de arquivos digital ou até mesmo num só instrumento como uma *pen* ou *cd*. No entanto, diz-nos a experiência de investigação, que de uma forma frequente, denota-se o evoluir destes agentes do crime, sendo que a tendência será para chegar ao preenchimento, na sua plenitude, da verificação desta característica em concreto.

Por último, muito embora respeitando a própria definição de prova digital que prezamos, concretamente no que concerne à própria evolução natural deste tipo de prova, não podemos concluir a inexistência de mais algum tipo de característica, e isto, por si só, define uma característica denominada por mutabilidade e, cumulativamente, a dinâmica. Vejamos, Benjamin Rodrigues assume que esta característica é relevante, considerando que este tipo de prova se traduz em pulsos eletromagnéticos que, momentaneamente, assumem, dinamicamente, um certo tipo de *dado papel no sistema ou rede informáticos*[55].

3- Meios de Obtenção de (prova) Dados Informáticos

Como até aqui já se chegou a demonstrar, a prova digital representa um género de epítome do próprio cibercrime, devendo ser vista como essencial, mas não exclusiva, para fundamentar uma condenação.

Para este efeito, a Lei do Cibercrime, bem como o próprio CPP, trazem-nos algumas ferramentas consideradas adequadas para produzir prova através dos meios de

[53] RAMOS (2022), p. 122.
[54] RODRIGUES (2011), p. 43.
[55] RODRIGUES (2011), p. 44.

obtenção de prova ditos como tradicionais[56], previstos amplamente no CPP, bem como os meios de obtenção de prova logicamente adequados para produzir a prova no ambiente do cibercrime.

Na verdade, a Lei do Cibercrime apresenta um novo regime sobre a obtenção de prova em suporte eletrónico, mas o seu âmbito de aplicação servirá para qualquer tipo legal de crime, nos termos do art. 11.º. Assim, como refere Sónia Fidalgo, *não se compreende, por isso, por que razão estas regras não foram inseridas no Código de Processo Penal*[57].

Os meios de obtenção de prova da Lei do Cibercrime estão previstos no art. 12.º ao art. 19.º, no entanto, do 12.º ao 17.º é que se verificam a possibilidade de acesso a dados informáticos[58], que a própria lei define no art. 2.º alínea b) como *qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função*.

3.1- Preservação Expedita de Dados – Art. 12.º da Lei do Cibercrime

O art. 12.º, logo no seu n.º 1 dispõe que s*e no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa.* Este meio de obtenção de prova poderá ainda ser requerido por órgão de polícia criminal, também designado por OPC, quando existe autorização da autoridade judiciária competente, ou ainda, quando existe urgência e perigo na demora, sendo que de seguida deverá dar notícia à autoridade judiciária, respeitando o procedimento elencado no art. 253.º do CPP[59], conforme se pode verificar no art. 12.º, n.º 2.

[56] Meios de obtenção de prova tradicionais num sentido meramente costumário.
[57] FIDALGO (2019a), p. 152.
[58] VENÂNCIO, Pedro Dias, Lei do Cibercrime Anotada e Comentada, Coimbra Editora, 2011, p. 99.
[59] O n.º 1 dispõe que *os órgãos de polícia criminal que procederem a diligências referidas nos artigos anteriores elaboram um relatório onde mencionam, de forma resumida, as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas.*

Embora se possa assumir a problemática nas diferenças entre dados de base[60], dados de tráfego[61] e dados de localização[62], inseridos no universo dos dados informáticos, aqui importa que o órgão de polícia criminal não deverá ter acesso a esses dados, limitando-se apenas a dar a ordem de preservação a quem detenha disponibilidade desses dados, visto que que dependerá da validação ou não, da autoridade judiciária competente[63].

Em concreto, esses dados informáticos poderão ser documentos eletrónicos (Decreto-Lei n.º 12/2021, de 09 de fevereiro), programas de computador (softwares), dados pessoais (cumprindo o determinado na Lei n.º 59/2019, de 08 de agosto), dados de tráfego bem como dados de localização (previstos na Lei n.º 41/2004, de 18 de agosto)[64].

Esses dados preservados poderão estar na esfera *material* do destinatário a quem tenha sido dada a ordem de preservação dos dados, como em qualquer outro local, desde que esteja sob o controlo do destinatário[65].

Ainda que o pressuposto basilar deste meio de obtenção de prova seja que a recolha desta prova seja necessária para a sua produção, a definição de *se no decurso do processo for necessário à produção da prova*, previsto no n.º 1, cinge-se apenas ao processo penal, excluindo-se assim o processo disciplinar, desportivo ou

---

Já o n.º 2 especifica o destinatário desse relatório, referindo que o mesmo *é remetido ao Ministério Público ou ao juiz de instrução, conforme os casos.*

[60] MILHEIRO, Tiago Caiado, *in* Comentário Judiciário do Código de Processo Penal, Comentário ao artigo 189.º, Almedina, 2021, p. 840, define dados de base como *conforme resulta da sua literalidade trata-se de dados recolhidos e que servem de base aos procedimentos necessários para realização de comunicações. Reportam-se a uma fase anterior a qualquer comunicação (independente desta) e são obtidos para que a mesma se concretize.* Dados como identidade do utilizador, contatos, correio eletrónico, moradas, bem como o próprio IP (*internet protocol)* associado ao visado.

[61] MILHEIRO (2021), p. 836, assumindo a existência de dúvidas interpretativas dadas as várias definições de *dados de tráfego* previstas em distintas leis, o autor define após uma análise conjunta de tais definições, que *dados de tráfego consistem em dados relacionados com a realização de concretas comunicações/conversações (o que pressupõe a realização das mesmas) por meio de um sistema informático, através de uma rede de comunicações eletrónicas ou no âmbito de um serviço de telecomunicações ou dados tratados para efeitos da comunicação ou faturação. Não incidem sobre o conteúdo, mas abrangem um conjunto de dados de onde é possível extrair informações de vária índole conexionadas com o tráfego.*

[62] MILHEIRO (2021), p. 838, define que *dados de localização* são *todos aqueles que fornecem informação sobre elementos que visam descortinar a posição geográfica de uma determinada pessoa (ou de um objeto) num determinado momento temporal.*

[63] RAMOS, Armando Dias, Do *Periculum In Mora* da Atuação da Autoridade Judiciária ao *Fumus Boni Iuris* da Intervenção Policial *in* IV Congresso de Processo Penal, I Congresso Luso-Brasileiro de Criminalidade Económico-Financeira, coordenado por Manuel Monteiro Guedes Valente, Almedina, 2016, p. 58.

[64] VENÂNCIO (2011), p. 99.

[65] NUNES (2021), p. 77.

contraordenacional, algo que o legislador deveria assumir um maior cuidado na tipificação desta norma, evitando assim erros de interpretação por parte do intérprete, visto que a ingerência de comunicações de natureza particular é algo que está exclusivamente reservada ao processo crime[66].

Para o efeito de valoração de prova, segundo o art. 12.º, n.º 3, a ordem de preservação deverá ser composta por vários requisitos cumulativos, o que a falha de um só, poderá determinar a insusceptibilidade de uso desse meio de prova. A ordem de preservação deve referir a natureza dos dados, a origem e destino dos dados, sempre que forem conhecidos e ainda o período temporal pelo qual deverão ser preservados, não podendo ultrapassar o prazo máximo de 3 meses. No entanto, referente ao seu prazo máximo, Benjamin Rodrigues afirma que na sua perspetiva, o prazo poderá ser renovado até ao prazo máximo de um ano, conforme estipula o art. 12.º n.º 5, mas, essa renovação deverá cumprir os requisitos de admissibilidade que vigoram no art. 12.º, seguindo um modelo análogo àquele existente nas escutas telefónicas[67].

O incumprimento desta ordem de preservação será o crime de desobediência. Não obstante não estar tipificado diretamente a consequência do não cumprimento, como por exemplo sucede no meio de obtenção de prova da injunção para apresentação ou concessão do acesso a dados, previsto no art. 14.º, n.º 1 da Lei do Cibercrime.

Neste sentido, considerando a falta de tipicidade concreta desta consequência, Duarte Nunes, embora aceite que o não cumprimento acarretará o crime de desobediência, acredita que só serão preenchidos os elementos do tipo após a sua cominação, enquadrando-se assim no art. 348.º n.º 1 alínea b) do CP[68].

Já Armando Ramos, aborda o mesmo assunto, assumindo a mesma consequência, mas parece que não considera necessária a existência da cominação, ou pelo menos não se alongou nessa ideia, apenas remetendo que o simples não cumprimento da ordem de preservação irá resultar na consequência jurídica prevista no art. 348.º do CP, não especificando qualquer alínea[69].

Este procedimento, quando tal se afigure necessário, conforme foi anteriormente explanado, ainda que não o seja, poderá ser enquadrado numa medida cautelar de

[66] RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo II – Bruscamente … A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal, Rei dos Livros, 2010, p. 442.
[67] RODRIGUES (2010), p. 443.
[68] NUNES (2021), p. 77.
[69] RAMOS (2016), p. 58.

polícia[70], tendo em vista o cumprimento da ideia de justiça assegurada por esse tipo de medida cautelar.

3.1.1- A Semelhança Processual entre Preservação e a Conservação de Dados

Quando abordámos este meio de obtenção de prova – preservação expedita de dados informáticos –, surge inevitavelmente a ideia da semelhança entre este regime e aquele que vigora na Lei n.º 32/2008 de 17 de julho, vulgarmente conhecida como *Lei dos Metadados*[71], no entanto, estes não se devem confundir. Vejamos, a preservação expedita acarretará, inevitavelmente, a existência de um inquérito, e a sua existência servirá o propósito de alcançar o(s) agente(s) do crime, quando tal se afigure necessário, conforme já foi explanado.

Já o regime que vigora na Lei n.º 32/2008 de 17 de julho, representará uma ideia semelhante da ótica da preservação, mas a sua finalidade será a de conservação de dados, o que na prática resulta em situações distintas. Isto significa que, quaisquer dados inseridos nas categorias previstas no art. 4.º da suprarreferida lei[72], deverão ser conservados no prazo previsto no art. 6.º, ou seja, 1 (um) ano. No entanto, no âmbito deste regime, não se afigura necessário a existência de um inquérito aberto, sendo que a conservação desses dados pelas entidades competentes abrange todos os utilizadores desses dados informáticos, não existindo o carecimento de um inquérito correr contra determinada pessoa[73].

A transmissão desses dados só deverá ocorrer quando existir ordem ou autorização nesse sentido, existindo uma semelhança com os pressupostos que legitimam a interceção de dados em tempo real, nomeadamente através de um despacho fundamentado por um

---

[70] *Ibidem*

[71] Recentemente, o Tribunal Constitucional foi chamado para se pronunciar a constitucionalidade ou inconstitucionalidade de algumas normas previstas nessa lei, a qual iremos abordar no subcapítulo seguinte.

[72] *1 - Os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar as seguintes categorias de dados: a) Dados necessários para encontrar e identificar a fonte de uma comunicação; b) Dados necessários para encontrar e identificar o destino de uma comunicação; c) Dados necessários para identificar a data, a hora e a duração de uma comunicação; d) Dados necessários para identificar o tipo de comunicação; e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento; f) Dados necessários para identificar a localização do equipamento de comunicação móvel.*

[73] NUNES (2021), p. 78 e 80.

juiz, bem como na fase em que pode ser ordenada a transmissão, ou seja, na fase de inquérito, muito embora esta última situação não esteja tipificada nos requisitos de transmissão de dados supracitados, previstos no art. 9.º da Lei dos Metadados[74].

Além disso, a transmissão de dados está inserida apenas num catálogo restritivo de crimes graves[75], e essa diligência terá que ser indispensável para a descoberta da verdade, o que corresponderá a muito difícil de obter prova de outra forma, ou até mesmo uma impossibilidade – aqui também se denota uma semelhança entre a produção da prova ser necessária, no que diz respeito à preservação expedita de dados da lei do cibercrime (12.º Lei do Cibercrime) e o meio de prova ser indispensável (9.º n.º 1 e n.º 2 Lei dos Metadados), previsto no diploma em estudo –, devendo respeitar os princípios da adequação, necessidade e proporcionalidade, art. 9.º n.º 4[76]. Também só podem ser transmitidos os dados relativos a suspeitos ou arguidos (alínea a), pessoa que recebe ou transmite através de alguma forma de comunicação eletrónica mensagens direcionadas ou provenientes do suspeito ou arguido (alínea b), se existir consentimento presumido ou efetivo da vítima (alínea c), nos termos do art. 9.º n.º 3[77].

Este regime, de certa forma, encontra-se duplicado naquele que vigora no art. 189.º do CPP, algo criticado por João Conde Correia, especificando que o legislador podia e deveria ter mantido a centralidade normativa no CPP[78].

3.1.2- Breve análise ao Acórdão n.º 268/2022 do Tribunal Constitucional[79]

O acórdão do Tribunal Constitucional n.º 268/2022, que foi recebido com alguma celeuma, diz respeito à pronúncia de uma eventual inconstitucionalidade nas normas constantes dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de julho. Foi requerido pela

[74] MILHEIRO (2021), p. 851.
[75] MILHEIRO (2021), p. 852. A definição de crimes graves está prevista claramente no art. 2.º, n.º 1, alínea g) como *crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou de títulos equiparados a moeda, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima.*
[76] CORREIA, João Conde, Prova Digital: as leis que temos e a lei que devíamos ter, *in* Revista do Ministério Público 139, julho:setembro, 2014, p. 33.
[77] *Ibidem*
[78] CORREIA (2014), p. 33 e 34.
[79] Acórdão que declara inconstitucional algumas normas na Lei n.º 32/2008, de 17 de julho.

Provedora de Justiça, nos termos do art. 281.º, n.º 2, alínea d) da CRP, por violarem o princípio da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada e familiar, previsto no art. 26.º, n.º 1 da CRP, ao sigilo das comunicações, previsto no art. 34.º, n.º 1 da CRP e ainda uma tutela jurisdicional efetiva, previsto no art. 20.º do n.º 1 da CRP.

Esse pedido, de uma forma breve, numa primeira fase apresenta como fundamentos que a Lei n.º 32/2008, de 17 de julho, transpôs a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006.

No entanto, esta diretiva deriva da diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas. A derivação resulta do cumprimento da restrição dos direitos e obrigações previstos na diretiva, incumbindo aos Estados-Membros a possibilidade de adotar medidas legislativas para esse efeito.

O Tribunal de Justiça da União Europeia, doravante designado TJUE, declarou a invalidade da diretiva 2006/24/CE, num acórdão datado a 8 de abril de 2014, processo *Digital Rights Ireland Ltd e outros, C-293/12 e C-594/12.*

Este último tribunal, fundamenta a invalidade por entender que viola o princípio da proporcionalidade, assumindo que a diretiva restringe os direitos de respeito pela vida privada e familiar e à proteção de dados pessoais, previsto nos artigos 7.º[80], 8.º[81] da Carta dos Direitos Fundamentais da União Europeia, direito que deverá ser transposto para a ordem jurídica nacional, nos termos do art. 51.º, n.º 1 referida Carta. Assim, a Lei n.º 32/2008, de 17 de julho, está diretamente vinculada pela Carta.

Essa violação está associada a dois elementos autónomos, nomeadamente, só o facto de operadores de telecomunicações serem obrigados a conservar os dados, resulta numa ofensa grave aos direitos individuais, mesmo que posteriormente não sejam utilizados pelas entidades públicas. O segundo elemento, o Tribunal justifica que após a primeira agressão, ocorre um acréscimo na violação, quando as entidades públicas têm acesso ou utilizam os dados que por si só já existem e estão a ser armazenados, ou seja,

[80] O art. 7.º dispõe que *todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.*

[81] Já o art. 8.º dispõe no n.º 1 que *todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.* No n.º 2 que *esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.* Por último, no n.º 3 que *o cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.*

acarretará o uso ou acesso a dados que a sua própria natureza ou existência já violam os direitos individuais dos seus detentores.

