Universidade de Lisboa

Faculdade de Direito

As dificuldades na obtenção e valoração de prova digital no crime de pornografia de menores

Ana Margarida Santos Norte

Dissertação de Mestrado em Direito e Prática Jurídica

Especialidade em Direito Penal

Orientadora:

Professora Doutora Inês Ferreira Leite

Lisboa, 2022

Universidade de Lisboa

Faculdade de Direito

As dificuldades na obtenção e valoração de prova digital no crime de pornografia de menores

Ana Margarida Santos Norte

Dissertação de Mestrado em Direito e Prática Jurídica

Especialidade em Direito Penal

Orientadora:

Professora Doutora Inês Ferreira Leite

Lisboa, 2022

Aos meus pais por me terem apoiado sempre e proporcionado o melhor possível.

À minha avó pela força e presença constantes.

Ao Felipe pelo carinho e pela ajuda incansável na desmistificação da informática.

Aos meus amigos pelos bons conselhos e palavras de incentivo.

À Professora Doutora Inês Ferreira Leite pela orientação deste trabalho e por me ter incutido o gosto pelo Direito Penal.

Resumo:

A investigação criminal no crime de pornografia de menores enfrenta ainda hoje grandes dificuldades com a utilização da *internet*, isto porque as características da prova digital são muito vantajosas para os cibercriminosos, como o recurso à *DarkWeb*. Tendo em conta a rapidez da evolução tecnológica, impõe-se o reconhecimento das dificuldades na obtenção e valoração de prova digital neste tipo de criminalidade.

Como tal, no presente estudo, analisamos os regimes jurídicos do crime de pornografia de menores e da prova digital de modo que nos possamos pronunciar sobre as temáticas mais controversas na recolha de prova digital e refletir sobre as grandes dificuldades existentes atualmente na obtenção e valoração de prova digital no crime de pornografia menores. Por último, sugerimos algumas possíveis soluções no sentido de rever certas medidas desadequadas e de implementar meios de obtenção e valoração de prova digital mais eficientes, dando prevalência à urgência na necessidade da alteração do regime jurídico, uma vez que o combate desta criminalidade está dependente de uma eficaz investigação criminal, sob pena de continuarmos a ter crianças extremamente desprotegidas.

Palavras-chave:

Pornografia de menores – Prova digital – *DarkWeb* - Investigação criminal

Abstract:

Criminal investigation in crimes of child pornography to this day faces great struggles due to the increased prevalence of the *internet*, since the characteristics of digital proof are very advantageous to cibercriminals, such as the usage of the DarkWeb. Considering the speed at which technological advances happen, it is crucial to identify the difficulties in collecting and evaluating digital evidence of this type of crime.

As such, in this paper we shall analyze the legal frameworks of child pornography crimes and digital evidence so that we can comment on the most controversial themes in the collection of digital evidence in crimes of child pornography. Lastly, we suggest some of the possible solutions that aim to revert certain maladjusted measures and to implement more effective methods of collection and evaluation of digital proof, highlighting the urgency to alter the legal framework, given that combating this type of crime is dependant on an effective criminal investigation, under penalty of children continuing to be put at extreme risk.

Keywords:

Child pornography – Digital evidence – DarkWeb - Criminal procedure

Siglas e Abreviaturas

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CP – Código Penal

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

DL – Decreto-Lei

EUA – Estados Unidos da América

FBI – *Federal Bureau of Investigation*

INMLCF – Instituto Nacional de Medicina Legal e Ciências Forenses

IP – Internet Protocol

JIC – Juiz de Instrução

LCib – Lei do Cibercrime

LEC – *Ley de Enjuiciamiento Criminal*

MP – Ministério Público

NCMEC – *National Center for Missing & Exploited Children*

OPC – Órgão(s) de Polícia Criminal

P2P – peer-to-peer

PGR – Procuradoria-Geral da República

PJ – Polícia Judiciária

SIMP- Sistema de Informação do Ministério Público

SMS – *Short Message Service*

STJ – Supremo Tribunal de Justiça

StPO - *Strafprozeßordnung* (Código de Processo Penal Alemão)

TC – Tribunal Constitucional

TEDH – Tribunal Europeu dos Direitos Humanos

TJUE – Tribunal de Justiça da União Europeia

TRC – Tribunal da Relação de Coimbra

TRE – Tribunal da Relação de Évora

TRL – Tribunal da Relação de Lisboa

TRP – Tribunal da Relação do Porto

UE – União Europeia

VoIP – *Voice over Internet Protocol*

Índice

I. Introdução

O crime de pornografia de menores constitui um dos crimes mais hediondos que pode ser praticado. Infelizmente, a *internet* tem proporcionado o aumento desta criminalidade devido a todas as características vantajosas que apresenta para quem se dedica à disseminação de conteúdo pedopornográfico, pois facilita a comunicação rápida e praticamente anónima entre os sujeitos localizados em qualquer ponto do globo.

Reconhecendo que o recurso à *internet* se tornou num verdadeiro terreno fértil para a prática desta criminalidade, pretendemos com o presente estudo determinar quais as dificuldades na obtenção e valoração de prova digital no crime de pornografia de menores, cujas características impedem a realização de uma investigação criminal eficaz, de modo a refletir sobre possíveis soluções para esta grande problemática do nosso século.

Como tal, começamos por analisar o regime jurídico do crime de pornografia de menores, presente no artigo 176.º do CP, enunciando as questões mais relevantes, como quais as condutas práticas que constituem este crime, bem como qual o bem jurídico protegido. Com especial atenção, pronunciamo-nos sobre a representação realista de menor e a mera detenção e visualização para autoconsumo devido à controvérsia que as envolvem.

De seguida, passamos para a importante análise da prova digital, verificando quais as suas características e apreciando o seu regime jurídico. As leis aplicáveis à prova digital estão envoltas numa enorme contradição, pelo que apreciaremos a articulação das diferentes leis que lhe são aplicáveis. De igual modo, analisamos com algum detalhe os meios de obtenção de prova existentes na LCib, como diploma regulador da prova digital por excelência. Ao longo desta investigação, tomamos posição sobre as questões mais controversas relacionadas com cada um destes métodos de obtenção de prova, relacionando com a sua eficiência na recolha de prova digital no crime de pornografia de menores. Ademais, abordamos as especificidades da *DarkWeb* que têm a maior importância, atualmente, no entendimento do funcionamento da *internet* e de como as grandes redes de pornografia infantil operam, fugindo frequentemente à alçada das autoridades.

Após a investigação do regime do crime de pornografia de menores propriamente dito e do regime jurídico, características e implicâncias da utilização de prova digital, cabe enumerar as grandes dificuldades de obtenção e valoração de prova digital neste crime que, no nosso entender, correspondem aos problemas associados à identificação

dos agressores e da vítima e da sua idade, à ineficácia dos meios de obtenção de prova presente na LCib, especialmente face às especificidades da *DarkWeb*, à complexidade do recurso à *cloud* e, por fim, à controversa decisão do TC relativamente à conservação e transmissão de metadados. Estas dificuldades que identificamos são as principais e mais complicadas no âmbito da investigação criminal e de recolha de provas digital nestas matérias.

Por fim, apresentamos algumas soluções que entendemos que ajudam a dirimir muitas destas dificuldades de obtenção e valoração de prova digital que apontamos ao longo do estudo, ao mesmo tempo que damos a nossa opinião sobre as maiores falhas existentes nesta problemática nos dias de hoje.

II. Crime de pornografia de menores

1. O conceito de pornografia de menores

O crime de pornografia de menores, previsto no artigo 176.º do CP, foi introduzido no direito penal português com a reforma de 2007. Anteriormente, as condutas típicas deste crime encontravam-se estipuladas nos antigos artigos 171.º e 172.º, n.º 3 do CP – que consistiam, essencialmente, em "atuar sobre menor" ou "utilizar menor" em situações com cariz pornográfico – e estas condutas cominavam num crime de abuso sexual de crianças, e não de pornografia. Entretanto, autonomizou-se o tipo legal de crime de pornografia de menores, mas mantiveram-se as condutas já estipuladas antes de 2007 e acrescentaram-se outras, não se tratando verdadeiramente de uma nova incriminação.[1]

Assim, verificou-se uma notória evolução do conceito de pornografia de menores e da sua incriminação. As constantes alterações ao preceito resultam da transposição de diversas normas europeias que têm tentado, incessantemente ao longo dos anos, combater o fenómeno global que é a pornografia de menores, especialmente com a facilidade de divulgação de conteúdos que a *internet* veio introduzir ao combate desta criminalidade, tais como, a transposição da Diretiva n.º 2011/93/UE, do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil – que veio substituir a importante Decisão-Quadro n.º 2004/68/JAI do Conselho, de 22 de dezembro de 2003 -,[2] mas também a Convenção de Lanzarote e a Convenção sobre o Cibercrime. A referida Diretiva define, desde logo, como objetivo «a repressão dos autores dos crimes, a proteção das crianças vítimas dos crimes e a prevenção do fenómeno», prevalecendo o superior interesse da criança e a sua proteção como manifestação dos direitos das crianças contemplados nos demais instrumentos europeus, nomeadamente o artigo 34.º da Convenção das Nações Unidas sobre os Direitos da Criança.[3] Ademais, define o conceito de pornografia infantil, no artigo 2.º, alínea c), como os «i) materiais que representem visualmente crianças

[1] MARIA JOÃO ANTUNES e CLÁUDIA SANTOS, *Comentário Conimbricense do Código Penal, Tomo I, anotação ao artigo 176.º*, 2012, p. 878.
[2] Disponíveis em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32011L0093 e https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32004F0068&from=HU, respetivamente.
[3] Disponível em https://www.unicef.pt/media/2766/unicef_convenc-a-o_dos_direitos_da_crianca.pdf. Além disso, a Diretiva menciona o Protocolo Facultativo à Convenção das Nações Unidas de 2000 sobre os Direitos da Criança relativo à Venda de Crianças, Prostituição Infantil e Pornografia Infantil e a Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração Sexual e o Abuso Sexual de 2007.

envolvidas em comportamentos sexualmente explícitos, reais ou simulados, ou ii) representações dos órgãos sexuais de crianças para fins predominantemente sexuais, iii) materiais que representem visualmente uma pessoa que aparente ser uma criança envolvida num comportamento sexualmente explícito, real ou simulado, ou representações dos órgãos sexuais de uma pessoa que aparente ser uma criança, para fins predominantemente sexuais, ou iv) imagens realistas de crianças envolvidas em comportamentos sexualmente explícitos ou imagens realistas dos órgãos sexuais de crianças para fins predominantemente sexuais».[4] Por sua vez, o artigo 20.º, n.º 2 da Convenção de Lanzarote define como pornografia de menores «todo o material que represente visualmente uma criança envolvida em comportamentos sexualmente explícitos, reais ou simulados, ou qualquer representação dos órgãos sexuais de uma criança, com fins sexuais».[5] A Convenção sobre o Cibercrime, no seu artigo 9.º, n.º 2, define pornografia infantil como «qualquer material pornográfico que represente visualmente: a) Um menor envolvido num comportamento sexualmente explícito; b) Uma pessoa que aparente ser menor envolvida num comportamento sexualmente explícito; c) Imagens realísticas que representem um menor envolvido num comportamento sexualmente explícito» e esclarece no n.º 3 a relevante noção de que «para efeitos do n.º 2, a expressão "menor" inclui qualquer pessoa com idade inferior a 18 anos».[6]

Resultante de todos estes esforços de combate à pornografia de menores, o artigo 176.º do CP sofreu várias alterações e verifica-se que o conceito de pornografia foi ampliado, passando, em traços gerais, a ser constituído por representação realista de menor, no n.º 4, pela detenção e aquisição intencional, mediante sistema informático ou outro meio aos materiais referidos na alínea b) do n.º 1, no n.º 5, pelo espetáculo pornográfico, no n.º 6, condutas que analisaremos *infra*. Além disso, em 2020, foi adicionado o n.º 8, que define o material pornográfico como «todo o material que, com fins sexuais, represente menores envolvidos em comportamentos sexualmente explícitos, reais ou simulados, ou contenha qualquer representação dos seus órgãos sexuais ou de outra parte do seu corpo». No entanto, o artigo 176.º do CP não apresenta qualquer definição do conceito de pornografia de menores, tendo o legislador optado antes por

[4] Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32011L0093.
[5] Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração Sexual e os Abusos Sexuais, de 25 de outubro de 2007 (Convenção de Lanzarote), disponível em https://rm.coe.int/168046e1d8.
[6] Convenção sobre o Cibercrime, de 23.11.2001 (Convenção de Budapeste), disponível em https://rm.coe.int/16802fa428.

elencar todos as condutas associadas a este crime como «reflexo das políticas de neocriminalização no âmbito dos crimes contra a liberdade e autodeterminação sexual».[7]

2. Bem jurídico

Assim como o conceito de pornografia de menores evoluiu, também o do bem jurídico protegido. Felizmente, a ideia de que o bem jurídico tutelado nos crimes sexuais era a moral e os bons costumes está completamente ultrapassada, remetendo o CP, atualmente, para o bem jurídico liberdade e autodeterminação sexuais.[8] Contudo, a doutrina e a jurisprudência dividem-se quanto à questão do bem jurídico no crime de pornografia de menores, por se tratar, como vimos, de um preceito em constante mutação, contendo várias condutas típicas.