Referente à eventual inconstitucionalidade do art. 4.º conjugado com o art. 6.º da Lei n.º 32/2008, de 17 de julho, o Tribunal Constitucional concluiu que, tendo em consideração a interpretação dos direitos à reserva da intimidade da vida privada e ainda à autodeterminação informativa, a conservação de todos os dados de todas as pessoas representam uma agressão excessivamente grave, levando à conclusão que se enquadra numa solução legislativa desequilibrada. Fundamentou que a abrangência de todas as pessoas e não apenas aquelas a qual exista suspeita de atividade criminosa, irá molestar os direitos fundamentais suprarreferidos, que, num *juízo de ponderação, não são contrapesadas pelos efeitos positivos no combate à criminalidade*.

No entanto, também admite que não se verifica este desequilíbrio quando são conservados apenas os dados de base e não os dados de tráfego ou de localização, por resultar numa agressão com uma intensidade inferior comparativamente com as últimas duas[82], estando assim em consonância com o direito da União Europeia, desde que estes sejam conservados em território da UE.

Assim, por considerar que a conservação dos dados de tráfego e de localização ultrapassam os limites da proporcionalidade, *viola-se o n.º 2 do artigo 18.º da Constituição na restrição aos direitos fundamentais à reserva da intimidade da vida privada e à autodeterminação informativa (artigos 26.º, n.º 1, e 35.º, n.º 1, da Constituição), perdendo relevância a questão de saber se os demais elementos de que dependeria a proporcionalidade da medida (o ajustamento do prazo de conservação ao estritamente necessário para os fins a alcançar; e a imposição de condições de segurança do respetivo armazenamento) são preenchidos pela regulamentação fiscalizada.*

A nosso ver de forma correta, o Tribunal Constitucional concluiu que, *razão pela qual deve ter-se por inconstitucional, por violação dos n.ºs 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o artigo n.º 18.º, n.º 2, da Constituição, a medida de conservação por um ano dos dados de tráfego e dos dados de localização, decorrente da conjugação do disposto do artigo 4.º com o artigo 6.º da Lei n.º 32/2008, de 17 de julho.*

No âmbito da sua pronúncia, referente à possível inconstitucionalidade do art. 9.º da Lei n.º 32/2008, de 17 de julho, o Tribunal Constitucional, após o requerimento da

[82] As definições de dados de base, tráfego e de localização já foram abordadas nas notas de rodapé 60, 61 e 62, respetivamente.

Provedora de Justiça, em consonância plena com o Acórdão do Tribunal de Justiça da União Europeia *Tele2*, de 21 de dezembro de 2016, concluiu que após a utilização ou acesso pelas autoridades nacionais dos dados conservados, os titulares dos direitos em causa devem ser informados a partir do momento em que essa informação não seja suscetível de comprometer a eficácia da investigação criminal. Isto resultará, a hipótese de recorrer aos tribunais quando os seus direitos forem violados, cumprindo assim o disposto previsto no art. 15.º, n.º 2 da Diretiva 2002/58/CE.

Ainda que no ordenamento jurídico nacional exista a possibilidade de dar a conhecer ao titular dos direitos que os seus dados foram transmitidos às autoridades de investigação criminal, tal só acontecerá após o requerimento do titular, o que em termos práticos, só irá ocorrer quando o titular detiver a convicção que essa transmissão ocorreu. Os mecanismos judiciais estão previstos no art. 18.º, n.º 2 e n.º 3 da Lei n.º 59/2019, de 8 de agosto, quando existam recusas por parte das entidades competentes na transmissão desses dados.

Assim, a nosso ver corretamente, o Tribunal Constitucional conclui que a*o não se prever tal notificação restringe-se de modo desproporcionado o direito à autodeterminação informativa, consagrado no artigo 35.º, n.º 1, da Constituição (na dimensão de controlo do acesso de terceiros a dados pessoais) afetando, igualmente, o direito a uma tutela jurisdicional efetiva (artigo 20.º, n.º 1, da Constituição), por prejudicar a viabilidade prática de exercício de controlo judicial de acessos abusivos ou ilícitos aos dados conservados*. Declarando dessa forma a inconstitucionalidade, com força obrigatória geral da norma do art. 9.º da Lei n.º 32/2008, de 17 de julho.

3.1.2.1- Previsível Resposta Legislativa ao Acórdão do TC

Foram vários os projetos lei que procuraram resolver o problema constitucional existente nos artigos 4.º (em conjugação com o art. 6.º) e 9.º da Lei n.º 32/2008, de 17 de julho.

O governo, pelo menos numa primeira fase, colocou de parte uma eventual alteração da Lei n.º 32/2008. Os seus esforços passaram por aproveitar a base de dados que servem o propósito de faturação para os serviços de comunicações eletrónicas,

prevista na Lei n.º 41/2004, de 18 de agosto, aditando a possibilidade desses dados[83] serem usados para fins de investigação criminal, em certos crimes.

Além disso, também procuraram resolver o problema da notificação dos cidadãos, quando os seus dados são utilizados ou acedidos e não represente uma possibilidade de prejudicar a investigação em causa, bem como a obrigação de respeitar uma portaria que transmita os trâmites que permita a transmissão de dados às autoridades, e ainda procurar expressar as condições que determinam a destruição dos dados conservados e transmitidos às autoridades.

A Proposta de Lei n.º 11/XV/1.ª[84], pretendia a alteração do art. 6.º da Lei n.º 41/2004, de 18 de agosto, em que a nova redação permitia a transmissão dos dados de tráfego às autoridades judiciárias, quando esses dados sejam indispensáveis para a descoberta da verdade, ou ainda seja impossível ou muito difícil de obter prova de uma forma distinta. Neste sentido, considerando que o prazo de conservação das operadoras dos dados para faturação são seis (6) meses, nos termos do art. 10, n.º 1 da Lei n.º 23/96, de 26 de julho, as autoridades poderiam ter acesso a esses dados nesse prazo.

No entanto, a alteração da redação do art. 6.º da Lei n.º 41/2004, de 18 de agosto, não referia a necessidade de existência de um despacho fundamentado por um juiz para que esses dados fossem transmitidos, algo que representaria uma afronta aos direitos fundamentais dos cidadãos, indo mesmo contra o próprio art. 9.º n.º 1 da Lei n.º 32/2008, em que era necessário um despacho fundamentado por um juiz de instrução para que os dados fossem transmitidos. Além disso, se essa alteração prosseguisse, iria revogar esta última lei.

Até ao momento de elaboração desta dissertação, também foram submetidos vários Projetos de Lei, cuja síntese prevê alterações ao prazo de conservação dos dados previsto na Lei n.º 32/2008, de 1 ano para 6 meses, 12 semanas e ainda 90 dias, em três Projetos de Lei distintos, sendo unânime que a conservação dos dados deverá ser em território da União Europeia.

---

[83] Recorde-se que os dados em causa, são os dados de tráfego e de localização, até porque o próprio Tribunal Constitucional não considerou que a conservação dos dados de base representa algum desequilíbrio Constitucional.

[84] Acessível através do Link:
https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=121504

3.1.3- Acórdão do TJUE Relativamente à Conservação Generalizada e Indiferenciada de Dados[85]

Mais recentemente, concretamente em setembro de 2022, o TJUE pronunciou-se sobre a conservação generalizada e indiferenciada dos dados de tráfego, bem como dos dados de localização.

Esta decisão é consequência de um pedido de fiscalização proveniente do Supremo Tribunal Administrativo Federal Alemão, tendo em vista confirmar se o direito da União se opõe à legislação nacional desse país, alegando algumas diferenças legislativas comparativamente aos países à qual o TJUE já se havia pronunciado[86].

Neste sentido, o TJUE pronunciou-se que o direito da União se opõe às legislações nacionais dos seus membros que, numa vertente preventiva, permitam a conservação generalizada e indiferenciada dos dados de tráfego bem como dos dados de localização, quando tenham o efeito de prevenir ameaças graves contra a segurança pública e/ou combater a criminalidade grave.

No entanto, este mesmo tribunal, aceita que o direito da União não se opõe que as medidas legislativas dos seus membros:

> *– permitem, para efeitos da salvaguarda da segurança nacional, impor aos prestadores de serviços de comunicações eletrónicas que procedam a uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, em situações em que o Estado-Membro em causa enfrenta uma ameaça grave para a segurança nacional que se revela real e atual ou previsível, desde que a decisão que prevê tal imposição possa ser objeto de fiscalização efetiva quer por um órgão jurisdicional quer por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos, destinada a verificar a existência de uma dessas situações e o respeito pelos requisitos e pelas garantias que devem estar previstos, e a referida imposição apenas possa ser aplicada por um período temporalmente limitado ao*

[85] Acórdão do Tribunal de Justiça da União Europeia, processos C-793/19 e C-794/19, de 20.09.2022.

[86] Até ao momento de elaboração desta dissertação, foram referidos estes acórdãos: 5 de abril de 2022, *Commissioner of An Garda Síochána*, e 6 de outubro de 2020, *Quadrature du Net* e o., C-511/18, C-512/18 e C-520/18.

estritamente necessário, mas renovável em caso de persistência dessa ameaça;

– preveem, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação seletiva dos dados de tráfego e dos dados de localização que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas renovável;

– preveem, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;

– preveem, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública, uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos; e

– permitem, para efeitos da luta contra a criminalidade grave e, a fortiori, da salvaguarda da segurança nacional, impor aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, que procedam, por um determinado período, à conservação rápida dos dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem.

O TJUE conclui que estas exceções devem ser adotadas com regulamentos específicos e evidentes, comprometendo-se que a conservação dos dados deverá respeitar as regras referidas nos regulamentos, bem como que as pessoas intervenientes devem de dispor de garantias eficazes contras os problemas adjacentes aos riscos de abuso.

Com este Acórdão, a legislação nacional já poderá, e deverá, auxiliar-se nestas considerações, tendo em vista compatibilizar o nosso direito com o direito da União.

3.2 Pesquisa de Dados Informáticos

Um dos basilares meios de obtenção de prova previstos na Lei do Cibercrime, é o estipulado no art. 15.º, que diz respeito à pesquisa de dados informáticos.

Este meio de obtenção de prova, será essencial nos crimes tipicamente informáticos, em que o objeto da ação da prática do crime é um computador ou qualquer outro equipamento que dependa de tecnologia para o seu funcionamento. Também será pertinente nos crimes essencialmente informáticos, em que fazem parte os crimes que o bem jurídico ofendido é um equipamento informático, desde que faça parte na proteção instituída pela Constituição que dignifique a suficiência da tutela de penal. Por último, os crimes acidentalmente informáticos, em que a sua síntese é a utilização de qualquer equipamento informático que seja utilizado para a prática do crime em causa[87].

O regime da pesquisa de dados informáticos encontra-se prevista no art. 15.º da Lei do Cibercrime[88], mas também poderá ser encontrado no art. 19.º da Convenção do

[87] ALMEIDA (2018), p. 38.

[88] O art. 15.º da Lei do Cibercrime dispõe que: *1 - Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.*
2 - O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade.
3 - O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando:
a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;
b) Nos 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.
4 - Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior:
a) No caso previsto na alínea b), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação;
b) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal.
5 - Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2.
6 - À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista.

Cibercrime[89], em que na epígrafe do artigo não está tipificado expressamente *pesquisa de dados informáticos*, mas sim¸ *busca e apreensão de dados informáticos armazenados*.

Neste sentido, parece-nos que o art. 189.º do CPP foi revogado tacitamente pelo art. 15.º da Lei do Cibercrime, com exceção do art. 189.º, n.º 2 do CPP, o que, em boa verdade, poderia também estar inserido no art. 15.º da Lei do Cibercrime[90].

3.2.1 Busca Informática ou Pesquisa de Dados Informáticos?

Neste sentido, já se compreende o motivo de alguns autores considerarem que este meio de obtenção de prova também se encontre intitulado como *busca informática*[91], como nos ensina Sónia Fidalgo, até porque a sua própria natureza constitui uma verdadeira busca, em que o próprio artigo 174.º n.º 1 do CPP representa um elo de

[89] O art. 19.º da Convenção do Cibercrime dispõe que: *1 — Cada Parte deverá adotar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a efetuar buscas ou de outro modo aceder:*
a) A um sistema informático, ou a parte do mesmo, bem como aos dados informáticos nele armazenados; e b) A um suporte informático de dados que permita armazenar dados informáticos; no seu território.
2 — Cada Parte deverá adotar as medidas legislativas e outras que se revelem necessárias para assegurar que, sempre que as suas autoridades efetuem 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.
3 — Cada Parte deverá adotar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a apreender ou de outro modo reter os dados informáticos aos quais se teve acesso nos termos do n.º 1 ou 2 do presente artigo. Essas medidas incluem o poder de:
a) Apreender ou de outro modo reter um sistema informático ou parte do mesmo, ou um suporte informático de dados;
b) Efetuar e reter uma cópia desses dados informáticos;
c) Preservar a integridade dos dados informáticos pertinentes armazenados;
d) Tornar esses dados informáticos inacessíveis ou retirá-los do sistema informático acedido.
4 — Cada Parte deverá adotar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes a impor a qualquer pessoa que conheça o funcionamento do sistema informático ou as medidas aplicadas para proteger os dados informáticos nele contidos, que forneça de forma ponderada todas as informações necessárias para permitir a aplicação das medidas previstas no n.º 1 e 2 do presente artigo.
5 — Os artigos 14.º e 15.º regulamentam os poderes e procedimentos referidos no presente artigo.
[90] CORREIA (2014), p. 36. Mais tarde o autor afirmou que excecionalmente o art. 189.º, n.º 2 do CPP não é revogado tacitamente pelo art. 15.º da Lei do Cibercrime, mas que poderia e deveria ser revogado expressamente neste último artigo, concretamente em CORREIA (2016).
[91] FIDALGO (2019a), p. 153.

proximidade, pelo menos no que diz respeito aos seus requisitos, tendo em vista o cumprimento do n.º 6 do art. 15.º[92]. Também Paulo Dá Mesquita, assume que a pesquisa de dados informáticos conserva *a verdadeira natureza processual de busca*[93], justificando a sua posição com os mesmos fundamentos anteriormente elencados.

As buscas, sejam elas domiciliárias ou não, assumem um carácter mais amplo do que a pesquisa de dados informáticos, visto que esta última só servirá como prova se o objetivo for obter dados informáticos específicos ou determinados armazenados num certo sistema informático, enquanto as buscas, embora o motivo que originou este meio de obtenção prova possa ser determinado ou específico, no seu cumprimento será apreendido todo e qualquer conteúdo relevante[94], existindo assim uma restrição significativa entre as pesquisas de dados informáticos e as buscas[95].

Benjamin Rodrigues[96], alerta para o cumprimento das regras de execução das buscas, presentes nos artigos 174.º a 177.º do CPP, e também art. 11.º do Estatuto do Jornalista, principalmente do n.º 6 ao n.º 8[97], nos termos do n.º 6 do art. 15.º da Lei do Cibercrime.