Alguns autores entendem que o bem jurídico tutelado é, de facto, a liberdade e autodeterminação sexuais dos menores, concordando com a sistemática do CP, mas não para todas as condutas típicas descritas na norma.[9] JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO sustentam que a criminalização das condutas que implicam uma *utilização direta de menores*, consagradas nas alíneas a) e b) do n.º 1 do artigo 176.º do CP, ainda tutelam o bem jurídico autodeterminação sexual dos menores. Porém, as condutas das alíneas c) e d) do n.º 1 que correspondem a uma *utilização indireta de menores*, uma vez que já não implicam a atuação ou a utilização de menores em material pornográfico, mas têm como objetivo punir condutas que contribuam para a proliferação de materiais pornográficos que envolvam menores, tais como, a produção ou o consumo, protegem apenas indiretamente a liberdade e autodeterminação sexuais de menores, existindo uma tutela antecipada do interesse superior da criança e do seu bem-estar físico e psíquico.[10]

---

[7] JOSÉ MOURAZ LOPES e TIAGO MILHEIRO, *Crimes Sexuais - Análise Substantiva e Processual*, 2021, p. 252.
[8] MARIA JOÃO ANTUNES, "Crimes contra a Liberdade e a Autodeterminação Sexual de Menores", *Revista Julgar*, n.º 12, 2010, pp. 154 e 155. De igual modo, COSTA ANDRADE, *Consentimento e Acordo em Direito Penal*, 1991, pp. 388 e 395.
[9] PAULO PINTO DE ALBUQUERQUE entende que «o bem jurídico protegido é, ainda que remotamente, a autodeterminação sexual do menor de 18 anos», *Comentário do código penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 2021, p. 762. O Acórdão do TRC de 11.11 2020, processo n.º 28/16.9PAACB.C1, relatora Elisa Sales, estabelece como bem jurídico tutelado a autodeterminação sexual dos menores, tendo em conta que «a pouca idade da vítima, pode, mesmo sem coação, prejudicar gravemente o livre desenvolvimento da sua personalidade», disponível em www.trc.pt.
[10] Cfr. JOSÉ MOURAZ LOPES e TIAGO MILHEIRO, *ob. cit.*, pp. 252-255.

Posição semelhante tem ANA PAULA RODRIGUES ao defender que a liberdade e autodeterminação sexual dos menores é tutelada, mas de uma forma indireta, nas alíneas c) e d) do n.º 1 do artigo 176.º do CP, tendo em conta que a *ratio* da norma é punir quem contribui para o «tráfico, exploração e comércio dos fluxos de conteúdos pornográficos envolvendo crianças», mas são estes comportamentos que atentam a violação da liberdade e autodeterminação sexual dos menores.[11]

De igual modo, MARIA JOÃO ANTUNES e CLÁUDIA SANTOS adotam a posição que sustenta que as alíneas a) e b) protegem o bem autodeterminação sexual dos menores, mas as alíneas c) e d) pretendem criminalizar o comércio de material pornográfico, acreditando que, nestes casos, existe já uma «tutela demasiado longínqua e indeterminada do livre desenvolvimento do menor».[12]

Outros autores defendem que o bem jurídico protegido no crime de pornografia de menores não é a liberdade e autodeterminação sexuais do menor, mas antes um bem jurídico supraindividual. Já em 1999, FIGUEIREDO DIAS, na antiga redação do artigo 172.º, n.º 3 do CP, como mencionado *supra*, particularmente na alínea d), referia que, quando está em causa a exibição ou cedência de material pornográfico envolvendo menores, tratava-se de um bem jurídico supraindividual diferente da liberdade e autodeterminação sexuais do menor.[13]

Por sua vez, ANA RITA ALFAIATE afirma que este bem jurídico supraindividual corresponde à proteção da infância e da juventude, previsto nos artigos 69.º e 70.º da CRP, não se podendo falar numa verdadeira liberdade sexual ou autodeterminação sexual, ainda que se tratem de menores até aos 18 anos de idade, partindo-se do pressuposto que o livre desenvolvimento da personalidade na esfera sexual deve ser protegido até esta idade, cabendo ao Estado assegurar esta proteção e justificando, por este motivo, as incriminações consagradas no artigo 176.º do CP. Quanto às condutas explanadas nas alíneas c) e d), entende a autora que a sua incriminação funda-se no perigo que

[11] ANA PAULA RODRIGUES, "Pornografia de menores: novos desafios na investigação e recolha de prova digital", Dossier Temático - Crimes contra a autodeterminação sexual e contra a liberdade sexual com vítimas menores de idade, *Revista do CEJ*, n.º 15, 1º semestre, 2011, p. 271.
[12] MARIA JOÃO ANTUNES e CLÁUDIA SANTOS, *ob. cit.*, p. 880. No mesmo sentido, MARIA JOÃO ANTUNES e SUSANA AIRES DE SOUSA, "Da relevância da identificação do bem jurídico protegido no crime de pornografia de menores", *Revista Portuguesa de Ciência Criminal*, Ano 29, N.º 2, Maio-Agosto 2019, pp. 253-256.
[13] FIGUEIREDO DIAS, *Comentário Conimbricense do Código Penal, Tomo I, anotação ao artigo 172º*, pp. 547 e 548.

representam para a infância e juventude, mediante a proliferação de materiais que «coisificam o menor e o reduzem a objeto sexual».[14]

Discordando que o bem jurídico se funda na norma constitucional da proteção da infância e da juventude, PEDRO SOARES ALBERGARIA e PEDRO MENDES LIMA recorrem antes à dignidade da pessoa humana, que decorre do artigo 1º da CRP, na sua dimensão supraindividual e objetiva, isto é, encarando a dignidade humana dos menores, no seu conjunto e não relativamente a um concreto menor, enquanto merecedores de tutela na sua esfera sexual.[15]

Para INÊS FERREIRA LEITE, desde logo, a distinção entre autodeterminação sexual e liberdade sexual não faz qualquer sentido, porque são conceitos intimamente relacionados, alegando que «a autodeterminação corresponde a uma das concretizações e manifestações da liberdade em sentido amplo» e que «sem autodeterminação não podemos falar na existência de verdadeira liberdade».[16] Ademais, considerar que o entendimento de que todo e qualquer ato sexual é prejudicial para o menor e que não tem discernimento para o consentimento, inclusive o menor de 14 anos, seria recusar-lhe o direito à liberdade sexual. Consequentemente, o mesmo raciocínio é aplicado ao crime de pornografia de menores, não se defendendo quer a liberdade sexual, quer a autodeterminação sexual como bem jurídico protegido, mas sim o livre desenvolvimento da personalidade do menor na esfera sexual, evitando quaisquer «influências negativas e perturbadoras».[17] [18]

---

[14] ANA RITA ALFAIATE, *A Relevância Penal da Sexualidade dos Menores*, 2009, pp. 90-115. No mesmo sentido, M. MIGUEZ GARCIA e J. M. CASTELA RIO ao afirmar que as condutas tipificadas no artigo 176.º, n.º 1 do CP pretendem proteger, mormente, a proteção da juventude, *Código Penal Anotado, Parte geral e especial com notas e comentários*, 2014, p. 731. No Direito Espanhol, que também prevê o direito constitucional de proteção da infância e da juventude, ÁLVARO E. CRESPO defende este direito como o bem jurídico tutelado no crime de pornografia infantil, "La pornografía infantil en el marco de los delitos informáticos y del llamado "derecho penal de las sociedades de riesgo". Cuestiones problemáticas", *Derecho Penal Online*, disponível em https://derechopenalonline.com/la-pornografia-infantil-en-el-marco-de-los-delitos-informaticos-y-del-llamado-derecho-penal-de-las-sociedades-de-riesgo-cuestiones-problematicas/.

[15] PEDRO SOARES ALBERGARIA e PEDRO MENDES LIMA, "O crime de detenção de pseudopornografia infantil - evolução ou involução?", *Revista Julgar*, n.º 12, 2010, p. 210.

[16] INÊS FERREIRA LEITE, *Pedofilia – Repercussões das Novas Formas de Criminalidade na Teoria Geral da Infração*, 2004, p. 27.

[17] *Id.*, pp. 36-37 e 48.

[18] Parecendo defender uma junção das várias posições, o Acórdão do STJ de 19.02.2020, processo n.º 4883/15.1TDLSB.L1.S1, relator Nuno Gonçalves, determina que o bem jurídico protegido é «um bem jurídico plurisubjetivo e coletivo que protege a indemnidade sexual, o bem-estar das crianças e adolescentes, a sua segurança formativa e a dignidade da infância no seu todo», ressalvando que tem ainda um âmbito de proteção da autodeterminação sexual do menor na sua esfera sexual, disponível em https://jurisprudencia.csm.org.pt.

Ainda outro entendimento parece ter sido adotado no Acórdão do STJ de 16.01.2020 ao estabelecer que o crime de pornografia de menores tem como escopo a punição do «ato de utilização do menor em filme ou fotografia, com perigo de disseminação do material pornográfico por um número (mais ou menos indiferenciado) de pessoas», e que, embora ainda pretenda proteger a autodeterminação sexual do menor, «primariamente, este tipo legal de crime protege a exploração sexual do menor», tanto nas situações em que o menor é utilizado, como nas situações em que haja divulgação de materiais pornográficos envolvendo o menor e, por isso, o bem jurídico em causa corresponde a um «bem jurídico coletivo de proibição e disseminação deste material, proteção esta antecipada pela simples utilização do menor, ainda que o material não tenha sido disseminado».[19]

Todas estas posições aqui enunciadas demonstram a mudança de paradigma em relação à teoria do bem jurídico proclamada por ROXIN, que se traduz, essencialmente, na função exclusiva do direito penal de proteção subsidiária de bens jurídico-penais, cujos bens «corresponderão a todas as condições e finalidades necessárias ao livre desenvolvimento do indivíduo, à realização dos seus direitos fundamentais e ao funcionamento de um sistema estatal construído em torno dessa finalidade».[20] Sempre que não estejam em causa comportamentos que ofendam estes bens jurídicos, não é legítima qualquer incriminação.[21] Todavia, na sociedade atual, caracterizada pelos fenómenos da globalização e da tecnologia – a chamada "sociedade de risco" -, a verdade é que defender apenas a tutela dos bens jurídicos clássicos, como a vida ou o património, já não aparenta ser suficiente, por se tratar de conceitos extremamente limitados e antropocêntricos face aos novos riscos que vão surgindo, pelo que se fala numa crise do direito penal do bem jurídico e na necessidade de adotar uma nova política criminal.[22]

Recentemente, perante esta crise, ROXIN voltou a defender a sua teoria, clarificando que, apesar das diferentes opiniões quanto à definição do bem jurídico, existe

---

[19] Acórdão do STJ de 16.01.2020, processo n.º 283/17.7JDLSB.L1.S1, relatora Helena Moniz, disponível em https://jurisprudencia.csm.org.pt.

[20] ROXIN, "O conceito de bem jurídico como padrão crítico da norma penal posto à prova", *Revista Portuguesa de Ciência Criminal*, Ano 23, N.º 1, 2013, p. 12.

[21] ROXIN explica no seu Código anotado que assim é por se entender que o direito penal resulta na maior ingerência possível do Estado na liberdade de um indivíduo, sendo necessário que este só intervenha nos casos graves que são determinados pela noção de bem jurídico, decorrência do princípio da proporcionalidade presente na Constituição e, por isso, se não existir qualquer bem jurídico a tutelar, não é lícita a incriminação de uma conduta que não se verifique ofensiva, *Derecho penal. Parte general*, 1997, pp. 52-60.

[22] Cfr. FIGUEIREDO DIAS, *Direito Penal, Parte Geral, Tomo I, Questões Fundamentais, A Doutrina Geral do Crime*, 2019, pp. 153-156.

uma complementaridade entre a teoria do bem jurídico e as exigências jurídico-constitucionais, estando o legislador vinculado ao princípio da proporcionalidade como ponto de referência.[23] Parece ser este o entendimento do TC, como se pode retirar do Acórdão n.º 867/2021, a propósito da incriminação dos maus tratos a animais de companhia, no qual se concluiu pela inconstitucionalidade da norma devido à ausência de bem jurídico, sob pena da violação do artigo 18.º, n.º 2 da CRP.[24]

De facto, estamos de acordo com a insuficiência da teoria do bem jurídico, na sua visão puramente tradicional, tendo em conta que o direito penal não pode ficar simplesmente estagnado em relação à evolução da sociedade e ao surgimento de novos riscos, logo uma posição que defenda apenas a tutela dos bens jurídicos clássicos está completamente obsoleta numa sociedade globalizada e tecnológica. A figura do bem jurídico não pode mais ser enquadrada num ponto de vista individual e antropocêntrico, sendo necessário referirmo-nos a bens jurídicos coletivos ou supraindividuais, desde que constitucionalmente protegidos. É para nós evidente que o crime de pornografia de menores, graças à evolução da tecnologia, passou a tratar-se de um problema global.

Posto isto, entendemos que o bem jurídico em causa não pode ser somente a liberdade sexual ou a autodeterminação sexual porque, à medida que o artigo 176.º foi evoluindo e foram sido acrescentadas as várias condutas típicas, mais parece que a pretensão do legislador aponta para um bem jurídico amplo, mesmo que o CP não tenha alterado a sua sistemática. Portanto, partilhamos aqui a posição de INÊS FERREIRA LEITE quando afirma que a diferenciação entre autodeterminação sexual e liberdade sexual é uma redundância, sendo que a primeira é uma decorrência da segunda, e que afirmar que o menor deve ser protegido de todos os atos sexuais não tem qualquer cabimento, negando-lhe qualquer liberdade de escolha no plano sexual. Assim, acreditamos que esta incriminação não protege a liberdade ou autodeterminação sexuais dos menores, mas antes um bem jurídico supraindividual que, não pondo em causa a capacidade de discernimento e de consentimento do menor, o proteja de condutas que o afetem negativamente durante o seu crescimento e o desenvolvimento do exercício da sua liberdade sexual de forma saudável.

[23] Cfr. ROXIN, "O conceito de bem jurídico como padrão crítico da norma penal posto à prova", pp. 35 e 36.
[24] Acórdão do TC n.º 867/2021, de 10.11.2021, processo n.º 867/19, relator Lino Rodrigues Ribeiro, disponível em www.tribunalconstitucional.pt.

Concluímos então que o bem jurídico supraindividual tutelado, com o devido respeito pelas demais opiniões, só pode ser o livre desenvolvimento da personalidade do menor na sua esfera sexual no crime de pornografia de menores, plasmado no artigo 176.º do CP.

3. Tipo objetivo de ilícito

Como foi referido *supra*, o crime de pornografia de menores tem sofrido variadíssimas alterações na sequência da tentativa de travar este tipo de criminalidade, alterações essas que cabe aqui analisar.

Relativamente ao agente e à vítima do crime, o agente corresponde, naturalmente, a qualquer sujeito com idade igual ou superior a 16 anos, de acordo com o artigo 19.º do CP, enquanto que a vítima é qualquer menor de 18 anos, independentemente de ter experiência sexual ou não.[25] Assim, a idade da vítima só releva para efeitos de agravação da pena, nos termos dos n.º 6 e 7 do artigo 176.º do CP, sendo que a pena é agravada de um terço, nos seus limites mínimo e máximo, se se tratar de um menor de 16 anos e agravada de metade, de igual forma, se tiver menos de 14 anos. Igualmente importante é a relação entre autor e vítima do crime, uma vez que também a pena se agrava de um terço, nos seus limites mínimo e máximo, nas situações de parentalidade ou de aproveitamento da situação de relação familiar ou de habitação, enunciadas nas alíneas a) e b) do n.º 1 do artigo 177.º, bem como quando o crime é cometido conjuntamente por duas ou mais pessoas, como prevê o n.º 4.[26] Além disso, o agente do crime de pornografia de menores pode, ainda, ser uma pessoa coletiva ou entidade equiparada, nos termos do n.º 2 do artigo 11.º do CP.

Especificamente quanto às modalidades de ação, a denominada *utilização direta dos menores* encontra-se plasmada nas alíneas a) e b) do n.º 1 do artigo 176.º, traduzindo-

[25] MARIA DO CARMO SARAIVA DE MENEZES DA SILVA DIAS ressalva, e bem, que não é só autor do crime quem pratica as condutas descritas no artigo 176.º, mas também quem as financia, referindo que se trata de autoria por indução à prática do crime, "Notas Substantivas sobre Crimes contra a Liberdade e Autodeterminação Sexual", *Revista do Ministério Público*, n.º 136, 2013, p. 92. De forma semelhante, INÊS FERREIRA LEITE, ainda quando o crime de pornografia de menores se encontrava plasmado no artigo 172.º do CP, afirmava que «os responsáveis pelo crime de pedopornografia serão todos aqueles que estejam envolvidos na produção do material pornográfico: os que filmam, mas também os que procedem à montagem dos filmes, à sua colocação no mercado e distribuição», *Pedofilia*, p. 82.

[26] Cfr. M. MIGUEZ GARCIA e J. M. CASTELA RIO, *ob. cit.*, p. 732 e MARIA JOÃO ANTUNES e SUSANA AIRES DE SOUSA, *ob. cit.*, p. 243.

se essencialmente na utilização propriamente dita do menor ou do seu aliciamento em espetáculo pornográfico e em fotografia, filme ou gravação pornográficos, sendo o legislador claro quando afirma expressamente que não interessa o suporte do conteúdo pornográfico para que se verifique o tipo objetivo de ilícito. PAULO PINTO DE ALBUQUERQUE designa que estes atos podem envolver «a prática pelo menor de atos sexuais de relevo, atos de contacto de natureza sexual, atos exibicionistas ou apenas a presença física no meio dos outros intervenientes no espetáculo, não bastando que o menor seja mero espetador do evento», enquanto que o aliciamento de menor, no crime de pornografia de menores, constitui um ato de execução do tipo objetivo, ao abrigo da alínea c) do n.º 2 do artigo 22.º do CP, convertido em elemento típico, concluindo que se trata de uma antecipação significativa da tutela, na qual se pune um ato de execução como se pune o crime consumado.[27] O aliciamento de menor define-se, segundo ANA PAULA RODRIGUES, como «qualquer ação de sedução, no sentido de induzir, atrair a criança a comportamentos de cariz sexual, por meio de conversas e outras condutas (ex. prometer presentes, dinheiro, fama) através da *internet* e outros meios de comunicação à distância, de modo a abarcar o agressor que começa por aliciar na mira de convencer o menor a intervir efetivamente».[28]

Por seu turno, as alíneas c) e d) do n.º 1 do artigo 176.º do CP consagram a *utilização indireta dos menores*, cujas condutas são diversas: produzir, distribuir, importar, exportar, divulgar, exibir, ceder ou disponibilizar os materiais descritos na alínea b), a qualquer título ou por qualquer meio, e adquirir, deter ou alojar esses mesmos materiais com o objetivo de os distribuir, importar, exportar, divulgar, exibir ou ceder. Ora, PAULO PINTO DE ALBUQUERQUE esclarece, novamente, que a produção e a

[27] PAULO PINTO DE ALBUQUERQUE, *Comentário do código penal*, pp. 762 e 763. No mesmo sentido, M. MIGUEZ GARCIA E J. M. CASTELA RIO, *ob. cit.*, p. 732.
A este propósito, não esquecemos a introdução do crime de aliciamento de menores para fins sexuais no artigo 176.º-A do CP, aquando da alteração legislativa em 2015, que visa punir a conduta do agente, maior de idade, que alicia menor para encontro, mediante tecnologias de informação e comunicação, para a prática dos atos descritos nos n.º 1 e 2 do artigo 171.º e das alíneas a), b) e c) do n.º 1 do artigo 176.º. Como determina ANDRÉ LAMAS LEITE, neste artigo parece estar-se perante uma «fase intermédia entre o aliciamento e o encontro do maior com o menor com intenção de cariz sexual», devendo recorrer-se ao conceito de tentativa do artigo 22.º para se «preencher o segmento normativo que temporalmente medeia entre o aliciamento e o efeito encontro», nem sendo sequer «condição objetiva de punibilidade do tipo legal de crime», "As alterações de 2015 ao Código Penal em matéria de crimes contra a liberdade e autodeterminação sexuais - Nótulas esparsas", *Revista Julgar*, n.º 28, 2016, p. 71. Ainda, este artigo abrange o fenómeno do *child grooming* que, nas palavras de JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO, ocorre quando «o agressor sexual estabelece uma ligação emocional com o menor, visando ganhar a sua confiança para propor formas de exploração sexual, quer através da *internet* ou outros meios de comunicação», *ob. cit.*, p. 282.
[28] ANA PAULA RODRIGUES, *ob. cit.*, p. 268.

distribuição dos materiais pornográficos referem-se a todos os comportamentos desde a criação do material em causa até à sua proliferação para os demais indivíduos que não pertençam à cadeia de produção, a importação e a exportação corresponde ao transporte do material, a divulgação e a exibição são os atos de publicar ou mostrar a indivíduos não envolvidos na cadeia de produção e, por fim, a cedência e a disponibilização deste material traduz-se nos atos de vender, alugar, doar ou emprestar gratuitamente ou onerosamente.[29] Por sua vez, JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO defendem que a conduta de disponibilização poderia ser subsumida pelas condutas de quem distribui, exporta, divulga ou cede, tendo em conta que todas estas implicam a própria disponibilização do material pornográfico ao consumidor final, mas que a intenção do legislador foi criminalizar a proliferação deste material por qualquer meio possível, que atualmente inclui, naturalmente, todos os meios de divulgação de conteúdo pela *internet*.[30]

Por sua vez, a conduta do n.º 4 do artigo 176.º do CP remete para a figura da representação realista de menor que, devido às suas particularidades enquanto modalidade de ação, será analisada autonomamente de seguida.

As condutas descritas nos n.º 5 e 6 do artigo 176.º do CP têm como elemento típico a utilização de sistema informático.[31] O n.º 5 ocorre quando o agente adquire, detém, acede, obtém ou facilita o acesso, de forma intencional, através de sistema informático ou qualquer outro meio, os materiais da alínea b) do n.º 1, sendo este punido com pena

---

[29] Cfr. PAULO PINTO DE ALBUQUERQUE, *Comentário do código penal*, p. 763.

[30] Cfr. JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO, *ob. cit.*, pp. 255-257. Ademais, os autores destacam, assim como PAULO PINTO DE ALBUQUERQUE, os programas de partilha de ficheiros, especialmente o P2P, como um dos meios principais de proliferação de material pedopornográfico, bem como um dos grandes obstáculos à obtenção de prova no crime de pornografia de menores, sendo a sua utilização para divulgar este material bastante para se verificar o preenchimento do tipo objetivo de ilícito, *Comentário do código penal,* p. 763. O sistema P2P funciona com base na ideia de vários pontos comunicarem entre si de forma igualitária, não existindo a noção de estrutura centralizada e de servidores, Conselho da Europa, *Eletronic Evidence Guide - A basic guide for police officers, prosecutors and judges*, 2013, pp. 108 e 188, disponível em https://rm.coe.int/16803028af.
Nesta senda, parece-nos ainda que M. MIGUEZ GARCIA e J. M. CASTELA vão longe demais quando afirmam que as alíneas c) e d) pretendem tutelar os interesses do Estado que ficariam lesados com a proliferação da pornografia de menores, porque, ainda que realmente não se trate de uma lesão direta do bem jurídico, nunca se pode falar aqui da lesão dos interesses do Estado, mas sim dos menores utilizados em materiais pornográficos e o papel do Estado deve ser a proteção destes menores, evitando a perpetuação desta indústria, mediante a criminalização de condutas que divulguem estes materiais, *ob. cit.*, p. 734..

[31] A definição de sistema informático encontra-se consagrada na alínea a) do artigo 2.º da LCib: «qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aqueles ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção».

de prisão até 2 anos. Já no n.º 6, o agente, que é maior, assiste, facilita ou disponibiliza o acesso a espetáculo pornográfico envolvendo a participação de menores presencialmente ou através de sistema informático ou outro qualquer meio, sendo punido com pena de prisão até 3 anos.[32] Nestas duas modalidades de ação, pretende-se punir qualquer conduta que difunda material pornográfico envolvendo menores, realçando a utilização dos meios informáticos, uma vez que a *internet* propicia, com bastante facilidade, a proliferação de pornografia, tendo como base a ideia de que tanto é punido quem assiste, como quem permite que outros assistam a este tipo de conteúdo.[33] Esta ideia encontra-se de modo bastante evidente no Acórdão do TRP de 07.06.2017 ao indicar que integra o crime de pornografia de menores, pelo n.º 6, «o recebimento e guarda de fotos de jovem de 14 anos de várias partes do seu corpo sem vestuário enviadas pela própria a terceiro através do *Facebook*, e que as reenviou a outrem que as recebeu e visualizou».[34] Adiante, falaremos detalhadamente da mera detenção ou visionamento de material pedopornográfico para autoconsumo.

De seguida, cabe verificar quais as *circunstâncias qualificativas* do crime de pornografia de menores, como consequência das abundantes alterações legislativas que este crime tem sofrido. Desde logo, o n.º 2 do artigo 176.º do CP estabelece que a *intenção lucrativa ou prática profissional* das condutas previstas no n.º 1 não tem como consequência a agravação da pena, presente no regime do artigo 177.º do CP, mas sim a qualificação do crime, isto é, o limite máximo da pena de prisão não é de 5 anos, mas sim de 8 anos. Esta mesma ideia está consagrada no n.º 7 relativamente aos atos dos n.º 5 e 6 do artigo 176.º, sendo o agente punido com pena de prisão até 5 anos e não até 2 e 3 anos, respetivamente. Esta qualificação justifica-se pela necessidade de punir com maior gravidade quem vive da produção de material pornográfico envolvendo menores.[35]

---

[32] A definição de espetáculo pornográfico é a da alínea e) do artigo 2.º da Diretiva n.º 2011/93/UE: «a exibição ao vivo, destinada a um público, inclusive com recurso às tecnologias da informação e da comunicação, de: i) crianças envolvidas em comportamentos sexualmente explícitos, reais ou simulados, ou ii) órgãos sexuais de crianças para fins predominantemente sexuais», disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32011L0093&from=MT.

[33] Cfr. JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO, *ob. cit.*, p. 264. Ainda, ANDRÉ LAMAS LEITE entende que os n.º 5 e 6, por remeterem para outro ramos de Direito extrapenais, devem ser consideradas como «leis em branco», *ob. cit.*, p. 69.

[34] Acórdão do TRP de 07.06.2017, processo n.º 481/14.5JABRG.P1, relator Cravo Roxo, disponível em www.dgsi.pt.

[35] ANA PAULA RODRIGUES explica que o *animus lucrandi*, enquanto elemento do tipo, é a circunstância que qualifica as condutas descritas, *ob. cit.*, p. 271.