No entanto, Armando Dias Ramos[98], alerta para que, apesar do legislador remeter no próprio art. 15.º n.º 6 da Lei do Cibercrime para os requisitos das buscas previstos no

---

[92] NUNES (2021), p.154 e 155.
[93] MESQUITA, Paulo Dá, Processo Penal, Prova e Sistema Judiciário, Coimbra Editora, 2010, p. 114.
[94] Nos Termos do n.º 1 e n.º 2 do art. 174.º do CPP, o objetivo das buscas é encontrar *animais, coisas ou objetos relacionados com o crime ou que possam servir de prova* em *local reservado ou não livremente acessível ao público*. Estes objetos podem ser aqueles utilizados para preencher um ilícito criminal ou estão relacionados com esse preenchimento, bem como aqueles suscetíveis de servir enquanto meio de prova dos factos.
[95] PEREIRA, Rui Costa, A Pesquisa de Dados Informáticos – Exigências práticas do Princípio da Proporcionalidade, *in* Revista Portuguesa de Ciência Criminal, ano 31, n.º 3, Gestlegal, setembro – dezembro, 2021, p. 572.
[96] RODRIGUES (2010), p. 450.
[97] *6 - A busca em órgãos de comunicação social só pode ser ordenada ou autorizada pelo juiz, o qual preside pessoalmente à diligência, avisando previamente o presidente da organização sindical dos jornalistas com maior representatividade para que o mesmo, ou um seu delegado, possa estar presente, sob reserva de confidencialidade.*
7 - O material utilizado pelos jornalistas no exercício da sua profissão só pode ser apreendido no decurso das buscas em órgãos de comunicação social previstas no número anterior ou efectuadas nas mesmas condições noutros lugares mediante mandado de juiz, nos casos em que seja legalmente admissível a quebra do sigilo profissional.
8 - O material obtido em qualquer das acções previstas nos números anteriores que permita a identificação de uma fonte de informação é selado e remetido ao tribunal competente para ordenar a quebra do sigilo, que apenas pode autorizar a sua utilização como prova quando a quebra tenha efectivamente sido ordenada.
[98] RAMOS (2016), p. 59.

CPP, com as adaptações julgadas adequadas, a pesquisa de dados informáticos não deve ser confundida com uma busca. Este autor, acredita que esta remissão, diz respeito apenas para os procedimentos que devem ser adotados após a realização da pesquisa de dados informáticos, concretamente, o facto que deve ser realizado o respetivo auto, com a devida assinatura de todos os intervenientes.

Ainda assim, certo é, pelo menos da nossa modesta opinião, que se verifica um paralelismo entre as buscas e a pesquisa de dados informáticos[99]. Isto é, da mesma forma que as buscas do CPP permitem o acesso a locais físicos inacessíveis, a pesquisa de dados informáticos permite a entrada em sistemas digitais. Assim, mesmo que não exista consentimento, poderá ser legítimo o arrombamento de algo para aceder a esse local físico – nas buscas tradicionais –, na pesquisa de dados informáticos – como verdadeira busca que é – também poderá ser necessário o recurso a um género de *arrombamento digital*, utilizando dispositivos ou softwares bem como todas as técnicas consideradas necessárias para aceder aos dados em causa[100].

Mais na ótica do paralelismo, é que o acesso físico ao conteúdo do dispositivo abrange dados informáticos, nomeadamente, telemóveis, computadores, ou seja, qualquer sistema informático que esteja inserido no art. 2.º, alínea a) da Lei do Cibercrime. No entanto, as pesquisas poderão ser autorizadas pelo Ministério Público, doravante designado MP, de acordo com o art. 15.º, n.º 1, existindo algumas situações que poderão ser realizadas pelo próprio órgão de polícia criminal, mas as buscas domiciliárias apenas poderão ser autorizadas por um juiz, existindo também algumas exceções para quando o OPC poderá efetuar uma busca domiciliária quando não exista autorização do juiz[101].

Relativamente ao ambiente digital, nos termos do art. 15.º, n.º 3 da Lei do Cibercrime, existe compatibilidade legislativa entre a possibilidade do órgão de polícia criminal efetuar uma pesquisa de dados informáticos sem autorização da autoridade judiciária, concretamente quando *a mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;* e ainda *nos 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.* Já a busca domiciliária pressupõe a possibilidade de ser efetuada sem autorização de um juiz nos

[99] MILHEIRO (2021), p. 859.
[100] *Ibidem*
[101] MILHEIRO (2021), p. 860.

casos em que exista *consentimento do visado, documentado por qualquer forma;* e ainda quando exista *flagrante delito pela prática de crime punível com pena de prisão superior, no seu máximo, a 3 anos*[102].

Nesta senda, existe ainda um enquadramento processual entre as buscas domiciliárias e a pesquisa de dados informáticos, em que será legítimo que um órgão de polícia criminal efetue uma busca domiciliária sem autorização de um juiz nos termos do art. 177.º n.º 1 do CPP. Falamos, naturalmente, da situação em que o visado é detido em flagrante delito por crime a que seja aplicável uma pena de prisão superior, no seu máximo, a 3 anos, nos termos do art. 177.º, n.º 2, alínea c) e n.º 3 alínea b) do CPP.

Não nos parece lógico este tratamento diferenciado que o legislador impôs entre o ambiente digital e o ambiente físico. Vejamos, numa situação prática, dada à própria natureza iminente das características da prova digital, poderá se afigurar necessário, numa ótica de cumprimento do requisito basilar da pesquisa de dados informáticos, proceder-se à pesquisa quando exista flagrante delito pela prática de algum crime a que seja aplicável uma pena de prisão.

Ainda que o art. 15.º, n.º 6 da Lei do Cibercrime determine a aplicação das regras de execução das buscas previstas no CPP, a situação acima apresentada não pode ser transposta para o regime da pesquisa de dados informáticos, dado que as regras de admissibilidade estão expostas no art. 15.º, demonstrando uma clara intenção em não estabelecer este regime mais abrangente na pesquisa de dados informáticos. Referente à parte das regras de execução estabelecidas no CPP, certos autores consideram que esse número só tem relevância para efeitos do art. 176.º do CPP[103].

Como é bom de se ver, pelo menos nesta vertente, verificamos que existe uma maior proteção entre o próprio ambiente digital em comparação com o mundo físico, muito embora ambos sejam merecedores da tutela de proteção constitucional. Num exemplo prático, imaginemos que no decorrer de uma investigação por abuso sexual de crianças, concretamente nas situações expostas no art. 171.º, n.º 3 do CP, em que a pena máxima aplicável é até três anos de prisão, mediante uma ação encoberta digital em que o agente do crime já está a ser investigado por crimes da mesma natureza, em tempo real, os órgãos de polícia criminal verificam um abuso sexual de uma criança, nos moldes do art. 171.º, n.º 3 do CP. Enquanto isso decorre, outros órgãos de polícia criminal da mesma

[102] Estas buscas domiciliárias poderão ser efetuadas entre as 21H e as 7H, nos termos do art. 177.º, n.º 3, alínea b) do CPP.
[103] PEREIRA (2021), p. 579.

equipa de investigação da ação encoberta digital, procedem a uma vigilância física ao agente do crime. Assim, afigurando-se a existência de todos os pressupostos para uma detenção em flagrante delito, os órgãos de polícia criminal em vigilância física devem efetuar a detenção do agente do crime.

Assim, como o crime em causa prevê uma pena máxima aplicável até três anos de prisão, pode ser efetuada uma busca domiciliária ou não domiciliária (art. 177.º, n.º 2, alínea c) e art. 174.º, n.º 5, alínea c), ambos do CPP), existindo assim legitimidade para proceder à apreensão dos equipamentos informáticos. Se não for necessário ou possível efetuar uma busca, também pode ser aplicada a medida cautelar de polícia de apreensão dos instrumentos informáticos, nos termos do art. 249.º do CPP, se existir urgência ou perigo na demora.

Nisto, considerando as próprias características que este meio de prova acarreta, poderá ser pertinente, o quanto antes, tendo em vista assegurar, verdadeiramente, a prova fundamental para condenar ou absolver o arguido, proceder naquele momento à pesquisa de dados informáticos, nos moldes do art. 15.º da Lei do Cibercrime, principalmente na perspetiva que podem existir várias outras provas além daquela que foi recolhida em flagrante delito, podendo existir provas de ligação com outras vítimas.

Em termos práticos, o material é apreendido e posteriormente pode ser ordenada ou autorizada pela autoridade judiciária competente a pesquisa de dados informáticos (art. 15.º Lei do Cibercrime). Neste tipo de prova, como essa ordem ou autorização poderá tardar, antes de ser efetuada a pesquisa de dados informáticos, arrisca-se a perda definitiva de matéria provatória essencial num processo desta natureza. Isto devido às características inerentes à prova digital, concretamente, a fragilidade, a simplicidade de ser suscetível a alterações e a volatilidade ou instabilidade. Neste sentido, existe ainda a possibilidade de terceiros acederem remotamente ao material apreendido e procederem à sua remoção ou alteração[104].

Ainda que elenquemos nesta dissertação este problema, que para nós não deixa de o ser, o órgão de polícia criminal no âmbito da apreensão proveniente – neste caso em concreto ou semelhante – de uma medida cautelar de polícia, deve *adotar as medidas cautelares necessárias à conservação da integridade dos animais e à conservação ou manutenção das coisas e dos objetos apreendidos*, nos termos da parte final do art. 249.º, n.º 2, alínea c) do CPP. Até que ponto, é que poderá ser possível conservar os meios de

[104] RAMALHO (2017), p. 116.

prova que poderiam ser recolhidos numa pesquisa de dados informáticos, ou ainda, se for efetuada uma conservação ou manutenção da prova recolhida numa clara semelhança à pesquisa de dados informáticos, será que essa prova será validada nas instâncias competentes? Não podemos auferir um grau de certeza, visto que o legislador não tipificou de uma forma expressa ou clara essa possibilidade. Principalmente no que diz respeito à apreensão do correio eletrónico ou comunicações de natureza semelhante.

As providências cautelares quanto aos meios de prova representam uma lógica de conservação dos meios de prova existentes na infração penal que pode ter sido denunciada ou presenciada, mesmo antes de terem sido recebidas instruções por parte do MP. A sua existência prende-se pela *necessidade* e *urgência* de intervenção. Também podem ser definidas como diligências imprescindíveis e inadiáveis para o inquérito[105]. O problema aqui atinente, é que a própria essência da prova digital, como não é clara num ponto de vista legislativo, poderão ser vistas numa perspetiva de abuso. Isto é, imagine-se que no âmbito da situação aqui em estudo, provavelmente, em sede própria, poderia ser determinado que a própria apreensão do respetivo sistema informático (seja telemóvel, computador…), poderia ser suficiente para a conservação do meio de prova. No entanto, como aqui tentamos explanar, por vezes isso não será suficiente, até porque a lógica de conservação exposta no art. 249.º, n.º 2, alínea c) do CPP, não nos parece atualizada para os tempos atuais, principalmente no que concerne à prova digital[106].

Por último, mas não menos importante, embora o despacho emitido pela autoridade judiciária competente não possa ser confundido com um mandado de busca também emitido pela autoridade judiciária competente, não faz sentido que este último meio de obtenção de prova não abarque o primeiro. Isto é, se o mandado de busca for

---

[105] COSTA, Eduardo Maia, Código de Processo Penal – Comentado, Comentário ao art. 249.º, 4.º Edição, Almedina, 2022, p. 896.

[106] Neste sentido, num percurso diferente, mas atingiu uma meta final semelhante, *já não basta unicamente interceptar uma comunicação, o seu conteúdo pode estar encriptado. Já não basta apreender um computador, o seu conteúdo pode ter sido encriptado ou eliminado automaticamente. Já não basta ativar o GPS de um smartphone para determinar a sua localização, as coordenadas podem ser fictícias. Destarte, os Estados necessitam de ponderar sobre a eficácia dos meios de obtenção de prova à disposição em seu ordenamento jurídico e de idealizarem novas formas de obtenção de prova capazes de ultrapassar os desafios erigidos pelas evoluções decorrentes da sociedade mundializada da informação, de modo a cumprir o seu dever de zelo pela segurança dos seus cidadãos, e, ao mesmo tempo, o dever de zelo pelos direitos e garantias fundamentais dos indivíduos investigados*. RIBOLI, Eduardo Bolsoni, A Utilização de Novas Tecnologias no Âmbito da Investigação Criminal e as Suas Limitações Legais: A Interceptação de Comunicações em Massa e os Softwares de Espionagem, *in* Galileu – Revista de Direito e Economia, Volume XIX, jul-dez, 2018, p. 51 e 52.

emitido pela autoridade judiciária competente, e se no local buscado se encontra algum equipamento ou sistema informático este poderá ser sujeito a uma pesquisa, bastando que faça sentido no ponto de vista de investigação. Não faz sentido que para um local em específico tenha que existir um mandado de busca e um mandado de pesquisa de dados informáticos emitido pela mesma ou outra autoridade judiciária. Também no âmbito do consentimento da busca, devem servir as mesmas regras, podendo ser apreendidos e sujeitos a pesquisa os equipamentos informáticos no local buscado se forem cumpridos todos os requisitos do consentimento, exceto se o visado não permitir a busca num certo local ou divisão, e por inerência não consente com a pesquisa de dados informáticos[107].

3.2.2. Grau de Subsidiariedade

Relativamente à sua admissão, muito embora este meio de obtenção de prova acarrete uma ofensa aos direitos fundamentais[108], diferentemente de alguns regimes também ofensivos, a pesquisa de dados informáticos não admite a existência de um catálogo de crimes que permita a utilização deste meio de obtenção de prova. Assim, podemos entender desde logo, que este meio de obtenção de prova poderá ser utilizado para qualquer tipo de crime, independentemente dos elementos típicos, entendimento esse subtraído do art. 15.º conjugado com o art. 11.º, n.º 1, alíneas a) a c) da Lei do Cibercrime[109].

A sua admissão passa por um grau de subsidiariedade, em que a pesquisa de dados informáticos só será admissível *quando no decurso do processo se tornar necessário à produção da prova, tendo em vista a descoberta da verdade*, parte integrante inicial do art. 15.º, n.º 1 da Lei do Cibercrime. Algo que representa uma lógica processual compatível com os direitos fundamentais aqui restringidos, direitos atingidos com um grau de intensidade médio/baixo[110].

Nesta senda, em consonância com a opinião de Duarte Nunes[111], quando a pesquisa de dados informáticos incide sobre qualquer tipo de sistema informático que envolva exercícios de uma atividade que envolva o sigilo profissional, ainda que o legislador não tenha expressado um regime de proporcionalidade diferenciado

[107] RAMOS (2016), p. 60.
[108] Veja-se o subcapítulo 3.2.5.
[109] MESQUITA (2010), p. 98.
[110] NUNES (2021), p. 176.
[111] *Ibidem*

relativamente aos sistemas que não envolvam este sigilo, deveremos entender que o grau de necessidade deve ser diferente. Tendo em conta o princípio da subsidiariedade Constitucionalmente existente, o requisito de *se tornar necessário à produção de prova, tendo em vista a descoberta da verdade*, especificamente nos sistemas que envolvam o sigilo profissional, deverá ser entendido que apenas poderá ser utilizado este meio de obtenção de prova apenas deve ser admissível *quando existam razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter*[112].

Esta lógica parte da mesma que representa a própria ideia do sigilo profissional, em que poderão estar envolvidos várias informações que envolvam a própria natureza íntima ou pessoal de vários cidadãos que poderão não ter qualquer ligação com o processo, principalmente no sigilo médico.

3.2.3- Autorização da Pesquisa

O artigo em estudo prevê que para ser possível proceder à pesquisa de dados informáticos, é necessário que a autoridade judiciária competente autorize ou ordene por despacho *que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência*.

Benjamim Silva Rodrigues, alerta que, nos mesmos moldes constitucionais que vigoram no art. 179.º n.º 3 do CPP, no que diz respeito à apreensão de correspondência, por força do art. 32.º n.º 4 da CRP, esta autorização deverá ser judicial e, o juiz que autorizou ou ordenou esta pesquisa, deverá presidir a diligência, numa lógica de garantir a cadeia de custódia da prova. Se tal formalidade não for cumprida, a prova recolhida através desse meio não deverá ser valorada, visto que não estão garantidos os requisitos de autenticidade, não contaminação e fidedignidade[113].