Igualmente, o n.º 3 representa uma circunstância qualificativa em relação às alíneas a) e b) do n.º 1 quando o agente, para tal, utilizar "violência ou ameaça grave", sendo punido com pena de prisão de 1 a 8 anos, em vez da pena de prisão de 1 a 5 anos. Segundo ANDRÉ LAMAS LEITE, estes conceitos devem ser entendidos de acordo com o que se encontra descrito no capítulo V, título I do livro II do CP, isto é, «a violência consiste no emprego de força, não apenas física, mas também psicológica e/ou moral, de tal modo que se possa afirmar existir uma imputação objetiva entre o emprego dessa mesma *vis* e o resultado ilícito projetado» e «a ameaça grave consiste em toda a promessa, pelo agente, de inflição de um mal futuro (independentemente de o mesmo se vir ou não a concretizar), a qual seja, pela própria natureza dos bens jurídicos que visa atingir, apta a cercear a liberdade de vontade do ofendido, de modo a que este pratique a ação ou omita, em função do que é pretendido pelo delinquente».[36]

No crime de pornografia de menores, a tentativa é punível, ao abrigo do n.º 9 do artigo 176.º do CP, decorrência da transposição do artigo 4º da Decisão-Quadro n.º 2004/68/JAI do Conselho, de 22 de dezembro de 2003, que designa que os Estados-Membros devem tomar as devidas medidas para garantir que a tentativa é punível quando está em causa, nomeadamente, a prática de produção ou distribuição, divulgação ou transmissão de pornografia infantil. Discordamos da opinião de PAULO PINTO DE ALBUQUERQUE que encara a tentativa de aliciamento de menor como uma tentativa de tentativa, pelo que não deve ser punível, defendendo o autor uma interpretação restritiva conforme a Constituição, de forma a evitar uma punição desproporcional e excessiva.[37]

---

[36] ANDRÉ LAMAS LEITE, *ob. cit.*, p. 68. Esta conduta integra o fenómeno de *sextortion*, uma das mais proeminentes formas de cibercriminalidade dos últimos anos. JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO descrevem *sextortion* como a situação em que «a vítima é coagida, "chantageada", pressionada, em virtude de posição de poder do agressor, ou ameaça de utilização de imagens de nudez, atos ou relações sexuais da vítima, que o agressor tem em sua posse», *ob. cit.*, p. 258. No Acórdão do STJ de 19.02.2020, processo n.º 4883/15.1TDLSB.L1.S1, relator Nuno Gonçalves, define-se *sexting* como «o primeiro passo, a fase preliminar e preparatória daquilo que, em regra geral, o agente criminoso adulto tem em mente: - ganhar a confiança da/o/as/os menor/es aliciada/o/s a fim de obter desta/e/s conteúdos pornográficos com atos sexuais explícitos e, seguidamente, concertar encontros para obter deles concessões de índole sexual», disponível em https://jurisprudencia.csm.org.pt.
A incidência do fenómeno da *sextortion* tem aumentado nos últimos anos globalmente. O FBI publicitou que até ao dia 31 de julho de 2021 recebeu 16.000 queixas de *sextortion*, correspondendo este número a dois terços das queixas de todo o ano de 2020 (informação retirada do site de notícias sobre cibersegurança *The Record*, disponível em https://therecord.media/fbi-americans-lost-more-than-8-million-to-sextortion-scams-this-year/). Em Portugal, a APAV dá conta de 134 denúncias de *sextortion* no seu relatório estatístico da Linha Internet Segura atinente ao ano 2021, disponível em https://internetsegura.pt/sites/default/files/2022-02/Estatisticas_APAV_LinhaInternetSegura_2021.pdf.
[37] Cfr. PAULO PINTO DE ALBUQUERQUE, *Comentário do código penal*, p. 764.

Posto isto, apenas referir que este é um crime de natureza pública. Em relação ao tipo de crime quanto ao grau de lesão do bem jurídico e quanto à conduta, tanto a doutrina como a jurisprudência identificam-no como crime de perigo abstrato, quanto ao grau de lesão do bem jurídico, e como crime de mera atividade, quanto à conduta.[38] MARIA JOÃO ANTUNES e CLÁUDIA SANTOS explicam que se trata de um crime de perigo porque basta a colocação em perigo do bem jurídico para se verificar o tipo objetivo de ilícito, e de perigo abstrato porque o perigo não é elemento do tipo.[39] ANDRÉ LAMAS LEITE aprofunda a questão, clarificando que o crime de pornografia de menores nas modalidades típicas dos n.º 1 a 3 do artigo 176.º do CP constitui um crime de perigo abstrato, tendo em conta que «o legislador considera as suas formas típicas tão gravosas para a autodeterminação sexual dos menores que só essas ações tipicamente cunhadas representam um potencial irremível de perigo para o bem jurídico», e um crime de mera atividade, visto que «a sua consumação opera com a utilização ou o aliciamento de menor em espetáculos de teor sexual ou com a sua utilização ou aliciamento para constarem de suportes fotográficos ou de outro tipo, independentemente de um resultado externo-objetivo».[40] Nas modalidades típicas dos n.º 5 e 6 trata-se igualmente de um crime de perigo abstrato, quanto à lesão do bem jurídico, e de mera atividade, quanto à consumação do ataque ao objeto da ação, mas por diferentes razões, que se traduzem, essencialmente, na tentativa de «"secar" todas as fontes que possam contribuir, direta ou indiretamente, para a existência de pornografia de menores, em linha com a legislação da União Europeia neste domínio».[41]

[38] Com mais detalhe, PAULO PINTO DE ALBUQUERQUE, *Comentário do código penal*, p. 762.
[39] MARIA JOÃO ANTUNES e CLÁUDIA SANTOS, *ob. cit.*, p. 880. Já o Acórdão do TC n.º 426/91, de 06.11.1991, processo n.º 183/90, relator José de Sousa e Brito, se havia pronunciado sobre o significado de crime de perigo abstrato, afirmando que o legislador não exige a efetiva lesão dos bens jurídicos tutelados para se verificar a sua consumação, ou seja, «não pressupõe nem o dano nem o perigo de um dos concretos bens jurídicos protegidos pela incriminação, mas apenas a perigosidade da ação para as espécies de bens jurídicos, abstraindo de algumas das outras circunstâncias necessárias para causar um perigo para um desses bens jurídicos», disponível em www.tribunalconstitucional.pt. Ilustrativo deste entendimento, o mais recente Acórdão TRE de 17.03.2015, processo n.º 524/13.0JDLSB.E1, relator Carlos Jorge Berguete, demonstra que a intenção do legislador é a tutela antecipada do bem jurídico protegido, disponível em www.dgsi.pt.
[40] ANDRÉ LAMAS LEITE, *ob. cit.*, p. 69. Em termos gerais, estamos perante um crime de mera atividade quando o tipo incriminador se preenche mediante a mera realização da conduta, independentemente da verificação ou não de um resultado, como ensina FIGUEIREDO DIAS, *ob. cit.*, p. 356.
[41] ANDRÉ LAMAS LEITE, *ob. cit.*, p. 70.

3.1. O consentimento do menor

A propósito das condutas típicas analisadas, é relevante pronunciarmo-nos brevemente sobre a questão da validade do consentimento do menor, tendo em conta que o n.º 3 do artigo 38.º do CP estabelece que o consentimento só é eficaz se for prestado por quem tiver mais de 16 anos de idade e se possuir discernimento para avaliar o seu sentido e alcance. Portanto, sendo as vítimas do crime de pornografia todos os menores de 18 anos, é necessário compreender se o seu consentimento é relevante ou não e se varia consoante a idade.

Ora, a lei parte do pressuposto que o consentimento do menor com idade inferior a 16 anos de idade é irrelevante, isto é, não possui capacidade para se autodeterminar sexualmente.[42] O Acórdão do STJ de 22.01.2013 justifica esta escolha do legislador: «o princípio que fundamenta a menoridade sexual não é qualquer suposição de que o jovem abaixo da idade definida legalmente não tenha desejo ou prazer sexual, mas, sim, que ele não desenvolveu ainda as competências consideradas relevantes para consentir em uma relação sexual. Só o tempo, por meio de um processo de socialização no qual o sujeito racional completo é (con)formado permitem a modelação de um processo de decisão corretamente elaborado».[43]

Para quem assim o entende, como ANA RITA ALFAIATE, numa situação em que o agente utilize o menor em material pornográfico, desde que se trate de menor com idade mínima de 16 anos, que dá o seu consentimento e que reúna as condições mencionadas, exclui-se a ilicitude da conduta do agente, com exceção das condutas de *utilização indireta* de menor, cuja visão já não é tão linear, visto que «o legislador baseou a incriminação destas condutas no perigo de perigo para a infância e juventude de proliferarem materiais que coisificam o menor e o reduzem a objeto sexual».[44] Inclusive, JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO entendem que o consentimento do menor com idade entre os 16 e os 18 anos, no âmbito da sua intimidade, em tirar fotografias ou fazer filmagens com cariz sexual exclui igualmente a ilicitude da conduta, só passando a relevar criminalmente se esse material for divulgado a terceiros

[42] Com um entendimento ainda mais conservador, MARIA DO CARMO SARAIVA DE MENEZES DA SILVA defende que o consentimento de menores com 16 anos de idade e que possuem discernimento é indiferente no caso da alínea a) do n.º 1 do artigo 176.º do CP, entendimento que nos parece ir mais além da intenção do legislador, *ob. cit.*, p. 92.
[43] Acórdão do STJ de 22.01.2013, processo n.º 182/10.3TAVPV.L1.S1, relator Santos Cabral, disponível em www.dgsi.pt.
[44] ANA RITA ALFAIATE, *ob. cit.*, p. 115.

sem o dito consentimento.[45] Com a mesma opinião, PEDRO SOARES ALBERGARIA e PEDRO MENDES LIMA fundamentam que «ser reduzido a objeto de satisfação sexual não é necessariamente o mesmo que ser coisificado, bem podendo ser um ato voluntário e assim um normal exercício da liberdade»,[46] visão com a qual concordamos totalmente.

Relativamente ao significado de consentimento válido, INÊS FERREIRA LEITE explica que este corresponde a «um verdadeiro e espontâneo acordo para a prática de atos sexuais».[47] Porém, esse acordo pode ser formalmente prestado, mas mediante um abuso ou aproveitamento, designadamente, através de intimidação, convencimento ou aproveitamento de falta de compreensão da conduta ou de opor resistência com menores de 14 anos, sendo que pode ser aproveitamento de posição de autoridade, de relação hierárquica ou de relação de dependência, entre outros. Em nenhum destes casos existe um verdadeiro consentimento ou acordo, logo não apresenta relevância jurídica.

Todavia, a verdade é que a evolução da tecnologia veio agravar a situação, permitindo uma maior facilidade de aproximação entre os menores e os seus agressores pelo que existe «a necessidade de conciliar a compreensão de crianças e jovens como sujeitos especiais, ou seja, necessitados de proteção e socialização, com o princípio de que são, também, indivíduos portadores de direitos».[48] Esta conciliação está longe de ser fácil e consensual. Nesta senda, o legislador parece fazer uma espécie de graduação de idades consoante o discernimento que entende que estes menores têm para consentir, ou seja, realiza a clara distinção entre os menores com menos de 14 anos de idade, os menores com idades compreendidas entre os 14 e os 16 anos de idade e, por último, os menores de 18 anos de idade, conclusão que retiramos do artigo 177.º do CP que vai agravando as penas quanto mais baixa for a idade do menor em causa. Porém, de forma geral, tendemos a ir no sentido do Acórdão do TRE de 21.09.2021 quando determina que «os limites da idade são meramente indicadores, isto porque não poderemos dizer, ao certo, quando é que o menor atinge o discernimento necessário ou a maturidade sexual exigida para a prática de tais atos».[49]

---

[45] Cfr. JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO, *ob. cit.*, p. 265.
[46] PEDRO SOARES ALBERGARIA e PEDRO MENDES LIMA, *ob. cit.*, p. 213.
[47] INÊS FERREIRA LEITE, "A tutela penal da liberdade sexual", *Revista Portuguesa de Ciência Criminal*, Ano 21, N.º 1, 2011, p. 76. A autora explica melhor que este acordo do menor é válido quando reúne três requisitos: a consciência do significado da conduta, a capacidade de avaliação da relevância do ato praticado e, por fim, a inexistência de elementos estranhos no processo de formação de vontade do menor, *Pedofilia*, p. 93.
[48] Novamente o Acórdão do STJ de 22.01.2013, processo n.º 182/10.3TAVPV.L1.S1, relator Santos Cabral, disponível em www.dgsi.pt.
[49] Acórdão do TRE de 21.09.2021, processo n.º 1144/17.5PBSTB.E1, relator Moreira das Neves, disponível em www.jurisprudência.pt.

Ainda assim, mesmo tendo defendido *supra* que o menor não deve ser protegido de todo e qualquer contacto sexual, sob pena de se estar a violar o seu direito ao normal desenvolvimento da sexualidade, não deixamos de constatar a possibilidade do aliciamento a enviar fotografias ou a participar noutro conteúdo sexual poder conduzir à potencial violação desse normal desenvolvimento, isto é, será que, só por si, poderão estas condutas configurar uma perturbação ao exercício saudável da vida sexual do menor ainda que este consinta? Qual parece ser a solução mais acertada? A nosso ver, é preciso atender ao caso concreto, tanto quanto às condutas praticadas, como à capacidade de discernimento do menor em causa para as praticar. Ora, revemo-nos na opinião de que um menor entre os 14 e os 18 anos de idade que consinta com discernimento, apurado no caso concreto, para tirar fotos ou vídeos com caráter sexual, desde que o faça no âmbito da sua intimidade, esse consentimento é válido e deve excluir a ilicitude da conduta, sob pena de se punir constantemente sujeitos por exercerem a sua vida sexual livremente. Mas, a partir do momento em que esse conteúdo íntimo seja partilhado a terceiros, a conduta já é criminalizada. Como exemplifica ROXIN, e bem, não é coerente punir a conduta de um jovem de 18 anos de idade que possua uma foto íntima da sua namorada de 17 anos, com o consentimento desta, não se punindo as relações sexuais que têm entre eles.[50] Seguindo este entendimento, o Acórdão do TRP de 22.04.2020 decidiu não criminalizar, segundo a alínea b) do n.º 1 do artigo 176.º do CP, a conduta do agente que solicitou a menor de 16 anos o envio de fotos desnudada, no contexto de uma relação de namoro, e tendo em conta que não as cedeu ou divulgou, afirmando que «se a uma adolescente com essa idade é atribuída, para efeitos penais, capacidade para avaliar os seus atos e se determinar de acordo com essa avaliação e lhe é conferida a faculdade de contrair casamento» são obrigados a concluir que o envio deste conteúdo «se inscreve no âmbito da autonomia da vontade que nessa idade já lhe é reconhecida», apesar da «"ressonância" na opinião pública».[51]

Contudo, apesar da avaliação no caso concreto nos parecer a solução mais acertada, admitimos que abaixo de uma certa idade será cada vez mais difícil que a conclusão seja que o menor possui discernimento para consentir, por ser bastante natural que não consiga reconhecer o impacto negativo que a sua participação em material pornográfico ou somente o seu aliciamento pode ter no livre desenvolvimento da sua

[50] Cfr. ROXIN, "O conceito de bem jurídico como padrão crítico da norma penal posto à prova", p. 19.
[51] Acórdão do TRP de 22.04.2020, processo n.º 573/18.1JAAVR.P1, relator José Piedade, disponível em www.dgsi.pt.

sexualidade e, muito menos, as consequências desse conteúdo para o qual consentiram ser largamente difundido e armazenado permanentemente na *internet*.

Portanto, é preciso muita cautela na apreciação da validade do consentimento prestado pelo menor, contrabalançando o discernimento para entender o alcance e sentido no caso concreto e o seu normal desenvolvimento da personalidade na esfera sexual, sem que este seja restringido em prol de conceções moralistas.

3.2. Representação realista de menor

Como foi supramencionado, o n.º 4 do artigo 176.º do CP remete para a representação realista de menor, isto é, incrimina a conduta do agente que praticar os atos previstos nas alíneas c) e d) do n.º 1 utilizando material pornográfico com representação realista de menor, sendo punido com pena de prisão até dois anos. Esta figura levanta diversas questões na doutrina e na jurisprudência, pelo que a analisaremos aqui autonomamente.

Esta incriminação resulta da transposição da Decisão-Quadro n.º 2004/68/JAI, de 22 de dezembro de 2003, na qual se considera que é material pornográfico o que descreve ou representa visualmente «pessoas reais com aspeto de crianças» e «imagens realistas de crianças não existentes» envolvidas em «comportamentos sexualmente explícitos ou entregando-se a tais comportamentos, incluindo a exibição lasciva dos seus órgãos genitais ou partes púbicas» e, assim, estamos perante pornografia infantil. Porém, os Estados-Membros não estão vinculados a transpor, tal qual, para o respetivo direito interno, podendo isentar de responsabilidade criminal os comportamentos associados à pornografia infantil quando a pessoa real com aspeto de criança possuir 18 anos ou mais ou, no caso de produção e posse de imagens de crianças que tenham atingido a maioridade, estas tenham o seu consentimento e seja unicamente para autoconsumo ou, ainda, se o produtor produzir e possuir o material pornográfico apenas para uso pessoal.[52]

Assim sendo, discute-se que tipo de condutas integram a representação realista de menor, começando pela distinção entre *pedopornografia aparente* e *pedopornografia virtual*. PEDRO SOARES ALBERGARIA e PEDRO MENDES LIMA definem *pedopornografia aparente* como «produção pornográfica com participação de adultos

[52] Cfr. artigos 1.º e 2.º da Decisão-Quadro 2004/68/JAI, de 22 de dezembro de 2003, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32004F0068&from=HU.

que pelos traços físicos ou caracterização aparentam ser menores» e *pedopornografia virtual* como «produções pornográficas em que os supostos menores participantes ou são uma pura criação de tecnologia gráfica (designadamente informática – imagens de geração computacional) ou o são pelo menos em parte (neste caso juntam imagens ou parte de imagens de menores – por exemplo colhidas de fotos de publicidade ou de outros suportes – com criações de técnica gráfica; o chamado *morphing*)».[53] Por sua vez, ainda existe a distinção entre *pedopornografia virtual total* e *pedopornografia virtual parcial* que MARIA JOÃO ANTUNES e CLÁUDIA SANTOS descrevem como «aquela que é puro fruto da tecnologia gráfica e da imaginação do seu autor» e «aquela que, embora fruto da tecnologia gráfica e da imaginação do autor, resultam, em parte, de imagens ou parte de imagens de menores de 18 anos de idade», respetivamente.[54]

Por um lado, existem autores que acreditam que a representação realista de menor inclui as duas modalidades de pedopornografia mencionadas. PAULO PINTO DE ALBUQUERQUE defende que a representação realista de menor «inclui não apenas a ficção integral ou parcial da imagem de um menor, como a utilização de pessoa real com aspeto de menor, com vista a criar a impressão no consumidor do material que se representa um menor».[55] De igual modo, ANA PAULA RODRIGUES entende que a representação realista de menor inclui a representação de pessoa maior que aparenta ser uma criança e as representações de crianças criadas, por exemplo, através do computador ou numa banda desenhada.[56] Também JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO com o fundamento de que a lei não exclui nenhuma das condutas, «delimitando a abrangência incriminatória pela aptidão do material pornográfico retratar imagens que aparentam de forma realista serem menores de idade».[57]

Para INÊS FERREIRA LEITE, é preciso ter muita cautela com a definição de "realista", uma vez que apenas pode incluir a «utilização de maiores com aparência de menores e a pornografia virtual que seja apta a convencer um observador médio (tendo em conta que o destinatário que se pretender proteger é o menor, e não o adulto consumidor de pedopornografia) que pode tratar-se de um verdadeiro menor».[58]

[53] PEDRO SOARES ALBERGARIA e PEDRO MENDES LIMA, *ob. cit.*, p. 214.
[54] MARIA JOÃO ANTUNES e CLÁUDIA SANTOS, *ob. cit.*, p. 884.
[55] PAULO PINTO DE ALBUQUERQUE, *Comentário do código penal*, p. 763.
[56] ANA PAULA RODRIGUES, *ob. cit.*, p. 272.
[57] JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO, *ob. cit.*, p. 261.
[58] INÊS FERREIRA LEITE, "A tutela penal da liberdade sexual", p. 59.

Por outro lado, existem autores que apenas consideram a *pedopornografia virtual*. MARIA JOÃO ANTUNES e CLÁUDIA SANTOS excluem a *pedopornografia virtual total* e só incluem a *pedopornografia virtual parcial* como representação realista de menor.[59] Também ANA RITA ALFAIATE considera apenas estar em causa a *pedopornografia virtual*, defendendo que o entendimento que se deve dar à representação realista de menor no nosso ordenamento jurídico é da representação visual de imagens realistas de crianças não existentes.[60]

Entendemos que a razão se encontra com os autores que defendem que a representação realista de menor abrange a *pedopornografia virtual* e *pedopornografia aparente*, tendo em conta que o legislador português parece ter decidido transpor para as definições presentes na referida Decisão-Quadro para o nosso ordenamento jurídico.

Efetivamente, a criminalização da representação realista de menor não é, de todo, consensual, inclusive noutros ordenamentos jurídicos, sendo que as principais reservas são especialmente a falta de dignidade jurídico-penal e a carência de bem jurídico e a colisão com o direito à liberdade de criação artística. De facto, nos EUA a discussão é prévia à Decisão-Quadro europeia, tendo-se decidido no famoso caso *Ashcroft, Attorney General, et. al. v. Free Speech Coalition et. al.* de 16.04.2002 pela inconstitucionalidade da criminalização da pedopornografia virtual que, segundo o *Child Pornography Prevention Act* de 1996, se caracteriza por "*any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture"* que *"is, or appears to be, of a minor engaging in sexually explicit conduct"* ou que *"conveys the impression of a minor engaging in sexually explicit conduct"*, com base na limitação da liberdade de expressão (*"free speech"*), prevista na Primeira Emenda da Constituição Americana.[61] Em sentido oposto, o caso *R. v. Sharpe* de 26.01.2001, decorrido no Canadá, determinou que deve criminalizar-se todo o material pornográfico que envolva menores, mesmo aquele que apenas apresente meras representações, por se entender que o papel da legislador nesta matéria é contrariar qualquer tipo de conduta que tenda a normalizar a prática de relações sexuais entre adultos e crianças, isto porque *"the use of child pornography to "groom" or seduce victims, showed a rational connection"*.[62]

---

[59] *Id.*
[60] ANA RITA ALFAIATE, *ob. cit.*, pp. 120 e 121.
[61] Acórdão *Ashcroft, Attorney General, et. al. v. Free Speech Coalition et. al.* do Supreme Court of the United States de 16.04.2002, disponível em https://www.law.cornell.edu/supct/pdf/00-795P.ZS.
[62] Acórdão *R. v. Sharpe* do Supreme Court of Canada de 21.01.2001, disponível em https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1837/index.do.

Na Europa, devido à adoção da mencionada Decisão-Quadro, observa-se uma tendência da criminalização da pornografia virtual, nomeadamente em Itália, na Alemanha e em França.[63] Pese embora a tendência no sentido da criminalização, continuam a existir vozes bastante críticas como a de GIOVANNI COCCO que alega que a punição da pornografia infantil virtual e aparente é completamente arbitrária, uma vez que não estão envolvidas crianças "de carne e osso" (*"minori in carne ed ossa"*) no processo de produção, não existindo uma verdadeira lesão do bem jurídico em causa nem das próprias crianças. Além disso, não vê a lógica de afirmar que a pornografia infantil virtual e aparente conduz a comportamentos desviantes, quando os seus consumidores são os pedófilos habituais, logo esta incriminação corresponde a uma mera censura moral, constituindo uma tutela penal demasiado ampla.[64] De modo semelhante, ÁLVARO CRESPO entende que a criminalização da representação realista de menor representaria uma injustificada expansão do direito penal, bem como uma violação do princípio da mínima intervenção do Estado, visto que a censura moral só se torna relevante quando a conduta em causa resulta numa lesão objetiva de um bem jurídico e, aqui, como não estão presentes verdadeiras crianças, não ocorre essa lesão.[65]

No panorama nacional, existem muitas vozes que se manifestam claramente contra esta criminalização. MARIA JOÃO ANTUNES critica a opção neocriminalizadora do legislador português que vai, no seu entender, além da intervenção mínima do Estado, observando que, para satisfazer os compromissos a nível europeu e internacional, tem-se criado uma «tendência atual de um direito penal do bem jurídico que é, afinal, permeável a criminalizações alheias ao critério da dignidade jurídico-penal e da carência (necessidade) de tutela do bem jurídico, servindo mesmo opções não propriamente político-criminais, mas antes apenas "político-criminalmente corretas"».[66] Segundo esta autora, esta incriminação não é legítima por falta de dignidade jurídico-penal e de tutela do bem jurídico, por já não se estar a proteger nem a liberdade sexual nem a autodeterminação sexual, nunca podendo permitir-se que o critério seja o da

[63] Detalhadamente, ANA RITA ALFAIATE que elenca os artigos 600-quater 1 do Código Penal italiano e o artigo 227-23 do Código Penal francês, bem como menciona o artigo 189.º do Código Penal espanhol que apenas pune a produção, venda, distribuição, exibição ou facilitação da existência de material pornográfico em que, não havendo utilização direta de menores, se utilize a sua voz ou imagem alterada ou modificada, *ob. cit.*, p. 122.

[64] GIOVANNI COCCO, "Può constituire reato la detenzione di pornografia minorile?", *Rivista Italiana di Diritto e procedura penale*, Anno XLIX, Fasc. 3 Luglio-Settembre, 2006, pp. 875-878.

[65] ÁLVARO CRESPO, *ob. cit.*, pp. 9 e 10.

[66] MARIA JOÃO ANTUNES, *ob. cit.*, pp. 155-158. Partilhando as mesmas reservas quanto à constitucionalidade material, ANDRÉ LAMAS LEITE, *ob. cit.*, p. 69.

moralidade ou dos bons costumes.[67] Concordando que esta ideia, VERA RAPOSO ao afirmar que a argumentação da Decisão-Quadro é insatisfatória quando não tutela a liberdade sexual, mas sim a imoralidade de possuir fantasias sexuais com crianças, o que não constitui uma efetiva lesão se não passar de isso mesmo, uma mera fantasia.[68] De igual modo, M. MIGUEZ GARCIA e J. M. CASTELA RIO dizem tratar-se de uma tutela ainda mais antecipada em relação aos crimes de perigo abstrato, chamando-lhe uma "tutela desmaterializada", não se podendo já reconduzir ao bem jurídico autodeterminação sexual.[69] Por seu turno, ANA RITA ALFAIATE sustenta que apenas a descriminalização desta conduta pode repor a tendência neocriminalizadora da moralidade nos crimes sexuais contra menores, devido à falta de dignidade penal e arbitrariedade do bem jurídico tutelado.[70] Bastante críticos, PEDRO SOARES DE ALBERGARIA e PEDRO MENDES LIMA insistem que esta incriminação é contraproducente, devendo as forças policiais aplicar o seu tempo e instrumentos na investigação de pornografia real que utiliza verdadeiros menores, em vez de gastar meios com a pedopornografia infantil.[71]

Além disso, trazendo à colação outro fundamento a favor da descriminalização da representação realista de menor, JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO referem a colisão com o direito à liberdade de criação artística, sendo este direito uma ramificação do direito à liberdade de expressão, previsto no artigo 37.º da CRP, isto porque a representação fantasiada do menor, ou seja, a criação de imagens de um menor numa qualquer relação sexual, – quer gerada por computador, quer ilustrada numa banda desenhada – ainda que possa ser considerada polémica não o afeta diretamente, não devendo restringir o direito à expressão artística do seu autor, logo estas imagens não podem «consubstanciar qualquer ilicitude e muito menos qualquer crime na medida em que se não individualizem muito concretamente quais os perigos que daí possam existir para o desenvolvimento das crianças».[72] Como vimos, o problema da colisão com o direito à liberdade de criação artística e de expressão foi um dos grandes argumentos para descriminalizar a pedopornografia virtual nos EUA.