Ainda que entendamos o princípio à qual este último autor se baseia, numa perspetiva lógica-prática, não nos parece possível cumprir, pelo menos de uma maneira eficiente, este pressuposto. Ainda que presidir a diligência se mostre efetivamente compatível com os direitos aqui ofendidos, a ideia de que o juiz terá de ser a *primeira*

[112] *Ibidem*

[113] RODRIGUES (2010), p. 447. O autor não transmite de uma forma direta que o juiz tem de ser a primeira pessoa a tomar conhecimento do conteúdo do material apreendido, apenas remete esta situação para o art. 179 .º, n.º 3 do CPP, alegando que o juiz deve presidir a diligência. No entanto, cremos que a ideia transmitida pelo autor parte em assumir o cumprimento total do artigo referido.

pessoa a tomar conhecimento do conteúdo, nos termos do art. 179.º n.º 3 do CPP, não nos parece viável, inoperante na prática, tendo logo em conta a quantidade imensamente superior de prova apreendida em comparação com a simples correspondência.

Desta forma, considerando a possibilidade de centenas ou milhares de ficheiros que poderão ser apreendidos, o juiz simplesmente não tem a capacidade de assegurar em tempo útil esse requisito, devendo-se apenas pautar pela presença na diligência, cumprindo o elemento literal da legislação estipulado no art. 15.º.

De acordo com o art. 97.º, n.º 5 conjugado com o art. 269.º, n.º 1, alínea f) do CPP, com inspiração Constitucional, nomeadamente do art 205.º, n.º 1[114], o despacho supramencionado terá necessariamente de preencher os requisitos do dever de fundamentação a que qualquer ato decisório está sujeito[115], sendo certo que por motivos de estratégia de investigação, quando tal se afigure necessário, os fundamentos deverão estar redigidos de uma forma genérica[116]. No entanto, como nos ensina Inês Godinho[117], o termo *fundamentar* corresponde a um *processo através do qual são apresentadas razões que sejam susceptíveis de reconhecimento (legitimidade) e aceitação (validade) pelos destinatários.* Assim, será sempre necessário cumprir o processo de fundamentação. Também deverá estar elencado o visado da pesquisa bem como o seu objeto.

No objeto da recolha estão inseridos os elementos necessários para a eficácia desse meio de obtenção de prova, no ponto de vista investigatório, devendo também estar elencados os sistemas informáticos que envolvam o visado, as infrações penais que originaram o despacho, bem como o género de dados que serão sujeitos a pesquisa para depois serem alvo de uma apreensão[118]. No entanto, não deve ser prejudicada a possibilidade de extensão prevista no art. 15.º n.º 5.

Esta ordem ou autorização tem um prazo máximo de validade de 30 dias, nos termos do art. 15.º, n.º 2, em que, se não for cumprido nesse prazo, acarretará uma

---

[114] GODINHO, Inês Fernandes, Direito Processual Penal II - Sumários Desenvolvidos, Edições Universitárias Lusófonas, 2021, p. 11.

[115] RODRIGUES, Sara, O Dever de Fundamentação das Decisões Proferidas pela Autoridade da Concorrência, *in* Julgar *Online*, 2014, p. 4.
Esta autora define que f*undamentar é demonstrar as razões, os motivos, o núcleo onde assenta cada escolha. O fundamento dá a razão da verdade do conhecimento. Por um lado é anterior à verdade porque a fundamenta, por outro, é-lhe interior porque faz parte da verdade reflexamente conhecida. É o que dá consistência ao conhecimento e o ilumina por dentro.*

[116] NUNES (2021), p.210.

[117] GODINHO (2021), p. 11.

[118] ALBUQUERQUE, Paulo Pinto de, Comentário do Código de Processo Penal – à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Universidade Católica Editora, 2009, p. 512.

nulidade insanável, nos termos do art. 15.º n.º 6 conjugado com os artigos 174.º, n.º 4 e ainda 126.º, n.º 3 do CPP[119]. A autoridade judiciária que emitir o respetivo despacho deverá também referir o momento em que o prazo se inicia, impedindo assim situações que poderão ser facilmente definidas como *cheques em branco*, permitindo assim que os órgãos de polícia criminal que cumpram o despacho alterem o início do prazo, tendo em vista compatibilizar com os interesses que daí podem advir, nomeadamente no âmbito de razões técnicas e/ou táticas existentes num processo[120].

Relativamente às situações que os órgãos de polícia criminal poderão proceder à pesquisa sem autorização da autoridade judiciária[121], Benjamin Rodrigues alerta que esta possibilidade em concreto representa um perigo, admitindo que a existência do art. 15.º, n.º 3 aproxima-se de um *arrepio do paradigma constitucional e legal de restrição dos direitos fundamentais*[122].

O autor salienta que o perigo anteriormente referido, está nos alicerces da vantagem desleal de os órgãos de polícia criminal poderão solicitar o acesso aos dados informáticos sem previamente informar o suspeito que o poderá recusar, agindo assim contra a ideia do princípio da não-autoincriminação, e assim o suspeito ser *encaminhado* a consentir *voluntariamente*, permitindo que o órgão de polícia criminal proceda à pesquisa de dados informáticos sem autorização prévia da autoridade judiciária, cumprindo assim o art. 15.º, n.º 3, alínea a).

Referente à possibilidade exposta na alínea b) do artigo em estudo, este autor alerta da existência de um direito processual penal do inimigo, em que aos terroristas ou criminosos violentos ou organizados, são subtraídas algumas garantias dos seus direitos fundamentais *à luz das legítimas expectativas e garantias processuais penais que gerou na sua mente em virtude do quadro geral processual penal e constitucional em vigor na ordem jurídica portuguesa*[123]. Nos termos do art. 15.º, n.º 4 nesta última situação, a diligência deverá ser imediatamente comunicada à autoridade judiciária competente tendo em vista proceder à análise de validação processual, em que o não cumprimento deste requisito formal acarreta uma nulidade. Também, nas situações expostas no n.º 3,

[119] Não pode ser ignorado que este meio de obtenção de prova implica a intromissão na vida privada. Assim, a prova obtida sem serem cumpridas as formalidades legais representam uma nulidade insanável.
[120] RODRIGUES (2010), p. 448.
[121] Anteriormente referidas no capítulo 4.2.2.
[122] RODRIGUES (2010), p. 448 e 449.
[123] RODRIGUES (2010), p. 448 e 449.

alínea a) e b), o relatório deverá ser redigido e enviado à autoridade judiciária competente, nos termos do art. 253.º do CPP.

No âmbito de uma pesquisa, poderá surgir a convicção por parte dos órgãos de polícia criminal que estão a proceder à mesma, que é possível aceder aos dados que necessitam para produzir a prova, noutro sistema informático que não aquele inicial. No entanto, se através desse sistema inicial for possível aceder a esses dados instalados noutro sistema de uma forma legítima, a pesquisa poderá ser estendida, se a autoridade judiciária competente assim o entender, nos termos do art. 15.º, n.º 5 da Lei do Cibercrime[124].

Nos mesmos moldes das buscas domiciliárias ou não, nos termos do art. 176.º, n.º 2 do CPP, antes da diligência ser iniciada, ao visado deverá ser entregue cópia do despacho[125], com exceção das situações expostas no art. 15.º, n.º 3, tendo em vista o cumprimento das regras de execução de buscas estabelecidas no CPP, em consonância com o art. 15.º, n.º 6.

3.2.4- Consentimento por Quem Tiver a Disponibilidade ou Controlo dos Dados Informáticos

Este corresponde a um dos problemas que vigoram na Lei do Cibercrime.
Conforme já foi referido, de acordo com o art. 15.º, n.º 3, alínea a) dessa mesma legislação, quem tiver a disponibilidade ou controlo dos dados pode autorizar ou consentir que esse instrumento seja sujeito a uma pesquisa de dados informáticos, desde que fique documentado de alguma forma.

Desde logo, aqui verificamos a presença de um requisito diferente daquele que vigora nas buscas. As buscas também poderão ser consentidas, de acordo com o estipulado no art. 174.º, n.º 5, alínea b) e ainda art. 177.º, n.º 2, alínea b) do CPP. No entanto, este consentimento além de ter que ser documentado de qualquer forma, necessita de ser consentido pelo visado da própria busca, e não por quem tiver a disponibilidade do local, ou seja, a pessoa alvo de investigação é que pode consentir a

[124] RODRIGUES (2010), p. 449 e 450.
[125] VALENTE, Manuel Monteiro Guedes, Revistas e Buscas, Almedina, 2005, p. 48.

violação do seu direito de inviolabilidade do lugar reservado não livremente acessível ao público[126].

O consentimento prestado, nos termos do art. 15.º da Lei do Cibercrime, terá de ser prestado por quem tiver a disponibilidade ou o controlo desses dados informáticos. Se algum destes pressupostos de validade não existir, estaremos perante uma prova ilícita, violando o disposto no art. 126.º, n.º 3 do CPP[127].

Relativamente aos requisitos do consentimento, este seguirá as próprias regras da unidade do sistema jurídico. Isto é, o consentimento terá de ser livre e esclarecido. Quem consentir não poderá estar de alguma forma a ser perturbado, terá que ter noção da amplitude do seu direito que irá ser restringido – a reserva à intimidade da vida privada – , bem como terá que ter noção que pode impedir essa restrição. O não cumprimento destes requisitos poderá ser enquadrado que essas provas correspondem a uma ofensa à integridade física ou moral das pessoas, mesmo que haja o consentimento delas, nos termos do art. 126.º, n.º 2, alínea a) e b) do CPP. Pedro Albergaria refere que *o consentimento tem que ser um consentimento informado, ou seja, o produto de uma vontade esclarecida, que pode ponderar as vantagens e as desvantagens da sua escolha*[128], se ainda assim existir consentimento, verificamos uma *volenti non fit injuria*[129].

Também ainda como requisito, o consentimento deve ser expresso, não vigorando aqui o consentimento presumido previsto no art. 39.º do CP, bem como se a pessoa for cega, surda, muda, analfabeta, desconhecedora da língua portuguesa ou poder existir algum grau de inimputabilidade, é necessária a presença de um defensor oficioso com o objetivo de clarificar que a pessoa em causa presta o consentimento de forma válida e eficaz, nos termos do art. 64.º, n.º 1, alínea d), art. 92.º, resultando assim numa nulidade insanável prevista no art. 120.º, n.º 2, alínea c) do CP[130].

Abordemos agora o problema do consentimento. Como já foi referido, para existir o consentimento na pesquisa de dados informáticos, o titular desse consentimento deve ser aquele que tenha a disponibilidade ou controlo sobre esses dados, nos termos do art. 15.º, n.º 3, alínea a) da Lei do Cibercrime. Já nas buscas, nos termos do art. 174.º, n.º 5,

[126] ALBERGARIA, Pedro Soares de, in Comentário Judiciário do Código de Processo Penal, p. 594, Almedina, 2021.
[127] NUNES (2021), p. 219.
[128] ALBERGARIA (2021), p. 595.
[129] NUNES (2021), p. 222. No sentido literal significa: *a quem consente não se faz injúria*.
[130] NUNES (2021), p. 221.

alínea b) do CPP, é necessário que o consentimento seja prestado pelo visado. Assim, recorrendo ao elemento gramatical de fundamenta a interpretação desta norma jurídica, fica assim aberta a possibilidade para que um terceiro permita, ou melhor, consinta, que os certos dados sejam alvos de pesquisa, permitindo assim o acesso aos dados ali guardados.

Relativamente às buscas domiciliárias, quando existam várias pessoas a residir num certo imóvel, a doutrina segue para que, nos termos estipulados no art. 34.º, n.º 2 e n.º 3 da CRP, resulta que o titular do direito à inviolabilidade do domicílio pertence a todos os seus habitantes, independentemente das relações jurídicas aí existentes, nomeadamente arrendamento, propriedade ou até mesmo posse[131]. O domicílio representa uma parte espacial da dignidade humana e como tal, todas as pessoas que residam nesse domicílio devem consentir a restrição desse direito fundamental para a busca domiciliária cumprir as regras do consentimento[132].

Partindo dessa lógica, imagine-se que um computador é propriedade de uma empresa, mas é partilhado com vários funcionários. A investigação conclui que pode ser produzida prova contra um dos funcionários que normalmente utiliza esse computador. Se um outro funcionário que não é um alvo na investigação tem num certo momento a disponibilidade desses dados, seguindo o elemento gramatical do art. 15.º, n.º 3, alínea a), esse poderá dar o consentimento para que seja realizada uma pesquisa de dados informáticos nesse computador. Não nos parece lógica que assim seja. Passemos à fundamentação.

Numa primeira fase, como relembra João Conde Correia[133], por exemplo o computador, representa atualmente uma extensão da própria personalidade, podendo conter vários tipos de ficheiros que sirvam como *núcleo intangível e absoluto da intimidade de cada um*. Assim, respeitando a unidade de sistema e uma apropriada interpretação sistemática, só o titular desse bem jurídico – reserva da intimidade da vida privada – poderá prescindir e assim consentir que esse seu direito seja violado[134].

Em termos análogos, dada a proximidade intrínseca entre a busca e a pesquisa de dados informáticos, da mesma forma que a busca só pode ser consentida pelo visado, a

[131] GONÇALVES (2009), p. 220 e 221.
[132] ANDRADE, Manuel da Costa, Sobre as Proibições de Prova em Processo Penal, Coimbra Editora, 1992, p. 51 e 52.
[133] CORREIA (2014), p. 51.
[134] PEREIRA (2021), p. 573, nota de rodapé 7.

pesquisa deverá respeitar o mesmo preceito[135], tornando-se irrelevante o consentimento prestado pela pessoa não visada no inquérito que possua fisicamente os dados ou possa aceder-lhes de uma forma legítima[136].

No exemplo que demos, na verdade, o titular do bem jurídico violado seria diferente daquele que o consentiu. Portanto, não podemos deixar de assumir que tal consentimento não seria válido e que todas as provas obtidas através desse consentimento entram em rota de colisão com o art. 126.º, n.º 3 do CPP, bem como, principalmente, do art. 26.º, n.º 1, também o art. 32.º n.º 8, e ainda artigos 34.º e 35.º da CRP[137]. Aliás, nesse mesmo sentido, além de que para o consentimento ser válido deve ser prestado pelo visado do inquérito, todos os outros funcionários, bem como a própria empresa, devem prestar o consentimento para esse ser efetivamente válido[138], pelo menos na nossa modesta opinião, usando para o efeito a fundamentação já referida referente às buscas domiciliárias em que residam várias pessoas no local buscado.

3.2.5- Direitos Fundamentais Restringidos

A Constituição da República Portuguesa representa um sentido orientador para a regulação da matéria criminal, estipulando certos princípios explícitos – em que a Constituição refere expressamente a sua existência – e ainda princípios implícitos, em que embora não estejam expressamente previstos, pressupõe-se uma certa necessidade de correspondência e de reconhecimento desses princípios, mediante a interpretação de algumas normas jurídicas.

Esses princípios consolidam uma perspetiva teleológica e axiológica reconhecida num estado de direito democrático, tendo em vista um equilíbrio processual que estimule certos limites, estando intrinsecamente relacionados com a dignidade da pessoa humana e a vontade do povo, procurando a reprodução de uma sociedade livre, justa e solidária[139].

[135] ALBUQUERQUE (2009), p. 488.
[136] NUNES (2021), p. 224.
[137] PEREIRA (2021), p. 573, nota de rodapé 7.
[138] NUNES (2021), p. 225.
[139] Princípio fundamental previsto logo no art. 1.º da Constituição da República Portuguesa, onde se compreende a necessidade de estabelecer logo no seu artigo inicial, o fundamento da existência da CRP. Além disso, reconhecemos um requisito de obrigatoriedade de obediência a este artigo, perante todas as normas jurídicas de todos os ramos do Direito.