---

[67] *Id.* Igualmente, MARIA JOÃO ANTUNES e CLÁUDIA SANTOS, *ob. cit.*, p. 884.
[68] VERA RAPOSO, "Da moralidade à liberdade: o bem jurídico tutelado na criminalidade sexual", 2003, p. 953.
[69] M. MIGUEZ GARCIA e J. M. CASTELA RIO, *Código Penal Anotado, Parte geral e especial com notas e comentários*, 2014, p. 735.
[70] ANA RITA ALFAIATE, *ob. cit.*, p. 121.
[71] PEDRO SOARES DE ALBERGARIA e PEDRO MENDES LIMA, *ob. cit.*, p. 216.
[72] JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO, *ob. cit.*, p. 260.

No entanto, existe quem seja favorável à criminalização da representação realista de menor. Adotando veemente este entendimento, PEDRO VAZ PATTO, pese embora o reconhecimento de que não se trata de verdadeiras crianças e que não existe uma efetiva lesão sobre estas, defende que o material pedopornográfico corresponde a um meio comum de aliciamento para a prática sexual, segundo a experiência das entidades policiais. Ademais, legitima a criminalização da pornografia infantil virtual, na medida em que a proliferação e o consumo deste tipo de material pornográfico facilita a prática de crimes sexuais contra crianças, até porque a evolução da tecnologia não só o permite, como permite ainda o aperfeiçoamento das representações realistas que se confundem com as imagens reais e, por isso, refuta a ideia de que o nexo de causalidade entre a proliferação e consumo deste material e a prática de crimes sexuais contra crianças é demasiado longínquo devido ao propósito intrínseco da pornografia em estimular sexualmente os seus consumidores, devendo tratar-se como qualquer outro crime de perigo abstrato. Nesta senda, nunca deverá o direito à liberdade de expressão e a consequente liberdade de criação artística sobrepor-se aos danos que este material provoca ou pode vir a provocar nas crianças a que ele estejam expostas.[73] No mesmo sentido, ÂNGELA PINTO argumenta que mesmo as meras representações realistas constituem «um perigo de incentivo de práticas abusivas, havendo o risco de provocarem fantasias, reforçarem convicções de que os atos sexuais com menores são aceitáveis e gerarem aceitação pelos próprios menores de que se trata de práticas normais, despertando ou encorajando-as (promovendo, assim, uma distorção cognitiva), para além da dificuldade que pode advir da evolução tecnológica em distinguir o que é uma imagem real e uma mera representação realista».[74]

Posto isto, cabe concluir pela incriminação ou não da representação realista de menor. Será que faz sentido? Como explica INÊS FERREIRA LEITE, a decisão do legislador português pela punição desta conduta não passa nem deve passar pela tutela de uma ideia de moralidade, mas antes devido ao papel da pedopornografia nos «processos causais de diminuição das resistências do menor face à prática abusiva de atos sexuais (*grooming*)», logo existe uma «perigosidade latente» na proliferação e consumo de material pornográfico em que se represente um menor porque normaliza e,

[73] PEDRO VAZ PATTO, "Pornografia Infantil Virtual", *Revista Julgar*, n.º 12, 2010, pp. 188-194. No mesmo sentido, ANA PAULA RODRIGUES, *ob. cit.*, pp. 271-273.
[74] PINTO, Ângela, "Crime de Abuso Sexual de Menores com Recurso à Internet – Enquadramento jurídico, prática e gestão processual", *Trabalhos Temáticos de Direito e Processo Penal*, Volume I, CEJ, 2016, pp. 113 e 114.

consequentemente, diminui a resistência de um determinado menor para a prática abusiva de atos sexuais – também considerando tratar-se de um crime de perigo abstrato -, mas isso não significa que se possa punir o «mero desejo sexual ou pensamento que envolva menores».[75] Ora, não nos parece fazer sentido a criminalização da *pedopornografia aparente* nem da *pedopornografia virtual total*, tendo em conta que não existe verdadeiramente um menor, nem a lesão de nenhum bem jurídico, desrespeitando os princípios constitucionais da proporcionalidade e da intervenção mínima do Estado. Assim já não o entendemos no que diz respeito à criminalização da *pedopornografia virtual parcial*, na medida em que ainda contém imagens ou parte de imagens de menores, ou seja, mesmo que seja fruto da tecnologia gráfica e da imaginação do autor, resulta, em parte, de imagens de menores reais, produto de uma efetiva lesão de um bem jurídico dos menores em causa. Aqui, não conseguimos conceber os argumentos da falta de dignidade penal por falta de bem jurídico, nem pela prevalência da liberdade artística.

Assim sendo, concluímos pela incriminação da *pedopornografia virtual parcial* por ser a única conduta que nos parece merecedora de tutela penal, existindo, a nosso ver, a lesão do bem jurídico livre desenvolvimento da personalidade do menor na esfera sexual.

3.3. Mera detenção ou visionamento para autoconsumo

A outra grande controvérsia atinente ao crime de pornografia de menores assenta na questão da criminalização da mera detenção ou visionamento de material pornográfico para autoconsumo. As normas que permitem punir estas condutas são os n.º 5 e 6 do artigo 176.º do CP, fruto da alteração realizada em 2015,[76] de forma a transpor as alíneas d) e f) do n.º 1 do artigo 20.º e 21.º da Convenção de Lanzarote que criminalizam a procura de pornografia de menores para si ou para terceiros, bem como quem acede a pornografia de menores, conscientemente, através das tecnologias de comunicação e de informação, assim como o n.º 4 do artigo 4.º da Diretiva n.º 2011/93/UE que, explicitamente, pune quem assiste a espetáculos pornográficos em tempo real envolvendo menores.[77]

[75] INÊS FERREIRA LEITE, "A tutela penal da liberdade sexual", pp. 57-59 e *Pedofilia,* pp. 63-65.
[76] Alteração do Código Penal pela Lei n.º 103/2015 de 24.09.2015, disponível em www.pgdlisboa.pt.
[77] Disponível em https://rm.coe.int/168046e1d8 e https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32011L0093.

Ora, antes desta alteração, era indubitável que o *download* de material pornográfico era punido, mas não era unânime quanto ao mero visionamento. Nessa altura, de facto, entendia-se, como dizia ANA PAULA RODRIGUES, que a lei pretendia punir a detenção ou posse e não o visionamento de material pornográfico disponível na *internet*, sendo punível sim o seu *download*.[78] MARIA DO CARMO SARAIVA DE MENEZES DA SILVA DIAS sustentava a necessidade de se verificar uma intenção por parte do agente para constituir crime, sendo que, se se tratasse de material para autoconsumo, o agente era punido apenas pela simples detenção.[79] Efetivamente que, somente criminalizando o *download,* os consumidores de pornografia infantil contornavam a lacuna presente na lei ao evitar a descarga desses ficheiros para os seus computadores, recorrendo antes às plataformas em que pudessem assistir a espetáculos ao vivo *online* ou *streaming*.[80] Simultaneamente, surgia o problema de quem não pretendia consumir material pedopornográfico, mas se deparava acidentalmente com ele, e cujo mero visionamento implicava uma descarga automática para o computador.[81] A introdução do advérbio "intencionalmente" no n.º 5 resultou da necessidade de se verificar a intenção do agente para que a conduta seja punível, resolvendo-se assim os casos acidentais de visionamento de material pedopornográfico, e a introdução dos outros verbos "aceder", "obter" ou "facilitar o acesso" em conjugação com a intenção do agente veio pôr término ao recurso dos consumidores às plataformas *streaming* de material pedopornográfico, punindo-se então mais do que o *download*.

Portanto, atualmente, pune-se tanto a mera detenção como o visionamento de material pornográfico envolvendo menores, ainda que não implique *download* ou a transferência de ficheiros provisórios, isto é, passou a punir-se o agente que acede a

[78] Cfr. ANA PAULA RODRIGUES, *ob. cit.*, p. 273.
[79] Cfr. MARIA DO CARMO SARAIVA DE MENEZES DA SILVA DIAS, *ob. cit.*, p. 93. ÂNGELA PINTO explica que concordava com esta opinião, anteriormente à alteração legislativa, porque a descarga automática para o disco do computador (os *temporary internet files*) opera mediante a consulta deste tipo de *sites* e permite a visualização dos ficheiros *online* por parte do agente quando este já não está ligado à rede e, por isso, se este agente tivesse conhecimento destes ficheiros, justificava-se a incriminação porque detinha conscientemente o material, *ob. cit.*, p. 115.
[80] Mesmo assim, até o *streaming* não é perfeito, uma vez que a sua visualização implica uma transmissão temporária de dados, que não ficam armazenados de forma permanente no computador, mas ficam temporariamente na *cache* do sistema, ao contrário da descarga de ficheiros *online*. No entanto, como explicam JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO, era a opção mais segura para os consumidores, na antiga redação do artigo, visto que "deter" significa um «domínio de facto sobre o material pornográfico que não coincide com a transitoriedade do *streaming*», *ob. cit.*, p. 262.
[81] M. MIGUEZ GARCIA e J. M. CASTELA sugerem que quem descarregar material pedopornográfico por engano deve proceder logo à sua eliminação do disco do computador, pois pode iniciar-se uma investigação penal que fica totalmente dependente da comprovação do dolo do agente, sendo a única base argumentativa para a sua defesa, *ob. cit.*, pp. 735 e 736.

material desta natureza, que facilita o seu acesso a terceiros e, ainda, que obtém este material para autoconsumo, não pretendendo uma contrapartida. No fundo, trata-se apenas de mais uma ampliação das condutas típicas que compõem o crime de pornografia de menores. Segundo PAULO PINTO DE ALBUQUERQUE, as condutas típicas desta incriminação incluem «a criação de *sites* pornográficos, a criação ou compilação de *hyperlinks* com *sites* pornográficos, a mera consulta temporária de uma página de *internet*, com ou sem pagamento do acesso, bem como o *download* de material pornográfico», «o acesso, a obtenção e a facilitação do acesso a materiais alojados fora da *internet*, como *pen-drives*, cartões de memória, DVD ou fotos digitais» e, ainda, a «disponibilização de acesso ao espetáculo pornográfico envolvendo a participação de menores».[82] Assim sendo, o verdadeiro *download* de ficheiros pornográficos não corresponde a uma conduta típica do n.º 5 do artigo 176.º do CP – que apenas pretende punir a mera detenção ou visionamento deste material sem que ocorra verdadeiramente um *download* - enquanto que o verdadeiro *download*, já antes considerado crime, é punido pela alínea c) do n.º 1 do artigo 176.º, sendo que "exportar" consiste na descarga de ficheiros para o computador ou *download* e "importar" ao seu inverso, o *upload*.

Na jurisprudência, já se manifestava a grande dificuldade em enquadrar os casos de mera detenção ou visionamento para autoconsumo na redação anterior do artigo, não existindo unanimidade, apenas criminalizando o *download*, ainda que se reconhecesse que a visualização em *streaming* e a detenção de material pornográfico não merecia menor censura penal.[83] Após a alteração legislativa, observa-se, então, um consenso quanto à incriminação do *download* pela alínea c) do n.º 1 do artigo 176.º e o mero detentor é punido pelo n.º 5 do artigo 176.º do CP. Ademais, o Acórdão do STJ de 17.05.2017 clarifica que o significado de *download* no âmbito da alínea c) consiste sempre na «receção num terminal informático de uma dada informação» - a mencionada descarga de ficheiros para o computador -, inclusive as situações em que a receção de conteúdo pedopornográfico tem origem noutro país, ainda enquadradas no significado de "importar", definindo que «o *download* constitui a forma pela qual o agente, num dado

[82] PAULO PINTO DE ALBUQUERQUE, *Comentário do código penal*, p. 764. Críticos desta opção legislativa, JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO entendem que o legislador português foi mais além do que era a pretensão da Convenção de Lanzarote, *ob. cit.*, p. 263.

[83] Como no Acórdão do TRE de 14.07.2020, processo n.º 649/19.8TELSB-A.E1, relator Renato Barroso, quando refere que o utilizador que «acedesse a um *site* com tais conteúdos e visualizasse um vídeo deste teor, sem o importar (*download*) para o seu computador (visualização em *streaming*), conduta esta que se considerou não merecer menos censura penal do que a de quem visualiza adquirindo previamente», disponível em www.dgsi.pt.

País, acede a um conteúdo».[84] Além disso, o Acórdão do TRE de 14.07.2020 esclarece que a alínea c) do n.º 1 do artigo 176.º pune a conduta de disseminação de ficheiros pornográficos a terceiro, bastando que a cedência ou divulgação ocorra somente com uma pessoa, distinguindo-se do n.º 5 do artigo 176.º cujo escopo é o agravamento da punibilidade das condutas de consumo de material pedopornográfico e da sua facilitação e não o desagravamento das condutas de «partilha, cedência ou distribuição de tal material entre produtores/utilizadores e utilizadores/utilizadores, o que, aliás, não fez».[85]

No direito europeu, tem-se observado a tendência da criminalização da mera detenção ou visionamento para autoconsumo. No direito espanhol, a mera detenção de material pornográfico infantil é considerada menos censurável penalmente em relação à sua difusão através da *internet* ou outra qualquer tecnologia de informação, tendo tido o legislador espanhol o brio de consagrar expressamente a possibilidade das autoridades judiciárias poderem adotar as medidas necessárias para a retirada dos conteúdos pedopornográficos, a interrupção dos serviços que oferecem predominantemente destes conteúdos ou o bloqueio de ambos quando o agente se encontrar no estrangeiro.[86] No direito francês, optou-se por criminalizar todo o material pedopornográfico que protagonize menores de 15 anos de idade, mesmo que sem o objetivo da sua divulgação e seja apenas para autoconsumo.[87] O direito italiano pune quem adquire ou detém material pornográfico conscientemente, bem como quem acede intencionalmente e sem motivo justificado, através da *internet* ou outro meio de comunicação, a material pedopornográfico, mas esta última conduta possui uma menor moldura penal.[88]

Relativamente à incriminação da mera detenção ou visionamento de material pornográfico para autoconsumo, existem variadíssimas visões na doutrina portuguesa. A favor da incriminação, JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO, exceto

---

[84] Acórdão do STJ de 17.05.2017, processo n.º 194/14.8TEL.SB.S1, relator Pires da Graça, disponível em www.dgsi.pt.

[85] Acórdão do TRE de 14.07.2020, processo n.º 649/19.8TELSB-A.E1, relator Renato Barroso, disponível em www.dgsi.pt. Este mesmo Acórdão trata ainda de uma questão bastante importante, que teremos oportunidade de densificar, relativamente à instalação de programas informáticos que permitem a partilha automática de ficheiros e a não deteção o endereço IP do agente, no caso, o programa TOR, que demonstram que, em conjugação com os materiais pedopornográficos encontrados na posse do arguido, era sua intenção não só o consumo deste conteúdo, como a sua partilha, pelo que esta conduta, nestes termos, é punível pela alínea d) do n.º 1 do artigo 176.º do CP, em vez do n.º 5 do mesmo artigo.

[86] Os artigos em causa são os artigo 189.º e 189.º bis. do Código Penal espanhol, disponível em www.boe.es. Uma escolha bastante curiosa do legislador espanhol foi a equiparação entre os casos de mera detenção para autoconsumo e o agente que contribuiu para a preparação do material pedopornográfico e que, para tal, utilizaram pessoas com deficiência com necessidades especiais de proteção como merecedores da mesma censura penal, previsto no n.º 5 do artigo 189.º.

[87] Artigo 227-3 do Código Penal francês, disponível em www.legifrance.gouv.fr.

[88] Artigo 600-quater do Código Penal italiano, disponível em www.altalex.com.

nos casos em que se verifique que o agente não tinha intenção de aceder a material pedopornográfico, mas esse comportamento resultou de «imperícia informática, desconhecimento informático, *links* que direcionam para *sites* pornográficos, reencaminhamentos não pretendidos na *internet*», ou, tendo intenção, a exceção são os casos em que se pretenda «obtenção de prova para um processo ou tem subjacente um estudo ou investigação científica».[89] No mesmo sentido, PEDRO SOARES DE ALBERGARIA e PEDRO MENDES LIMA afirmam que o legislador criou um crime de detenção pura como forma de tutela ainda mais antecipada do direito penal, isto é, não sendo necessário que se verifique qualquer resultado ou perigo para o bem jurídico, mas justifica-se a incriminação da mera detenção ou visionamento para autoconsumo pelo facto da simples posse de material pedopornográfico se traduzir na lesão da liberdade ou autodeterminação do menor – tendo em conta que a sua produção tem subjacente o aproveitamento ou o abuso de um determinado menor – e o constante visionamento dessa lesão leva a uma potencial perturbação psicológica e/ou relacional do menor.[90]

Em sentido contrário, ANA RITA ALFAIATE começa logo por dizer que a incriminação não faz qualquer sentido, referente à redação antiga do artigo, uma vez que a mera detenção de material pedopornográfico – por exemplo, a posse de uma fotografia pornográfica de um menor, dado pela autora - por parte do agente que não possui nenhuma intenção de a distribuir ou divulgar, não se reconduz numa lesão para o menor em concreto.[91] De modo semelhante, INÊS FERREIRA LEITE entende que esta incriminação não tem razão de ser: primeiro, porque não se deve assumir que os consumidores de pedopornografia são obrigatoriamente abusadores de menores e, segundo e mais importante, o único meio de ser favorável a esta incriminação é partindo do pressuposto que a dignidade do menor é afetada pela produção, cedência e consumo de material pedopornográfico, logo o bem jurídico aqui em causa não pode corresponder à liberdade ou autodeterminação sexual do menor e, por esse motivo, parece que punir a mera detenção ou visionamento para autoconsumo pretende, sim, a tutela da moral e dos

[89] JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO, *ob. cit.*, p. 263.
[90] Cfr. PEDRO SOARES DE ALBERGARIA e PEDRO MENDES LIMA, *ob. cit.*, pp. 197-198 e 208.
[91] Cfr. ANA RITA ALFAIATE, *ob. cit.*, pp. 119 e 120. É preciso ter em atenção que na antiga redação do artigo, ainda quando se tratava do n.º 4, não se punia o visionamento, apenas a detenção de material pedopornográfico e, é por esta razão, que a autora entende que não faz sentido punir-se a mera detenção, não se punindo o mero visionamento e já se tendo acautelado a criminalização da detenção com intenção de a distribuir ou divulgar, concluindo que a mera intenção de deter não constitui um perigo para a infância e a juventude. Expressamente contra esta opinião, PEDRO SOARES DE ALBERGARIA e PEDRO MENDES LIMA sustentavam, já na altura, que não era «absolutamente líquido que o mero visionamento de material pornográfico seja de todo isento de pena, sendo que a punição da tentativa abre caminho a que quem apenas visiona, ao menos quando o faça com intenção de adquirir», *ob. cit.*, p. 209.

bons costumes ou dos sentimentos gerais da sociedade, uma vez que não consegue reconhecer um bem jurídico claro que se pretenda proteger.[92] Contudo, a autora reconhece que, mesmo quando seja apenas mero consumo, está sempre inerente uma situação de aproveitamento de um ato de abuso sexual ou exploração sexual de um menor e pode considerar-se que a liberdade sexual do menor pode ser ainda mais lesada devido à «durabilidade do suporte pornográfico e a constância dos efeitos nefastos do momento de lesão ou de condicionamento da liberdade sexual do menor».[93] No entendimento de MARIA JOÃO ANTUNES e SUSANA AIRES DE SOUSA, a criminalização desta conduta, enquanto "crime de detenção" que não tutela diretamente um bem jurídico e é baseado numa «perigosidade abstrata», traduz-se numa expansão exagerada da intervenção penal e, por isso, não aceitável.[94]

Com o devido respeito, temos de concluir pela não criminalização da mera detenção ou visionamento de material pedopornográfico para autoconsumo, apenas devendo criminalizar a conduta de quem pretende divulgar esse conteúdo, contribuindo para a perpetuação do consumo deste conteúdo. Portanto, o agente que realiza o *download* deste material com intenção de o divulgar a terceiros é, certamente, punido pelo crime de pornografia de menores, bem como o agente que dá instruções ao abusador sexual, participando no abuso de forma indireta, nos casos de *streaming*. No fundo, entendemos ser necessário provar a conduta dolosa do agente, isto é, a intencionalidade na difusão de material pedopornográfico, porque, só com essa intenção, se verifica uma efetiva lesão do bem jurídico. Isto não significa que não consideramos o mero consumo deste conteúdo uma conduta puramente censurável, mas a verdade é que não são os consumidores que lesam o bem jurídico tutelado e, se não divulgarem o conteúdo, estão a aproveitar-se de uma situação de abuso que já foi praticada, devendo antes ser punidos os abusadores sexuais e os membros da cadeia de produção e distribuição de material pedopornográfico.[95]

[92] INÊS FERREIRA LEITE, *Pedofilia*, pp. 60-65.
[93] INÊS FERREIRA LEITE, "A tutela penal da liberdade sexual", p. 57.
[94] MARIA JOÃO ANTUNES e SUSANA AIRES DE SOUSA, *ob. cit.*, p. 247.
[95] Revemo-nos aqui na afirmação de INÊS FERREIRA LEITE quando determina que não pretende defender que o consumo de pedopornografia deve ser tratado como um direito absoluto, mas simplesmente não consegue reconduzir a incriminação a um verdadeiro bem jurídico, *Pedofilia*, p. 65.

4. Tipo subjetivo

Relativamente ao tipo subjetivo, o crime de pornografia de menores é um crime doloso, quer seja por dolo direto, necessário ou eventual, de acordo com as modalidades prevista no artigo 14.º do CP.[96] Excecionalmente, a conduta descrita do n.º 5 exige dolo direto ou necessário, nos termos dos n.º 1 e 2 do artigo 14.º, por se tratar de um crime de intenção, isto é, tem subjacente uma intencionalidade na conduta do agente que constitui elemento específico do tipo subjetivo de ilícito e, por isso, afasta a exigência de dolo eventual, mas necessita de prova da dita intencionalidade para criminalizar a conduta do agente.[97] O mesmo sucede com as condutas dos n.º 2 e 7 que exigem intenção lucrativa, logo a verificação dessa intencionalidade afasta o dolo eventual.[98] Também a alínea d) do n.º 1 do artigo 176.º do CP corresponde a um crime de intenção através da expressão «com o propósito de».

Para PAULO PINTO DE ALBUQUERQUE, a conduta consagrada na alínea d) corresponde a um *crime de ato cortado*, tendo em conta que inclui uma intenção de atingir um resultado que não integra o tipo, mas que é alcançado através de uma intenção posterior do agente, ou seja, o agente tem «o propósito de» de distribuir, importar, exportar, divulgar, exibir ou ceder materiais pedopornográficos após a sua aquisição ou detenção, bastando que o agente possua essa intenção mesmo que não verifique qualquer resultado.[99] No entanto, parece-nos mais acertada a visão de MARIA JOÃO ANTUNES e SUSANA AIRES DE SOUSA quanto à definição desta alínea como um *crime de resultado cortado*, na medida em que o preenchimento do tipo subjetivo exige tanto a verificação de atuação dolosa, como a verificação da específica intenção de produzir um

[96] Cfr. MARIA JOÃO ANTUNES e CLÁUDIA SANTOS *ob. cit.*, p. 882, M. MIGUEZ GARCIA e J. M. CASTELA RIO, *ob. cit.*, p. 736. ANA PAULA RODRIGUES diz expressamente que as condutas são admissíveis até a título de dolo eventual, *ob. cit.*, p. 274. Ainda, INÊS FERREIRA LEITE sustenta que basta existir dolo eventual na maioria das incriminações relativas a agressões sexuais a menores de 14 anos de idade, pois é indiferente, na ótica da vítima, se se verifica uma motivação especial do agente ou se este pretende satisfazer os seus instintos sexuais ou produzir material pornográfico, a lesão do bem jurídico ocorre de qualquer modo, *Pedofilia*, p. 86.

[97] PAULO PINTO DE ALBUQUERQUE define "crime de intenção" como a incongruência entre o tipo objetivo e o tipo subjetivo do crime, uma vez que o tipo subjetivo exige uma determinada intenção na conduta do agente que o tipo objetivo não exige e engloba duas formas: o *crime de resultado cortado* que se define pelo tipo subjetivo possuir uma intenção de realização de um resultado que não faz parte do tipo objetivo, mas este é provocado pela ação típica do agente e o *crime de ato cortado* no qual o tipo objetivo tem uma intenção de realização de um resultado que não faz parte do tipo objetivo, mas ocorre devido a uma ação posterior que o agente ou terceiro pratica, *Comentário do código penal*, p. 162 e 763-764.

[98] Cfr. MARIA JOÃO ANTUNES e SUSANA AIRES DE SOUSA, *ob. cit.*, pp. 245 e 246 e ANDRÉ LAMAS LEITE, *ob. cit.*, p. 70. Contrariamente, PAULO PINTO DE ALBUQUERQUE defende que a conduta descrita no n.º 5 exige dolo direto, *Comentário do código penal*, p. 764.

[99] *Id.*, p. 762. No mesmo sentido, M. MIGUEZ GARCIA e J. M. CASTELA RIO, *ob. cit.*, p. 736.

resultado que não se exige no tipo objetivo, no caso, não se pretende punir aqui a mera detenção ou aquisição de materiais pornográficos, até porque essa conduta é punida, como vimos, no n.º 5, mas sim a intenção da sua difusão.[100] Não levantando dúvidas, o n.º 7 é considerado como *crime de resultado cortado*, visto que não é necessária a verificação de um lucro obtido pelo agente, desde que se confirme a sua intenção lucrativa.