Referente aos princípios implícitos, verificamos uma clara ligação subjetiva entre a CRP e o Direito Penal do bem jurídico[140], o princípio da subsidiariedade do direito penal[141], o princípio da culpa[142] e o princípio da proporcionalidade das sanções penais[143].

Já relativamente aos princípios explícitos, na Constituição reconhecemos a existência do princípio da legalidade[144], princípio da reserva de lei[145], princípio da aplicação da lei penal mais favorável[146], insusceptibilidade de transmissão da responsabilidade penal[147] e ainda o princípio da não automaticidade dos efeitos das penas[148].

O direito processual penal, segundo vários juristas, representa *verdadeiramente um direito constitucional aplicado*[149], em que se verifica uma complementaridade jurídica entre a CRP e o CPP, em que na prática, este último estabelece as medidas em concreto suscetíveis a serem aplicadas compostas por requisitos, e o primeiro servirá como uma linha guia ou orientadora que essas medidas devem respeitar.

Já o direito penal, servirá como um reforço de validade à própria Lei Fundamental. Logo no seu art. 1.º, a CRP dispõe que *Portugal é uma República soberana, baseada na dignidade da pessoa humana e na vontade popular e empenhada na construção de uma sociedade livre, justa e solidária.* Nestes termos, é a finalidade principal de um Estado de Direito Democrático, a realização da justiça penal.

Esta finalidade, deverá ser entendida como um valor fundamental para a coexistência de uma comunidade.

---

[140] Art. 18.º, n.º 2 da CRP. Figueiredo Dias defende que os bens jurídicos político-criminalmente existentes, vigoram com a necessidade de uma reflexão Constitucional reconhecida. O mesmo é dizer que o bem jurídico para ser sujeito a proteção penal é necessário que a Constituição assim o determine- DIAS, Jorge de Figueiredo, Direito Penal, Parte Geral, Tomo I, 3.ª Edição, Gestlegal, 2019, p. 51 e ss. Embora a doutrina seja divergente, concordo com a posição de Faria Costa, em que recorrendo a uma fundamentação onto-antropológica do direito penal, associa que para um bem jurídico ser alvo de proteção penal, a CRP deve ser considerada uma orientação importante, mas já não obrigatória ou exclusiva.

[141] Art. 18.º, n.º 2 da CRP. O Direito Penal só intervém em *ultima ratio,* quando nenhum outro direito o consiga fazer.

[142] Deriva do próprio art. 1.º e do art. 27.º, n.º 1 da CRP.

[143] Deverá ser aplicada uma pena proporcional face à gravidade das infrações. Deriva do art. 1.º, art. 13.º, art. 18.º e art.º 25 da CRP.

[144] Previsto no art. 29.º, n.º n.º 1 e n.º 3 da CRP.

[145] A CRP determina em relação às mais variadas matérias, qual o órgão competente para legislar nessas matérias.

[146] Art. 29.º, n.º 4, p.f. da CRP.

[147] Art. 30.º, n.º 3 da CRP.

[148] Art. 30.º, n.º 4 da CRP.

[149] ANTUNES (2016), p. 16.

A Lei Fundamental, servirá como farol ou como guia orientadora, para todos os preceitos que envolvam a matéria criminal, a qual o Direito Penal deverá respeitar. Desde logo, o art. 18.º n.º 2 da CRP estabelece a necessidade imperiosa de só poderem ser restringidos determinados direitos, liberdades e garantias, nos casos expressamente previstos na Constituição. Já o art. 29.º da CRP estabelece vários requisitos obrigatórios para cumprimento, para ser possível a aplicação da lei criminal.

Assim, Jorge Reis Novais[150], alerta que, tendo em conta que a recolha deste meio de obtenção de prova implica necessariamente, uma limitação de Direitos, Liberdades e Garantias, deverá ser respeitado o princípio constitucional da proibição do excesso, terminologia adotada por este autor, ou então, o princípio da proporcionalidade comummente denominado, assim, tal e qual como em todo o universo dos meios de obtenção de prova.

Nesta senda, devemos pautar pelo respeito do dever de fundamentação previsto nos atos decisórios, neste caso, no despacho de autorização da pesquisa de dados informáticos, tendo em vista evitar *pesquisas informáticas meramente exploratórias*, que se revelam inconciliáveis com a ideia do princípio da proporcionalidade ou proibição do excesso[151], à qual Duarte Nunes citando Thomas K. Clancy, denominou como *fishing expeditions*[152].

3.2.6- Apreensão de dados informáticos

O regime de apreensões desses dados, está regulado em lei especial, também na Lei do Cibercrime, especificamente no art. 16.º.

Para a pesquisa de dados informáticos cumprir o seu objetivo, é necessário que esses dados sejam apreendidos para posteriormente ser validada a apreensão, cabendo essa parte à autoridade judiciária, existindo o prazo de 72 horas, nos termos art. 16.º, n.º 4 da Lei do Cibercrime, mesmo prazo previsto no CPP, especificamente, no art. 178.º, n.º 6.

[150] NOVAIS, Jorge Reis, Os Princípios Constitucionais Estruturantes da República Portuguesa, Coimbra Editora, 2004, p. 161 e 193.
[151] NUNES, Duarte Alberto Rodrigues, O Problema da Admissibilidade dos Métodos "Ocultos" de Investigação Criminal Como Instrumento de Resposta À Criminalidade Organizada, Gestlegal, 2019, p. 473.
[152] NUNES (2021), p. 211.

Esta apreensão deverá ocorrer quando esses dados forem encontrados no âmbito de uma pesquisa informática ou qualquer tipo de acesso legítimo[153] a um sistema informático, desde que esses dados sejam necessários para produzir a prova, sempre com o fundamento da descoberta da verdade material. Nesses dados estão inseridos os *metadados*, os *documentos informáticos*, bem como os programas que se afigurem necessários para proceder à respetiva análise dos dados apreendidos. Esta apreensão além de corresponder a um meio de obtenção de prova, podemos referir que se trata de um meio de conservação de prova[154].

Também aqui se inserem a apreensão de dados recolhidos através de uma fonte aberta[155], nomeadamente dados adquiridos numa rede social ou qualquer tipo de situação que se revele compatível com a ideia base fonte aberta[156].

Os dados ou documentos informáticos que poderão ser atentatórios contra a intimidade do titular desse direito fundamental, bem como de terceiro não visado nessa pesquisa, devem ser apresentados ao Juiz, que, consoante os próprios interesses da investigação do caso em concreto, pondera se devem ou não ser anexos ao processo, nos termos do art. 16.º, n.º 3 da Lei do Cibercrime[157]. Aqui verificamos a ideia de um género de proibição relativa, visto que esse meio de prova se não for apresentado e juntado ao processo por um juiz, acarretará uma nulidade de prova[158], violando o art. 126.º, n.º 3 do CPP.

A apreensão dos dados informáticos, considerando os interesses do caso em concreto, bem como os princípios da proporcionalidade e da adequação, assume diversas formas, devidamente expostas no art. 16.º, n.º 7 da Lei do Cibercrime. Em boa verdade, apenas a alínea a) e b) do artigo aqui em estudo, parece-nos que representam a verdadeira lógica de apreensão, enquanto as alíneas c) e d) representam um género de meios de proteção da prova[159].

---

[153] Aqui podem-se inserir, a título de exemplo, a busca ou revista em que o sistema informático esteja no local buscado ou na pessoa revistada, nos termos dos artigos 174.º e seguintes do CPP. Já a situação de entrega de dados informáticos no âmbito da apresentação de uma queixa por parte do queixoso, já não se enquadra num acesso legítimo, mas não deixa de ser uma apreensão válida.
[154] NUNES (2021), p. 261.
[155] *Open source*. Dados livremente acedidos pelo público em geral.
[156] NUNES (2021), p. 262.
[157] NUNES (2021), p. 269.
[158] RODRIGUES (2010), p. 451.
[159] FIDALGO (2019a), p. 155.

3.2.7- Conhecimentos Fortuitos e a Pesquisa de Dados Informáticos

Existem algumas ligações dos conhecimentos fortuitos com a pesquisa de dados informáticos. Desde logo, os conhecimentos fortuitos ocorrem no âmbito de uma investigação criminal que corra contra certo suspeito, em que exista fundamento para a admissibilidade de escutas telefónicas, estando preenchidos os seus requisitos[160], os órgãos de polícia criminal, obtém mediante esse meio de obtenção de prova lícito, conhecimento de quaisquer factos com índole criminosa que não estão relacionados com o crime que previu a admissibilidade das escutas telefónicas. A título exemplificativo, imaginemos que um certo e determinado individuo está a ser investigado sobre a prática de um crime de tráfico de estupefacientes[161] e foi autorizado pelo juiz de instrução, a admissibilidade de recolher meios de prova desse crime através desse meio de obtenção. Nesse âmbito, através das escutas, o suspeito reconheceu que se apropriou de um veículo para apenas se deslocar para um certo local e que não tinha o *animus* de ser o novo proprietário de veículo, enquadrando-se assim no preenchimento do tipo legal de crime com a epígrafe *furto de uso de veículo*, nos termos do art. 208.º do CP. Este último ato ilícito, não é enquadrável nos crimes de catálogo pré-estabelecidos pelo legislador para efeitos de admissão da utilização desse meio de obtenção de prova. Relativamente ao *furto de uso de veículo*, será que este meio probatório poderá ser usado para efeitos de aplicação de uma consequência jurídica?

Nas palavras de Costa Andrade, *qui dinde quanto aos conhecimentos ou factos fortuitamente recolhidos, isto é, que não se reportam ao crime cuja investigação legitimou a sua realização?*[162].

Desde já, é possível estabelecer uma relação direta com os conhecimentos fortuitos e o regime das escutas telefónicas, regime esse que para efeitos de admissibilidade da restrição do direito à privacidade, pressupõe requisitos limitadores, tendo em vista a proteção desse mesmo direito, nos termos do art. 34.º, n.º 1 da CRP onde dispõe que *o domicílio e o sigilo da correspondência e dos outros meios de comunicação*

[160] Requisitos de admissibilidade previsto no art. 187.º, n.º 1 do CPP, em que as escutas *só podem ser autorizadas durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público,* quanto a crimes catálogo, previstos no n.º 1 e 2.
[161] Crime catálogo previsto no art. 187.º, n.º 1, alínea b) do CPP.
[162] ANDRADE (1992), p. 304.

privada são invioláveis e o n.º 4 do mesmo artigo, dispõe que *é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal.* Nestes termos, a lei que regula a matéria de processo criminal é o CPP, existindo uma conexão deste artigo da Constituição com o regime das escutas telefónicas estipulados nos artigos 187.º a 190.º do CPP.

Ainda neste âmbito, existe uma diferença entre os conhecimentos fortuitos e os conhecimentos de investigação. Costa Andrade identifica os conhecimentos da investigação *os factos que estejam numa relação de concurso ideal e aparente com o crime que motivou e legitimou a investigação por meio da escuta telefónica* conclui que *o mesmo valendo para os delitos alternativos que com ele estejam numa relação de comprovação alternativa de factos*[163]. Como se compreende, verifica-se uma certa semelhança entre os dois tipos de conhecimentos, sendo que este último, estará melhor relacionado quando esteja a decorrer uma investigação contra uma certa associação criminosa, num sentido mais amplo.

Ainda utilizando como referência o exemplo anteriormente referido, complementa-se agora que o suspeito terá utilizado o citado veículo para se deslocar até ao local onde iria vender ou adquirir o produto estupefaciente, ou seja, nestes termos enquadrar-se ia num conhecimento de investigação e não apenas num conhecimento fortuito.

Desta forma, subentende-se uma certa subsidiariedade, visto que todos os conhecimentos obtidos que não se insiram no conhecimento de investigação inserem-se no conhecimento fortuito.

Dada à ligação intrínseca existente entre os conhecimentos fortuitos e as escutas telefónicas, o art. 187.º n.º 7 do CPP responde à possibilidade de valoração de provas obtidas através desse meio. Esta norma, embora não utilize a expressão que neste momento está em estudo, prevê a admissibilidade desses conhecimentos serem valorados em juízo, admitindo que se tiver sido obtida alguma informação contra alguma pessoa

[163] ANDRADE (1992), p. 306.

inserida no n.º 4 do mesmo artigo[164], pode o conhecimento fortuito ser valorado, na medida em que for indispensável à prova de algum crime previsto no catálogo tipificado no n.º 1, ou seja, se o conhecimento fortuito seja ele por si só um crime em que há a admissibilidade de escutas telefónicas, considerar-se-á uma prova lícita. Esta prova pode ser utilizada em outro processo, em curso ou ainda em processos a instaurar. Em qualquer dos casos, mesmo que não preencha os requisitos anteriormente expostos, os órgãos de polícia criminal devem transmitir a notícia do crime ao MP, nos termos do art. 248.º do CPP[165]/[166].

Antes da introdução da Lei n.º 48/2007, de 29 de agosto[167], Francisco Aguilar[168] abordou a temática sobre a valoração dos conhecimentos fortuitos através de escutas telefónicas, utilizando com referência o ordenamento jurídico Alemão. Este autor, considerando a inexistência do n.º 7 no art. 187.º do CPP, assumiu a *recusa total de valoração* dos conhecimentos fortuitos *por força da reserva constitucional da mesma*. Fundamentou que a sua valoração representaria uma devassa da vida privada e ao sigilo das comunicações, e que a sua restrição só deverá ocorrer quando a lei assim o determine, nos termos dos artigos 18.º, n.º 2 e 34.º, n.º 4 da Constituição. Reforçou que se os conhecimentos fortuitos representavam uma prova proibida, e a consequência da sua valoração é a nulidade insanável, nos termos do art. 128.º, n.º 3 do CPP.

No entanto, Francisco Aguilar[169], conclui que o legislador deveria possibilitar a valoração dos conhecimentos fortuitos, quando os conhecimentos preencham os elementos catalogares das escutas telefónicas e, cumulativamente, quando não seja possível obter prova de outra forma, *reforçando-se, assim, o postulado da perseguição penal exigido pela necessidade de prevenção geral sem, contudo, se postergarem os limites decorrentes da reserva de lei, da proporcionalidade (no elenco legal de delitos assim elucidáveis) e da subsidiariedade (em face das necessidades probatórias do novo*

---

[164] A intercepção e a gravação previstas nos números anteriores só podem ser autorizadas, independentemente da titularidade do meio de comunicação utilizado, contra:
a) Suspeito ou arguido;
b) Pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou
c) Vítima de crime, mediante o respectivo consentimento, efectivo ou presumido.

[165] SILVA (2008), p. 256.

[166] ANDRADE (1992), p. 309.

[167] Lei que procedeu a várias alterações ao CPP, aditando o art. 187.º n.º 7.

[168] AGUILAR, Francisco, Dos Conhecimentos Fortuitos Obtidos Através de Escutas Telefónicas – Contributo para o seu Estudo nos Ordenamentos Jurídicos Alemão e Português, Almedina, 2004, p. 108 e 109.

[169] AGUILAR (2004), p. 109.

processo). Na verdade, após a publicação da obra do autor agora em estudo, parece-nos que o legislador seguiu esse caminho na introdução da Lei n.º 48/2007, de 29 de agosto.

Relativamente à opinião jurisprudencial, ela segue o mesmo caminho que a doutrina. O Tribunal da Relação do Porto[170] dispôs que *I – Os chamados conhecimentos da investigação são factos obtidos através de uma escuta telefónica que se inserem na mesma história de vida do crime investigado, pelo que podem validamente ser usados na investigação. II – Os conhecimentos da investigação podem validamente ser usados na investigação mesmo que o arguido seja terceiro relativamente a quem respeitava a autorização de interceção e gravação das comunicações, desde que essa autorização se refira a um suspeito, que os crimes dos arguidos escutados e os que assim se evidenciaram como praticados respeitem a crimes de catálogo e, por fim, que os crimes de que o arguido é suspeito se inseriram na história da investigação representada por aqueloutros. III - Ainda que se tratasse de conhecimentos fortuitos as escutas e consequentes transcrições das comunicações telefónicas efetuadas seriam prova válida contra o recorrente não escutado na medida em que nada impede que a condição de suspeito ou de arguido resulte da própria escuta, desde que reportada a crime de catálogo. Neste sentido, tanto a doutrina como a jurisprudência, na sua grande maioria, admitem a possibilidade de valoração.*

No entanto, como aqui já foi abordado, a pesquisa de dados informáticos não pressupõe a existência de crimes catálogo, sendo difícil reconhecer a equiparação entre as escutas telefónicas e a pesquisa de dados informáticos.

Para este efeito, embora subsista alguma semelhança entre os conhecimentos fortuitos e a pesquisa de dados informáticos, os seus efeitos são tendencialmente diferentes, visto que os conhecimentos fortuitos poderão ser valorados como prova, dada à existência do princípio da necessidade.

Embora o regime dos conhecimentos fortuitos esteja previsto expressamente no art. 187.º do CPP relativamente às escutas telefónicas, essa possibilidade não parece existir no art. 15.º da Lei do Cibercrime.

Desde logo, o próprio art.15.º, n.º 1, artigo onde expõe os pressupostos de admissão de pesquisa de dados informáticos, informa da necessidade de esses dados informáticos serem *específicos e determinados*, demonstrando, claramente, a ideia de aplicar um regime mais restritivo na recolha da prova, diferentemente daquele estipulado

[170] Acórdão do TRP - Processo n.º 1885/10.8PIPRT.P1, de 05.06.2013.

nas escutas telefónicas, ainda que a admissão deste último meio de obtenção de prova terá que ser *indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter*, existindo ainda os requisitos dos crimes catálogo já referidos.

Os dados informáticos estão definidos no art. 2.º alínea b) da Lei do Cibercrime como *qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função*. Cremos que a ideia adjacente ao pressuposto da pesquisa de dados informáticos em que esses dados devem ser *específicos e determinados*, resultam numa ideia de que os dados informáticos aqui em causa, terão que ser necessários para produzir a prova do inquérito que deu origem à pesquisa.

Esta especificidade exposta no regime de admissão da pesquisa de dados informáticos, muito embora não exista previsão legal que preveja este entendimento, é do nosso entender que os conhecimentos fortuitos na pesquisa de dados informáticos deverão ser considerados, mesmo que não exista inquérito a correr contra o visado da pesquisa relativamente à suspeita do tipo legal de crime que deu origem a esse conhecimento fortuito.

Para este entendimento, sustentamos a ideia da existência deste meio de obtenção prova, até porque, muito embora possamos referir que este meio de obtenção de prova é lesivo dos direitos fundamentais do visado, este não representa um meio de obtenção de prova de *ultima ratio*, diferentemente daquele que vigora nas escutas, até porque a própria ofensa não representa uma lesão intensa aos direitos fundamentais do visado, existindo até autores que defendem que para a pesquisa ser efetuada, bastará que exista um grau de suspeita objetificável, que significa o mesmo grau de suspeita que dá origem à instauração de um inquérito[171].

Assim, tendo em consideração os princípios da proporcionalidade, adequação e o da necessidade, se os dados informáticos obtidos forem diferentes daqueles que originou a pesquisa, mas poderão configurar um tipo legal de crime, devem ser considerados como meios de prova válidos para efeitos de valoração, devendo ser validados pela autoridade judiciária competente.

Este nosso entendimento também tem por base o regime legal que vigora em Espanha, sobre este meio de obtenção de prova. O art. 588 bis i. da *Ley de Enjuiciamiento*

[171] NUNES (2021), p. 176 a 178.

Criminal[172], remete para o art. 579 bis[173]., que significa que os conhecimentos fortuitos ou *descobertas casuales*, terão de ser analisados pelo juiz que emitiu o despacho da pesquisa de dados informáticos. Esse mesmo juiz terá de analisar o pedido inicial que deu origem à pesquisa, o despacho que a proferiu, bem como todos os pedidos e decisões de prorrogação presentes no processo original. Assim, se esse juiz considerar que estão preenchidos todos os pressupostos para a valoração da prova, este poderá autorizar a valoração dos conhecimentos fortuitos[174].

No âmbito da pesquisa de dados informáticos, os conhecimentos fortuitos representam uma realidade, merecendo uma melhor atenção por parte da doutrina e da jurisprudência. Não raras as vezes, a prova recolhida poderá configurar um tipo legal de crime distinto daquele que deu origem ao processo, especialmente a prova recolhida através da apreensão de correio eletrónico e de registos de comunicação de natureza semelhante.

Assim, podemos considerar que a pesquisa de dados informáticos (art. 15.º) está direcionada para dois caminhos distintos, em simultâneo ou não, concretamente, a apreensão de dados informáticos (art. 16.º)[175] e/ou a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante (art. 17.º)[176], existindo regimes processuais distintos a aplicar, consoante o caso em concreto.

---

[172] *Artículo 588 bis i. Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales.*
El uso de las informaciones obtenidas en un procedimiento distinto y los descubrimientos casuales se regularan con arreglo a lo dispuesto en el artículo 579 bis.

[173] *Artículo 579 bis. Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales.*
1. El resultado de la detención y apertura de la correspondencia escrita y telegráfica podrá ser utilizado como medio de investigación o prueba en otro proceso penal.
2. A tal efecto, se procederá a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia. Se incluirán entre los antecedentes indispensables, en todo caso, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen.
3. La continuación de esta medida para la investigación del delito casualmente descubierto requiere autorización del juez competente, para la cual, éste comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento. Asimismo se informará si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, comunicando el momento en el que dicho secreto se alce.

[174] RAYÓN BALLESTEROS, Maria Concepción, Medidas de Investigación Tecnológica en el Proceso Penal: La Nueva Redacción de La Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015, *in* Anuario Jurídico y Económico Escurialense, LII, 2019, p. 183 e 184, rodapé 4.

[175] Já abordado no capítulo 3.2.6.

[176] Abordado no capítulo 4.

4- Apreensão de Correio Eletrónico e de Registos de Comunicação de Natureza Semelhante

4.1- Acórdão do Tribunal Constitucional n.º 687/2021

Recentemente, o Tribunal Constitucional foi requisitado pelo Presidente da República, nos termos do art. 278.º, n.º 1 da Constituição, no âmbito de uma fiscalização preventiva de constitucionalidade, para submeter à apreciação de uma alteração ao art. 17.º da Lei do Cibercrime proposta pelo Decreto n.º 167/XIV.

Este decreto propunha que o art. 17.º passasse a redigir:

> Artigo 17.º
>
> Apreensão de mensagens de correio eletrónico ou de natureza semelhante
>
> 1 – Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontradas, armazenadas nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou de natureza semelhante que sejam necessárias à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a sua apreensão.
>
> 2 – O órgão de polícia criminal pode efetuar as apreensões referidas no número anterior, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 15.º, bem como quando haja urgência ou perigo na demora, devendo tal apreensão ser validada pela autoridade judiciária no prazo máximo de 72 horas.
>
> 3 – À apreensão de mensagens de correio eletrónico e de natureza semelhante aplica-se o disposto nos n.os 5 a 8 do artigo anterior.
>
> 4 – O Ministério Público apresenta ao juiz, sob pena de nulidade, as mensagens de correio eletrónico ou de natureza semelhante cuja apreensão tiver ordenado ou validado e que considere serem de grande interesse para a descoberta da verdade ou para a prova, ponderando o juiz a sua junção aos autos tendo em conta os interesses do caso concreto.
>
> 5 – Os suportes técnicos que contenham as mensagens apreendidas cuja junção não tenha sido determinada pelo juiz são guardados em envelope lacrado, à ordem do tribunal, e destruídos após o trânsito em julgado da decisão que puser termo ao processo
>
> 6 – No que não se encontrar previsto nos números anteriores, é aplicável, com as necessárias adaptações, o regime da apreensão de correspondência previsto no Código de Processo Penal.

O requerente suscitou as suas dúvidas de compatibilidade Constitucional, podendo existir um vício de incompatibilidade material, por *violação do direito à inviolabilidade do domicílio e da correspondência, na interpretação que lhe tem sido dada pelo Tribunal Constitucional, e do direito à utilização da informática, não respeitando a exigência de proporcionalidade resultante do regime material dos direitos, liberdades e garantias, conforme decorre da conjugação do artigo 18.°, n.º 2, respetivamente, com os artigos 34.°, n.º 4, por um lado, e com o artigo 35.°, por outro, todos da Constituição da República Portuguesa (doravante, CRP).*

Aqui em causa, como dispôs o requerente, é que aparentemente, embora o correio eletrónico ou comunicações de natureza semelhantes sejam análogos à correspondência tradicional, o que em bom rigor, numa perspetiva de evolução, o primeiro veio substituir este último, se esta alteração procedesse, iriam existir dois regimes diferentes que tratam matérias iguais. Isto é, enquanto o correio eletrónico ou comunicações de natureza semelhante admitiria a possibilidade de apreensão sem a intervenção do juiz, o correio tradicional, regime que vigora no art. 179.º do CPP, exigiria sempre a intervenção do juiz.

Os Juízes conselheiros, com a Constituição como referência, atendendo que a Lei Fundamental permite a *ingerência das autoridades públicas* nas comunicações, quando esteja previsto no processo penal, nos termos do art. 34.º, n.º 4, esta competência é exclusiva e indelegável ao Juiz, numa perspetiva de garantia dos direitos fundamentais no processo criminal, nos termos do art. 32.º n.º 4 da CRP. Ademais, esta ingerência por parte de um Juiz poderá apenas ser dispensada, em situações pontuais, numa perspetiva excecional, e logicamente rigorosas, garantindo que a recolha de prova não se revele excessiva, compatibilizando com os próprios interesses da investigação criminal. Especificaram que estes casos representam as atuações preventivas ou cautelares, quando exista perigo na demora ou urgência, numa perspetiva de conservação da prova, sendo ainda necessária a validação judicial[177].

Referiram ainda que, considerando os princípios orientadores que vigoram no nosso sistema jurídico, principalmente na Constituição, a nova redação do art. 17.º não se revela compatível com o princípio da necessidade e da proporcionalidade, bem como a exigência de excecionalidade que o art. 18.º, n.º 2 da CRP assim exige para que a lei restrinja os direitos fundamentais. Assim, para a apreensão do correio eletrónico ou registos de comunicações de natureza semelhante, não se vê a necessidade de afastar a intervenção do JIC.

Concluíram que, embora esta intromissão assuma um interesse relevante para a investigação criminal, avocando assim a possibilidade da exceção da inviolabilidade da correspondência e sigilo das comunicações, nos termos do art. 34.º, n.º 1 e n.º 4, bem como a possibilidade da restrição da proteção dos dados pessoais, neste caso, no âmbito da utilização da informática, nos termos do art. 35.º, n.º 1 e n.º 4, e ainda a possibilidade da violação das manifestações da própria reserva de intimidade da vida privada, nos termos do art. 26.º, n.º 1, todos direitos fundamentais. Esta exceção deverá ser assegurada

[177] Vulgo Medidas Cautelares de Polícia

pelo JIC, como órgão de soberania independente, imparcial, e *especialmente vocacionado para a proteção dos direitos fundamentais*, nos termos do art. 32.º, n.º 4, e deverá ser compatível com as exigências impostas no art. 18.º, n.º 2 da Lei Fundamental, numa perspetiva fundamental de proporcionalidade.

Assim, o Tribunal Constitucional pronunciou que a nova redação proposta do art. 17.º da Lei do Cibercrime é inconstitucional, *por violação dos direitos fundamentais à inviolabilidade da correspondência e das comunicações (consagrado no artigo 34.º, n.º 1, da CRP), à proteção dos dados pessoais no âmbito da utilização da informática (nos termos do artigo 35.º, n.ºs 1 e 4, da CRP), enquanto refrações específicas do direito à reserva de intimidade da vida privada, (consagrado no artigo 26.º, n.º 1, da Constituição), em conjugação com o princípio da proporcionalidade (nos termos do artigo 18.º, 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).*

4.2- Apreensão de Correspondência

Partindo de uma definição do termo *correspondência*, encontramos um auxílio real que nos permite chegar a uma conclusão na própria legislação. O próprio art. 179.º do CPP enquadra-nos que a apreensão de correspondência poderão ser *cartas, encomendas, valores, telegramas ou qualquer outra correspondência*[178].

A apreensão de correspondência é regulada por uma forma especial de apreensão, incluída no CPP, em que dado a sua intrínseca ligação com a violação do segredo de correspondência com alicerce Constitucional, é necessário o preenchimento de certos pressupostos para acautelar a violação desse direito. O art. 34.º, n.º 1 da CRP estipula a inviolabilidade da correspondência, do domicílio bem como de outros meios de comunicação privada. No entanto, o n.º 4 procura evidenciar algumas exceções quando a lei de matéria de processo criminal assim o preveja. Esta apreensão, também implica uma restrição ao direito de propriedade sobre a correspondência apreendida, também com proteção Constitucional, especificamente no art. 62.º[179].

[178] Art. 179.º, n.º 1 do CPP.
[179] CORREIA, João Conde, *in* Comentário Judiciário do Código de Processo Penal, Comentário ao Artigo 178.º, Almedina, 2021, p. 653.

Correspondência, de um ponto de vista tradicional, representa uma ideia de comunicação entre duas pessoas que se encontram distantes[180], mas também abrange as *missivas, encomendas, valores, telegramas e qualquer forma estereotipada de correio, desde que enviada para um destinatário determinado*[181].

Só um juiz pode ordenar ou autorizar a apreensão da correspondência, e, após a dita apreensão, será o primeiro a ter conhecimento do conteúdo da correspondência. Se o conteúdo se revelar útil para a descoberta da verdade, deverá ser apensado ao processo. Já se não tiver qualquer fundamento para o processo, a correspondência deve ser devolvida ao visado[182].

Existe uma linha ténue que limita a acção desta proteção. Falamos, naturalmente, da correspondência fechada, o que representa a sua confidencialidade. Neste campo, tanto a doutrina como a jurisprudência são unânimes no gozo da proteção aqui explanada[183]. No entanto, em sentido oposto, quando a correspondência é aberta pelo destinatário, deixa de usufruir desta proteção, passando a usufruir da proteção de um mero documento, nos termos do art. 178.º do CPP[184].

Ainda para concluir, a ideia da diferença de proteção entre a correspondência fechada ou aberta está também associado à previsão do tipo legal de crime previsto no art. 194.º do CP, em que dispõe que preenche o tipo legal de crime quem, sem qualquer consentimento, abrir a correspondência que se encontre fechada.

4.3- Correio Eletrónico e Registos de Comunicações de Natureza Semelhante

Partindo da apreensão da correspondência, avançamos para o correio eletrónico. O correio eletrónico surge como uma ferramenta considerada essencial nos tempos de hoje. Por isso, considerando a necessidade de recolha de prova que poderá ser essencial para um processo, o art. 17.º da Lei do Cibercrime pretendeu salvaguardar a apreensão

[180] RODRIGUES, Benjamin Silva, Das Escutas Telefónicas à Obtenção da Prova [em ambiente] Digital, Tomo II, Coimbra Editora, 2009, p. 56.
[181] ALBUQUERQUE (2009), p. 493.
[182] ALBUQUERQUE (2009), p. 494.
[183] ANDRADE (2009), p. 159; Ainda CORREIA (2021), p. 656. Também, ALBUQUERQUE (2009), p. 493.
[184] ALBUQUERQUE (2009), p. 493.

do correio eletrónico e registos de comunicações de natureza semelhante[185], no decurso de uma pesquisa de dados informáticos. Neste sentido, o artigo em referência dispõe que *quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, 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, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.*

Pedro Dias Venâncio, associa a criação deste artigo, a uma conjuntura processual entre o art. 15.º, 16.º e 17.º da Lei do Cibercrime, previamente exposta no art. 19.º da Convenção do Cibercrime[186]. Já Duarte Nunes[187], associa que o nosso legislador, tendo em conta a sua *liberdade de conformação*, criou esta norma sem qualquer tipo de articulação com a Convenção do Cibercrime.

A par da pesquisa de dados informáticos, também inexiste qualquer catálogo de crimes que permita a aplicação deste meio de obtenção de prova, muito embora dada a correspondente analogia entre o regime exposto no art. 17.º e o art. 179.º do CPP – em que este último exige que para apreender correspondência é necessário que o crime seja punível com uma pena de prisão superior a 3 anos –, acreditamos que o que rege a correspondente apreensão é que o exposto no art. 17.º conjugado com o art. 11.º, n.º 1 alínea a) a c), existindo assim um *universo aberto de crimes* que permitam a apreensão de correio eletrónico e de registos de comunicação de natureza semelhante[188].

4.3.1- Apreensão do Correio Eletrónico Lido e não Lido

Neste âmbito existem várias posições em sentido oposto[189]. Há doutrina que apoia a tese de que o correio eletrónico merece toda a proteção existente na apreensão de

[185] Aqui poderão se inserir uma panóplia de comunicações em constante evolução seja através de comunicação escrita, gráfica ou até mesmo por mensagens de voz, nomeadamente qualquer comunicação de uma rede social, seja, *Facebook, Snapchat, whatsapp, instagram, viber, Teams, Messenger,* bem como muitas outras que poderão se inserir neste campo. Como seria de esperar, também se inserem as SMS, MMS ou até EMS.
[186] VENÂNCIO (2011), p. 116.
[187] NUNES (2021), p. 329 e 330.
[188] NUNES (2021), p. 351.
[189] ANDRADE (2009), p. 164.

correspondência tradicional, mesmo que se possa considerar árduo o apuramento se a mensagem eletrónica já foi lida pelo destinatário – visto que a qualquer momento o visado pode marcar o email como não lido –, devendo vigorar as mesmas regras que se encontra na correspondência tradicional. Isto é, para efetivamente ser necessário despacho judicial para apreender o correio eletrónico, é necessário que a mensagem eletrónica não tenha sido lida. Se tudo indicar que a mensagem eletrónica além de recebida já foi lida, vigoram aqui as regras de apreensão gerais, não sendo necessário despacho judicial[190]. Ademais, como estamos a falar de meios eletrónicos, aqui já não falamos das regras gerais do art. 178.º do CPP, mas sim, das regras elencadas no art. 16.º da Lei do Cibercrime, aqui já referidas, sendo suficiente a intervenção do magistrado do MP[191].

Assim, a correspondência eletrónica entregue e já lida, como resulta num mero documento, o destinatário pode fazer o uso que bem entender, nomeadamente, até poderá entregar esse mero documento aos órgãos de polícia criminal ou ao MP, tendo em vista sustentar a prova no âmbito de uma perseguição criminal, não sendo necessário despacho judicial, visto que já não se verifica a existência do sigilo da correspondência[192].

Seguimos de perto a tese de Sónia Fidalgo. Isto é, para ser possível apreender correio eletrónico e registos de natureza semelhante é necessário existir despacho judicial prévio. Vejamos, é o próprio art. 17.º da Lei do Cibercrime que remete para o regime da apreensão de correspondência previsto no art. 179.º, n.º 1 do CPP, em que é necessária a intervenção de um juiz para a apreensão ser válida. Além disso, o próprio art. 17.º é imperativo, onde dispõe que *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 doutrina contrária[193], aponta para problemas na aplicação prática deste regime, devido à imensidão de correspondência eletrónica cuja apreensão o juiz terá de autorizar ou ordenar, defendendo que o correio eletrónico pode ser submetido a um género de *apreensão cautelar* ou *provisória,* e mais tarde, remetido ao juiz para efetivamente autorizar a apreensão e proceder à junção da prova ao processo. Se o juiz não autorizar, a apreensão *cautelar* não se mantém. É certo que poderão surgir dificuldades na aplicação

[190] VERDELHO, Pedro, Apreensão de Correio Eletrónico em Processo Penal, *in* Revista do Ministério Público, ano 25, Out/Dez, 2004, n.º 100, p. 159;
[191] CORREIA (2014), p. 41.
[192] CORREIA (2021), p. 657.
[193] VERDELHO, Pedro, A Nova Lei do Cibercrime, Revista de Direito Comparado Português e Brasileiro, Tomo LVIII, n.º 320, Scientia Ivridica, Universidade do Minho, Out-Dez 2009, p. 743 e 744.

prática, mas o que ainda se revela mais certo é a que a lei faz essa exigência[194], aliás, como foi confirmado, mais recentemente pelo Tribunal Constitucional[195].

No que concerne à correspondência lida ou não lida, ou então, aberta ou fechada, no correio eletrónico ou registos de comunicações de natureza semelhante, não nos parece ser assim tão idêntico, principalmente, porque contrariamente à correspondência tradicional, o correio eletrónico ou registos de comunicações de natureza semelhante, facilmente podem ser alteradas de um estado de lido para não lido, literalmente à distância de um único *click.* Assim, atendendo à evidente manipulação processual que daí pode advir, tanto dos órgãos de justiça como do próprio arguido, também porque aqui em estudo estão Direitos Fundamentais em que a sua restrição deverá ser bem fundamentada, bem como o próprio elemento gramatical exposto no art. 17.º da Lei do Cibercrime, não suscita qualquer regime de aplicação diferente quando o correio eletrónico ou registos de comunicações de natureza semelhante seja lido ou não lido pelo seu destinatário, acreditamos que este conceito não deve vigorar, sendo necessária a intervenção do juiz, mediante um despacho judicial prévio, para proceder à apreensão de qualquer correio eletrónico ou registos de comunicações de natureza semelhante, seja lido ou não lido[196].

A par da apreensão da correspondência, não existe qualquer diferença de aplicação processual no que diz respeito à correspondência aberta ou lida em detrimento da correspondência fechada ou não lida. Pelo menos, de um ponto de vista legislativo, esta diferença não é imediatamente visível, deixando abertura para um conflito desnecessário de ideias, em que não se consegue absorver na legislação, perentoriamente, a diferença entre correio eletrónico ou correspondência tradicional lida ou não lida, sendo necessário o recurso à doutrina e à jurisprudência para sanar o conflito[197].

Rogério Bravo[198], embora tenha defendido a sua tese num período anterior à Lei do Cibercrime, parece defender, admitindo que representa uma minoria, que o correio eletrónico ou as mensagens de correio eletrónico, quando são recebidas num certo sistema informático, serão apenas dados informáticos armazenados, comparando esse documento

[194] FIDALGO (2019a), p. 157 e 158.
[195] Acórdão n.º 687/2021.
[196] Com a mesma opinião, FIDALGO, Sónia, Apreensão de Correio Eletrónico e Utilização Noutro Processo das Mensagens Apreendidas, *in* Revista Portuguesa de Ciência Criminal, Vol. 29, n.º 1, 2019b, p. 69 e 70.
[197] Neste sentido, CORREIA (2014), p. 40.
[198] BRAVO, Rogério, Da Não Equiparação do Correio-electrónico ao Conceito Tradicional de Correspondência por Carta, *in* Revista Polícia e Justiça, Janeiro – Junho 2006 – III Série, n.º 7, Coimbra Editora, 2006, p. 3.

com a apreensão de um simples documento redigido num processador de texto, de cálculo ou até para apresentação de slides, que estejam armazenados num computador, concluindo que esses dados informáticos não gozam da proteção da correspondência tradicional, tenham sido ou não lidos pelo destinatário.

Concordamos com a tese defendida por Sónia Fidalgo[199], e mais recentemente, pelo Tribunal Constitucional[200]. O tribunal defende que, considerando os bens-jurídicos constitucionais, os direitos fundamentais aqui constantes, bem como a necessidade de estabelecer uma compreensão atualista da *tutela jusconstitucional* emanada pela CRP, não deve ser entendido qualquer distinção entre a apreensão de correio eletrónico lido ou não lido.

4.3.2- Conhecimento do Conteúdo

Ainda surge um outro problema relativamente às regras de execução existentes na própria ideologia exposta na apreensão de correspondência. Diz-nos o art. 179.º, n.º 3 do CPP que o juiz que autorizou a apreensão de correspondência deve ser o primeiro a ter conhecimento do conteúdo específico da apreensão. Como já referimos, é o próprio art. 17.º da Lei do Cibercrime que remete para as regras específicas do art. 179.º do CPP.

No entanto, ainda que exista esta remissão, bem como através da ideia do elemento gramatical tipificado no art. 17.º– o artigo refere que *o juiz pode ordenar ou autorizar a apreensão* –, surgem algumas dúvidas nesta aplicação, principalmente por não se acreditar que existe uma viabilidade prática no cumprimento deste conceito.

Rita Castanheira Neves[201], partindo da dificuldade do cumprimento do conceito em que o juiz será o primeiro a ler o correio eletrónico apreendido, especialmente no que diz respeito à imensidade de *e-mails* que poderão ser alvo de apreensão, parece admitir que, embora isso represente a situação ideal, por vezes, os órgãos de polícia criminal poderão apreender os *e-mails* que se revelem determinantes para a produção da prova. Um dos métodos que pode ser utilizado, será o do OPC proceder a uma pré-seleção dos *e-mails*, usando técnicas de pesquisa, nomeadamente através de palavras-chave no

[199] FIDALGO (2019b), p. 69 e 70.
[200] Acórdão do TC n.º 687/2021.
[201] NEVES, Rita Castanheira, As Ingerências nas Comunicações Electrónicas em Processo Penal, Coimbra Editora, 2011, p. 275.

próprio sistema do *e-mail*, escolher um determinado período de datas ou até selecionar os *e-mails* provenientes de um certo remetente[202].

Benjamin Rodrigues[203], considerando a apreensão massiva de *e-mails* que têm de ser lidos primeiramente pelo juiz, mostra que em termos sistémicos, não é viável o cumprimento deste conceito. Para fundamentar a sua ideia, ainda estipula o regime que vigora no art. 189.º, n.º 1 do CPP – interceção em tempo real de correio eletrónico, em que aqui vigoram as regras das escutas telefónicas, aqui acrescentamos o próprio art. 18.º da Lei do Cibercrime –, em que as circunstâncias formais de apreensão nos processos que resultem numa intrusão mais gravosa aos direitos fundamentais do visado em comparação com a apreensão do correio eletrónico, os OPC's e o MP procedem à leitura e só depois efetuam uma seleção do material que consideram pertinente para o juiz ter conhecimento.

Seguimos a opinião de Sónia Fidalgo[204]. Pelos motivos aqui expostos, não podemos ignorar o problema aqui atinente, em que os e-mails ou registos de comunicações de natureza semelhantes apreendidos, o juiz que ordenou ou autorizou essa apreensão deverá ser o primeiro a ter conhecimento do conteúdo. O direito à privacidade e ao sigilo da correspondência eletrónica previstos nos artigos 26.º, n.º 1 e 34.º n.º 4 da CRP, não ignoram a remissão prevista no art. 17.º da Lei do Cibercrime, abrangendo assim também o exposto no art. 179.º n.º 3 do CPP. Assim, como foi confirmado pelo Tribunal Constitucional[205], o Juiz é o primeiro a ter conhecimento do conteúdo, exceto se existir uma justificação *cabal, robusta e bem determinada*, não podendo exceder os limites impostos por uma solução meramente excecional.

Pelo menos para nós, estes conflitos ficaram sanados com o acórdão do Tribunal Constitucional após um pedido de fiscalização preventivo por parte do Presidente da República[206].

[202] CONTARDO, Ricardo Wittler, Apreensão de Correio Eletrónico em Portugal: Presente e Futuro de Uma Questão de "Manifesta Simplicidade", *in* Novos Desafios da Prova Penal, Almedina, 2020, p. 284.
[203] RODRIGUES (2010), p. 454.
[204] FIDALGO (2019a), p. 158 e 159.
[205] Acórdão do TC n.º 687/2021.
[206] Abordado no capítulo 4.1.

4.4- Procedimentos a Adotar Após a Pesquisa

Por vezes, no seguimento do cumprimento da pesquisa de dados informáticos previsto no art. 15.º, poderá afigurar-se necessário apreender correio eletrónico suscetível de servir a prova do processo. Neste campo, como já aqui encaminhamos, o art. 17.º torna-se especialmente relevante. No entanto, até que ponto podemos garantir a eficácia prática de aplicação destas regras específicas, principalmente tendo em conta que existem várias especificidades que alteram o cerne da questão.

Imagine-se que no decorrer de uma busca informática legítima, sem qualquer autorização da autoridade judiciária competente, torna-se pertinente a apreensão de correio eletrónico, nomeadamente nas situações em que existe o consentimento por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado, bem como nos 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.

Aqui, principalmente nos casos expostos na segunda hipótese, a pertinência da leitura de algum *e-mail* ou qualquer comunicação de natureza semelhante, poderá ser a resposta investigatória que poderá resultar no resgate de um cidadão ou até mesmo vários, nomeadamente nas situações de raptos, tráfico humano ou até mesmo atos terroristas.

Nestes casos, a lei devia clarificar o regime que vigora, em que muito embora essa diligência deva ser comunicada imediatamente à autoridade judiciária competente, nos termos do art. 15.º, n.º 4, não parece viável o aguardar pela decisão do juiz para proceder à apreensão e posterior leitura, nos termos do art.º 17.º conjugado com o art. 179.º do CPP.

Nesse sentido, acreditamos que dada a natureza cautelar e urgente que vigora nesse momento, podemos abordar o art. 252.º, n.º 2 do CPP, onde dispõe que *tratando-se de encomendas ou valores fechados susceptíveis de serem apreendidos, sempre que tiverem fundadas razões para crer que eles podem conter informações úteis à investigação de um crime ou conduzir à sua descoberta, e que podem perder-se em caso de demora, os órgãos de polícia criminal informam do facto, pelo meio mais rápido, o juiz, o qual pode autorizar a sua abertura imediata.*

O cerne da questão, é que o artigo suprarreferido apenas parece autorizar a abertura imediata quando se trate de *encomendas ou valores fechados*, deixando assim de parte a correspondência eletrónica, seja correio eletrónico ou qualquer comunicação de

natureza semelhante. Ademais, em termos de praticidade, aparenta que a finalidade desta medida cautelar não é garantir que não ocorra uma ofensa à integridade física ou até mesmo à vida, mas sim apenas um meio de obtenção de prova de um crime que já foi cometido[207]. Ainda assim, a epígrafe do artigo em estudo dispõe *apreensão de correspondência*. Como aqui já abordamos, correspondência, inclui, também, o correio eletrónico, devendo assim ser enquadrado a apreensão e a abertura imediata desse tipo de correspondência, em causa de urgência, isto é, quando existam informações úteis à investigação que poderão ser extraviadas em caso de demora. Neste sentido, já existe jurisprudência que admite esta possibilidade[208].

Em boa verdade, assim sendo, no decurso de uma pesquisa de dados informáticos, se o despacho não tiver sido emitido por um juiz, e a apreensão de correio eletrónico se revelar de um grau de necessidade elevado para a descoberta da verdade material, o OPC deverá solicitar o pedido de apreensão a um juiz, em que este poderá autorizar. Para acautelar este risco de perturbação de recolha de prova, no âmbito das diligências de investigação, o OPC que coadjuvar o MP deverá verificar a necessidade de apreensão de correio eletrónico, e se existirem razões fundadas para a apreensão, o MP deverá requerer ao JIC a emissão do despacho de pesquisa de dados informáticos, ou seja, será a autoridade judiciária competente, nos termos do art. 15.º, e assim, fazer menção no despacho também da apreensão de correio eletrónico ou registos de comunicações de natureza semelhante, conjugando o artigo 15.º com o 17.º.

5- Conclusões

Ensina-nos Figueiredo Dias[209] que o verdadeiro fim do processo penal é a *descoberta da verdade* e a *realização da* justiça. Complementa que a última poderá bastar para justificar o fim do processo penal, considerando que a primeira faz parte integrante essencial desta última.

Assumimos, assim, vários problemas do foro sistemático e ético. Até esta fase, acreditamos que o entendimento é unânime no que concerne às próprias características imanentes presentes na recolha e valoração da prova eletrónico-digital, sendo necessário

[207] ALBUQUERQUE (2009), p. 669.
[208] Acórdão do TRL - Processo n.º 5412/08.9TDLSB-A.L1-5, de 11.01.2011.
[209] DIAS (2004), p. 43.

recorrer a vários conceitos amplos, definidores da própria essência humana, tendo em vista compatibilizar com as ideias presentes no próprio sistema de justiça.

Como já referimos, a Lei do Cibercrime regula, não só, um direito substantivo (estando previstos tipos legais de crime bem como suas consequências jurídicas), mas também o direito processual, servindo o princípio de *lex specialis derrogat legi generali*. Isto é, a propósito desta matéria a lei especial (Lei do Cibercrime) derroga a lei geral (CPP).

Assim, a par da grande maioria da doutrina, o legislador deveria ter inserido o direito substantivo no CP e o direito processual, no próprio CPP. A sua não inserção resulta em vários entendimentos contrários, confusos e, acima de tudo, dispersos.

Concluímos que o nosso CPP necessita de uma alteração substancialmente sistemática, tendo em vista compatibilizar e aprimorar uma melhor aplicação, evitando dissabores e entendimentos contrários, inserindo os meios de obtenção de prova previstos na Lei do Cibercrime, num capítulo adequado, uniformizando a legislação.

São vários os outros problemas que vigoram no sistema jurídico, especificamente no que concerne à Lei do Cibercrime. Num primeiro grupo, o consentimento previsto na pesquisa de dados informáticos, previsto no art. 15.º da Lei do Cibercrime, deveria pertencer apenas ao visado da pesquisa, e não a quem tem a disponibilidade ou controlo dos dados, devendo vigorar exatamente as mesmas regras que vigoram nas buscas domiciliárias, até porque, atualmente, os nossos sistemas informáticos representam uma extensão da nossa personalidade e privacidade, existindo uma certa analogia com o Direito Fundamental da inviolabilidade do domicilio e da correspondência previsto no art. 34.º da CRP. Ainda na pesquisa de dados informáticos, consideramos pertinente a adição de um novo pressuposto que permita o OPC proceder a uma pesquisa de dados informáticos sem autorização da autoridade judiciária, nomeadamente, quando exista flagrante delito de um tipo legal de crime que seja necessário proceder à pesquisa de dados informáticos para garantir a prova.

Relativamente ao Correio Eletrónico e de Registos de Natureza Semelhante previsto no art. 17.º da Lei do Cibercrime existem vários conflitos na doutrina, tendo já sido alvo de fiscalização preventiva por parte do Tribunal Constitucional, numa nova alteração que, de certa forma, restringia os direitos fundamentais dos cidadãos. O Tribunal Constitucional, considerou, a nosso ver de uma forma correta, que a apreensão do correio eletrónico ou registos de natureza semelhante deverá ocorrer com despacho judicial prévio, bem como o primeiro a tomar conhecimento do conteúdo deverá ser o juiz que

emitiu o despacho. Além disso, não existe qualquer distinção entre correio eletrónico lido ou não lido, devido ao simples facto da sua fácil manipulação, tanto por parte de quem necessita de apreender o correio eletrónico ou até mesmo do visado, considerando que com um simples *click*, pode ser alterado o estado de não lido para lido ou vice-versa. Exemplo são as teses defendidas pela jurisprudência e pela doutrina, na situação da correspondência eletrónica ou registos de natureza semelhante que possam já ter sido lidas ou não pelo destinatário, levando a caminhos opostos, consoante o caso em concreto. Essa diferença, simplesmente, não deve existir, pelos motivos já expostos, e por tantos outros que podem e devem assumir a natureza garantística que a nossa Lei Fundamental procura orientar.

Na alteração à Lei do Cibercrime, reiterando-se que a mesma demorou doze (12) anos a acontecer, o legislador podia e devia preocupar-se com outras situações relevantes. Aqui, podemos enumerar mais algumas alterações que deveriam ter sido efetuadas. Noutro ponto, de uma forma expressa, deveria existir uma maior preocupação tanto por parte do legislador como da doutrina, em reconhecer a existência dos conhecimentos fortuitos na pesquisa de dados informáticos, em que concordamos, que se todas as regras de valoração do meio de obtenção de prova que deu origem ao conhecimento fortuito forem cumpridas, também os conhecimentos fortuitos aí originados os devem ser, sendo iniciado um inquérito, como já refere a *Ley de Enjuiciamiento Criminal*.

Também a nova alteração deveria responder à questão da revelação coerciva da palavra-chave de acesso aos sistemas informáticos, em que a própria legislação não clarifica essa possibilidade, existindo opiniões distintas, em que uma admite a sua não obrigação, tendo em vista cumprir o princípio da não autoincriminação, previsto no art. 32.º, n.º 10 da Lei Fundamental. Ainda assim, considerando que não se trata de um princípio absoluto, deveriam ser clarificadas, em matéria legislativa, as situações em que esse direito é restringido.

As apreensões de correio eletrónico ou de registos de natureza semelhante no decurso de pesquisa de dados informáticos, quando ordenadas pelo MP ou cumpridas pelo OPC sem autorização da autoridade judiciária competente, não deverão ocorrer. Com o objetivo de acautelar a valoração da prova recolhida em sede de pesquisa de dados informáticos, o OPC deverá solicitar ao MP que promova ao juiz a emissão de despacho judicial prévio. Este permitirá a apreensão de correio eletrónico ou registos de natureza semelhante. Só dessa forma é que a recolha de prova poderá ser valorada em sede própria, após o juiz ser o primeiro a ter conhecimento do conteúdo dessa apreensão. Se assim o

achar determinante para a produção de prova ou de grande interesse para a descoberta da verdade, deverá juntar essa prova ao objeto do processo. De salientar que a descoberta da verdade é o fim essencial que o nosso Direito Processual Penal procura atingir.

Consideramos assim que, a Lei do Cibercrime pode e deve ser melhorada, atendendo à sua aplicação numa panóplia de situações diversas no Ciberespaço. Nomeadamente, deve ser inserida em local apropriado, concretamente no CPP, deve ser clarificada com o fim de resolver os conflitos jurídicos existentes e alterada nos aspetos considerados desadequados. Nesta senda, não pode ser ignorado que aquilo que for praticado ou auxiliado no mundo digital irá resultar em consequências no mundo físico ou real.

Bibliografia

- ABREU, Karen Cristina Kraemer, História e Usos da Internet. Disponível em: http://bocc.ufp.pt/pag/abreu-karen-historia-e-usos-da-internet.pdf. Acesso em: 10-02-2023.
- AGUILAR, Francisco, Dos Conhecimentos Fortuitos Obtidos Através de Escutas Telefónicas – Contributo para o seu Estudo nos Ordenamentos Jurídicos Alemão e Português, Almedina, 2004.
- ALBERGARIA, Pedro Soares de, in Comentário Judiciário do Código de Processo Penal, Almedina, 2021.
- ALBUQUERQUE, Paulo Pinto de, Comentário do Código de Processo Penal – à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Universidade Católica Editora, 2009.
- ALMEIDA, Ivo de, A Prova Digital, Librum Editora, 2018.
- ANDRADE, Manuel da Costa, Bruscamente no Verão Passado, a Reforma do Código de Processo Penal – Observações Críticas Sobre Uma Lei que Podia e Devia Ter Sido Diferente, Coimbra, Coimbra Editora, 2009.
- ANDRADE, Manuel da Costa, Sobre as Proibições de Prova em Processo Penal, Coimbra Editora, 1992.
- ANTUNES, Maria João, Direito Processual Penal, Almedina, 2016.
- BRAVO, Rogério, Da Não Equiparação do Correio-electrónico ao Conceito Tradicional de Correspondência por Carta, *in* Revista Polícia e Justiça, Janeiro – Junho 2006 – III Série, n.º 7, Coimbra Editora, 2006.
- CABRAL, José António Henriques dos Santos, Código de Processo Penal – Comentado, 4.º Edição, Almedina, 2022.
- CONTARDO, Ricardo Wittler, Apreensão de Correio Eletrónico em Portugal: Presente e Futuro de Uma Questão de "Manifesta Simplicidade", *in* Novos Desafios da Prova Penal, Almedina, 2020.
- COSTA, Eduardo Maia, Código de Processo Penal – Comentado, 4.º Edição, Almedina, 2022.
- CORREIA, João Conde, Prova Digital: as leis que temos e a lei que devíamos ter, in Revista do Ministério Público 139, julho:setembro, 2014.

- CORREIA, João Conde (2016, abril, 08). Prova Digital: Enquadramento legal *in* Prova em Direito Penal, Cibercriminalidade e Prova Digital. Centro de Estudos Judiciários, Lisboa. https://educast.fccn.pt/vod/clips/13vwtviahd/streaming.html?locale=pt.
- CORREIA, João Conde, *in* Comentário Judiciário do Código de Processo Penal, Almedina, 2021.
- DIAS, Jorge de Figueiredo, Direito Processual Penal, Clássicos Jurídicos, Coimbra Editora, Impressão 2004.
- DIAS, Jorge de Figueiredo, Direito Penal, Parte Geral, Tomo I, 3.ª Edição, Gestlegal, 2019.
- FIDALGO, Sónia, A Recolha de Prova em Suporte Eletrónico – Em Particular, A Apreensão de Correio Eletrónico *in* Julgar, n.º 38, 2019a.
- FIDALGO, Sónia, Apreensão de Correio Eletrónico e Utilização Noutro Processo das Mensagens Apreendidas, *in* Revista Portuguesa de Ciência Criminal, Vol. 29, n.º 1, 2019b.
- GODINHO, Inês Fernandes, Direito Processual Penal II - Sumários Desenvolvidos, Edições Universitárias Lusófonas, 2021.
- GONÇALVES, Fernando, A Prova do Crime, Meios Legais Para a Sua Obtenção, Almedina, 2009.
- GONÇALVES, João Gama, A Prova Digital em 2017 – Reflexões Sobre Algumas Insuficiências Processuais e Dificuldades da Investigação, CEDIS Working Papers, outubro 2017.
- MACHADO, João Baptista, Introdução ao Direito e ao Discurso Legitimador, Almedina, 2002.
- MESQUITA, Paulo Dá, Processo Penal, Prova e Sistema Judiciário, Coimbra Editora, 2010.
- MILHEIRO, Tiago Caiado, in Comentário Judiciário do Código de Processo Penal, Almedina, 2021.
- NEVES, Rita Castanheira, As Ingerências nas Comunicações Electrónicas em Processo Penal, Coimbra Editora, 2011.
- NOVAIS, Jorge Reis, Os Princípios Constitucionais Estruturantes da República Portuguesa, Coimbra Editora, 2004.
- NUNES, Duarte Alberto Rodrigues, O Problema da Admissibilidade dos Métodos "Ocultos" de Investigação Criminal Como Instrumento de Resposta À Criminalidade Organizada, Gestlegal, 2019.

- NUNES, Duarte Rodrigues, Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime, Gestlegal, 2021.
- PEREIRA, Rui Costa, A Pesquisa de Dados Informáticos – Exigências práticas do Princípio da Proporcionalidade, *in* Revista Portuguesa de Ciência Criminal, ano 31, n.º 3, Gestlegal, setembro – dezembro, 2021.
- RAMALHO, David Silva, Métodos Ocultos de Investigação Criminal em Ambiente Digital, Almedina, 2017.
- RAMOS, Armando Dias, Do *Periculum In Mora* da Atuação da Autoridade Judiciária ao *Fumus Boni Iuris* da Intervenção Policial *in* IV Congresso de Processo Penal, I Congresso Luso-Brasileiro de Criminalidade Económico-Financeira, coordenado por Manuel Monteiro Guedes Valente, Almedina, 2016.
- RAMOS, Armando Dias, O Agente Encoberto Digital - Meios Especiais e Técnicos de Investigação Criminal, Almedina, 2022.
- RAYÓN BALLESTEROS, Maria Concepción, Medidas de Investigación Tecnológica en el Proceso Penal: La Nueva Redacción de La Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015, *in* Anuario Jurídico y Económico Escurialense, LII, 2019.
- RIBOLI, Eduardo Bolsoni, A Utilização de Novas Tecnologias no Âmbito da Investigação Criminal e as Suas Limitações Legais: A Interceptação de Comunicações em Massa e os Softwares de Espionagem, *in* Galileu – Revista de Direito e Economia, Volume XIX, jul-dez, 2018.
- RODRIGUES, Benjamin Silva, Das Escutas Telefónicas à Obtenção da Prova [em ambiente] Digital, Tomo II, Coimbra Editora, 2009.
- RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo II – Bruscamente … A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal, Rei dos Livros, 2010.
- RODRIGUES, Benjamim Silva, Da Prova Penal, Tomo IV – Da Prova – Electrónico-Digital e da Criminalidade Informático- Digital, Rei dos Livros, 2011.
- RODRIGUES, Sara, O Dever de Fundamentação das Decisões Proferidas pela Autoridade da Concorrência, *in* Julgar *Online*, 2014.
- SILVA, Germano Marques, Processo Penal, Vol. II, Verbo, 2008.
- VALENTE, Manuel Monteiro Guedes, Cadeia de Custódia da Prova, Almedina, 2021.
- VALENTE, Manuel Monteiro Guedes, Revistas e Buscas, Almedina, 2005.
- VENÂNCIO, Pedro Dias, Lei do Cibercrime Anotada e Comentada, Coimbra Editora, 2011.

- VERDELHO, Pedro, Apreensão de Correio Eletrónico em Processo Penal, *in* Revista do Ministério Público, ano 25, Out/Dez, 2004.
- VERDELHO, Pedro, A Nova Lei do Cibercrime, Revista de Direito Comparado Português e Brasileiro, Tomo LVIII, n.º 320, Scientia Ivridica, Universidade do Minho, Out-Dez 2009.

Jurisprudência

- Acórdão do TRL - Processo n.º 5412/08.9TDLSB-A.L1-5, de 11.01.2011.
- Acórdão do TRP - Processo n.º 1885/10.8PIPRT.P1, de 05.06.2013.
- Acórdão n.º 687/2021 do Tribunal Constitucional.
- Acórdão n.º 268/2022 do Tribunal Constitucional.
- Acórdão do Tribunal de Justiça da União Europeia, processo *Digital Rights Ireland Ltd e outros, C-293/12 e C-594/12,* de 08.04.2014.
- Acórdão do Tribunal de Justiça da União Europeia *Tele2,* de 21.12.2016.
- Acórdão do Tribunal de Justiça da União Europeia, processos C-793/19 e C-794/19, de 20.09.2022.