No que diz respeito ao erro, podemos estar perante erro quanto à idade da vítima e erro quanto ao tipo de material pornográfico com representação realista. O erro quanto à idade da vítima afasta, naturalmente, o dolo, nos termos do n.º 1 do artigo 16.º do CP, logo não se pune a ação do agente que não percebe que a vítima é menor de idade. Porém, concordando com INÊS FERREIRA LEITE, a verdade é que pode acontecer que o agente se encontre na dúvida relativamente à idade do menor em causa dado o seu aspeto físico e/ou maturidade e se se provar efetivamente que existiu essa dúvida e, mesmo assim, o agente nada fez para averiguar a real idade do menor em causa, antes conformando-se, esta ação do agente já não pode ficar impune, punindo-se a título de dolo eventual.[101] Já o erro quanto ao tipo de material pornográfico com representação realista constitui erro sobre a factualidade típica, ao abrigo da primeira parte do n.º 1 do artigo 16.º do CP, o que significa que o agente não representou os elementos do tipo ou representou-os erroneamente e, por esse motivo, exclui-se o dolo do tipo.

5. Concurso de crimes

No que diz respeito à prática de vários crimes de pornografia de menores, cumpre analisar se se trata de uma pluralidade de crimes ou de um único crime, de acordo com o estipulado no artigo 30.º do CP. Ora, o n.º 1 deste artigo prevê que "o número de crimes determina-se pelo número de tipos de crimes efetivamente cometidos ou pelo número de vezes que o mesmo tipo de crime for preenchido pela conduta do agente", enquanto que o n.º 2 define crime continuado como "a realização plúrima do mesmo tipo de crime ou de vários tipos de crime que fundamentalmente protejam o mesmo bem jurídico, executada por forma essencialmente homogénea e no quadro da solicitação de uma mesma situação exterior que diminua consideravelmente a culpa do agente". Por fim, o

[100] *Ibidem.*
[101] INÊS FERREIRA LEITE, *A tutela penal da liberdade sexual*, pp. 91 e 92.

n.º 3 estabelece que o crime continuado não abrange os crimes praticados contra bens eminentemente pessoais.

Deste modo, para quem considera que o bem jurídico a proteger é a liberdade e autodeterminação sexuais do menor, o agente comete tantos crimes quanto o número de menores que utilizar ou aliciar em espetáculo, fotografia, filme ou gravação pornográficas, devido ao bem ser eminentemente pessoal. Neste sentido, PAULO PINTO DE ALBUQUERQUE, M. MIGUEZ GARCIA e J. M. CASTELA RIO e JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO em relação às alíneas a) e b) do n.º 1 do artigo 176.º do CP, mas já não com o mesmo raciocínio em relação às alíneas c) e d) do n.º 1 e os n.º 4, 5 e 6, sendo irrelevante o número de fotografias, filmes ou gravações existentes, ainda que se refiram a diferentes sujeitos, ou seja, independentemente do número de materiais pornográficos existe apenas um crime.[102]

Em sentido contrário, defendendo que o bem jurídico em causa corresponde a um bem jurídico supraindividual diverso da liberdade e autodeterminação sexuais do menor, isto é, não se tratando de bens eminentemente pessoais, ANA PAULA RODRIGUES e ÂNGELA PINTO definem que comete um único crime o agente que detém, exibe ou cede imagens pornográficas independentemente do número de menores.[103] Neste prisma, nada obsta que ao agente seja imputado um crime continuado de pornografia de menores, desde que se verifiquem os requisitos do n.º 2 do artigo 30.º. Portanto, a figura do crime continuado exige a verificação de uma situação exterior que diminua consideravelmente a culpa do agente. MARIA JOÃO ANTUNES e SUSANA AIRES DE SOUSA justificam essa diminuição de culpa com base no argumento de que o desenvolvimento da tecnologia veio conferir uma maior facilidade de acesso e partilha de materiais pornográficos de forma anónima, o que leva à repetição da conduta.[104] Não podemos partilhar este entendimento, na medida em que não é aceitável defender que a culpa do agente é sensivelmente diminuída devido à facilidade e anonimato que a *internet* confere à prática dos seus atos ilícitos, estar-se-ia quase a "desculpar" a censurabilidade da conduta do

[102] Cfr. PAULO PINTO DE ALBUQUERQUE, *Comentário do código penal*, p. 765, M. MIGUEZ GARCIA e J. M. CASTELA RIO, *ob. cit.*, p. 736 e JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO, *ob. cit.*, p. 267. Estes últimos autores desenvolvem o raciocínio ao concluir que a utilização de materiais pedopornográficos, tratando-se de uma forma indireta de tutela da liberdade e autodeterminação sexuais, não releva para a individualização de crimes consumados, mas sim para a medida da pena.

[103] ANA PAULA RODRIGUES, *ob. cit.*, pp. 274 e 275 e ÂNGELA PINTO, *ob. cit.*, p. 116. Com este entendimento, mas apenas em relação às alíneas c) e d) do n.º 1 e aos n.º 4, 5 e 6 do artigo 176.º do CP, MARIA JOÃO ANTUNES e SUSANA AIRES DE SOUSA, *ob. cit.*, p. 258.

[104] *Id.* Contra a admissibilidade do crime continuado, PAULO PINTO DE ALBUQUERQUE, *ob. cit.*, pp. 765 e 766.

agente por se sentir "tentado" a praticar condutas que a *internet* incita, quando não é essa a sua função.

Assim, concluímos pela não admissibilidade do crime continuado na pornografia de menores, nos termos do n.º 3 do artigo 176.º, pois, apesar de considerarmos que o bem jurídico tutelado é um bem jurídico supraindividual, o livre desenvolvimento do menor na sua esfera sexual, este não deixa de conter caráter eminentemente pessoal.[105]

Na jurisprudência, após a introdução do n.º 3 do artigo 30.º do CP que veio pôr fim à aplicação da figura do crime continuado nos crimes praticados contra bens eminentemente pessoais, começou a tentar resolver-se o problema da contagem do número de crimes recorrendo à figura do crime de trato sucessivo. Contrariamente ao crime continuado, pune-se um só crime, mas com um progressivo agravamento da culpa com a sucessão de condutas, ou seja, pune-se o ilícito mais grave. Todavia, o Acórdão do STJ de 13.03.2019 determinou expressamente que a jurisprudência do STJ tem, na sua maioria, negado recorrer às figuras do crime continuado e do crime de trato sucessivo no que toca aos crimes que tutelam bens eminentemente pessoais, sendo que a «indeterminação relativamente ao número de crimes cometidos em determinado período de tempo não deve ser colmatada com o recurso à figura do trato sucessivo».[106]

De facto, é bastante comum que existam situações de concurso de crimes, visto que ao crime de pornografia de menores está, muitas vezes, associado um concreto abuso do menor utilizado ou aliciado para material pedopornográfico, podendo ocorrer mediante variadíssimas formas, especialmente nas redes de pornografia infantil. Portanto, sempre que esteja em causa uma situação de abuso sexual de criança, atos sexuais com adolescentes, recurso à prostituição ou lenocínio, presentes nos artigos 171.º a 175.º do CP, e, ainda, de ofensa à integridade física do menor, nos termos do artigos 143.º, 144,º e 145.º do CP, em conjugação com o crime de pornografia de menores, estamos perante concurso efetivo, porque ambas as condutas possuem um desvalor autónomo, tomando como exemplo o agressor que filma a relação sexual com a vítima.[107]

---

[105] Cfr. Acórdão do STJ de 17.05.2017, processo n.º 194/14.8TEL.SB.S1, relator Pires da Graça, disponível em www.dgsi.pt.

[106] Ac. STJ de 13.03.2019, processo n.º 3910/16.0T9PRT.P1.S1, relator Vinício Ribeiro, disponível em www.dgsi.pt.

[107] Exemplo dado por JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO, *ob. cit.*, p. 267. Com a mesma opinião quanto ao concurso efetivo, ANA PAULA RODRIGUES, *ob. cit.*, p. 274. Com uma posição intermédia, INÊS FERREIRA LEITE ao defender que não se pode exigir concurso efetivo se o agente que abusar sexualmente de menor e proceder à sua gravação, agindo de forma unitária, nunca a divulgar, é, por isso, excecionalmente punido pelo crime mais grave, *Pedofilia*, p. 144.

III. Prova digital

6. Definição e características da prova digital

A *internet* tem um papel fundamental na atualidade, encontrando-se presente em todos os aspetos da vida em sociedade e contribuindo para o desenvolvimento das mais variadíssimas áreas. Ainda que o desenvolvimento de novas tecnologias possua bastantes vantagens, também veio trazer um campo muito fértil para a prática de atos ilícitos, isto porque a *internet* potencia a comunicação a nível global, praticamente sem riscos para o agente que utiliza um aparelho eletrónico para a realização de crimes – quer seja um computador, *smartphone*, *tablet* - podendo até nem se identificar e, por isso, diminuindo a probabilidade de uma punição. O crime de pornografia de menores não é exceção, sendo que o fenómeno da *internet* serviu como catalisador tanto para a sua prática como para a sua evolução, inclusive permitindo a criação de redes de pornografia infantil, principalmente instaladas na *Darkweb* - como veremos adiante -, uma vez que é facilitada a comunicação e a partilha de conteúdos pedopornográficos.

Assim, a cibercriminalidade é cada vez mais uma realidade e um desafio para a investigação criminal, na medida em que a tecnologia está sempre em constante mudança e desenvolvimento e o Direito tem a árdua tarefa de se ir atualizando com esta evolução. Como afirma PEDRO DIAS VENÂNCIO: «as especificidades da criminalidade informática colocam-se não só na transferência de comportamentos ilícitos para o ambiente digital, como na tipificação de novos crimes como elementos caracterizadores de natureza digital».[108]

Ora, como decorrência desta mudança de paradigma na investigação criminal, surgiu o conceito de prova digital. Apesar do legislador não ter estabelecido uma definição de prova digital na LCib, esta pode ser definida como «qualquer tipo de informação, com valor probatório, armazenada [em repositórios eletrónico-digitais de armazenamento] ou transmitida [em sistemas e redes informáticas ou redes de comunicação eletrónicas, privadas ou publicamente acessíveis], sob a forma binária ou digital».[109] Por sua vez, o Conselho da Europa define como *«any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact*

[108] PEDRO DIAS VENÂNCIO, *Lei do Cibercrime Anotada e Comentada*, 2011, p. 15.
[109] BENJAMIM SILVA RODRIGUES, *Da Prova Penal, Tomo IV, Da prova eletrónico-digital e da criminalidade informático-digital*, p. 30.

disputed in legal proceedings».[110] Este tipo de prova é, então, totalmente diferente do conceito de prova tradicional, sendo necessário que as autoridades policiais e judiciárias tenham conhecimentos específicos sobre a sua obtenção e análise, na medida em que contém características muito particulares.

A prova digital caracteriza-se por ser imaterial, efémera, frágil, alterável, volátil, instável, imaterial, complexa, codificável e dispersa.[111] Estas características resultam, grosso modo, da própria natureza da comunicação informacional, ou seja, a prova digital é facilmente transmitida entre vários indivíduos, numa fração de segundos e em grandes quantidades, não ficando a informação necessariamente guardada num local fixo, assim como podendo ser facilmente alterada, frequentemente por programas informáticos com essa mesma função. Além disso, apresenta um caráter deslocalizado e transfronteiriço, encontrando-se em vários locais do mundo, pois o objetivo é a disseminação da informação em larga escala, com baixos custos e a uma grande velocidade, como ocorre no caso da disseminação de pornografia infantil. Esta dispersão acarreta um dos maiores desafios da prova digital e da cibercriminalidade, que corresponde à dificuldade na determinação da lei aplicável, colocando em crise o princípio da territorialidade, previsto na alínea a) do artigo 4.º do CP, não podendo aqui encontrar-se a solução, pois dificultaria em grande medida a investigação criminal nestes crimes, como veremos melhor *infra*.

No fundo, é a imaterialidade da prova digital que configura o ponto de partida para todas as suas outras características, visto que se encontra armazenada nos sistemas informáticos, mas não significa isto que não exista além do suporte físico onde está guardada.

Posto isto, é incontestável a necessidade de conhecimento técnico e especializado na recolha e preservação da prova digital, de modo a garantir a sua integridade, autenticidade e fiabilidade, logo recorre-se a um perito informático que, em conjunto com a autoridade judiciária e os OPC, procedem à realização da investigação criminal.[112] Desde logo, é crucial que todas as etapas da investigação decorram sempre com a autorização da autoridade judiciária e que sejam devidamente registadas, explicitando

---

[110] Conselho da Europa, *Eletronic Evidence Guide*, p. 11.

[111] Cfr. BENJAMIM SILVA RODRIGUES, *Da Prova Penal*, *Tomo IV*, pp. 42-44, DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, 2011, pp. 102-108 e DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova previstos na Lei do Cibercrime*, 2021, pp.48-50.

[112] Em Portugal, a PJ é o OPC responsável pela investigação criminal em conjunto com as autoridades judiciárias, bem como da prevenção e deteção criminal, ao abrigo dos artigos 2.º a 4.º do DL n.º 137/2019 de 13 de setembro, e do artigo 7.º da Lei n.º 49/2008, de 27 de agosto (Lei de Organização da Investigação Criminal), disponíveis em www.pgdlisboa.pt.

qual é o relevo probatório. A este propósito, é comum falar-se na preservação da cadeia de custódia ou "*chain of custody*", isto é, o registo de todas as ações realizadas ao longo da investigação criminal pelo seu responsável, de modo a manter a integridade da prova digital obtida, pois a quebra na cadeia de custódia pode resultar na não valoração da prova.[113] Esta preocupação com a fiabilidade na recolha de prova digital decorre da natureza da *internet* que se traduz numa rede descentralizada, permitindo que a comunicação percorra diferentes trajetos até chegar ao seu destinatário.

Nesta senda, a investigação começa por verificar a existência da prova digital e a sua consequente obtenção e, para tal, começa por identificar-se a sua fonte, que pode corresponder a um local físico ou a um local virtual. No primeiro caso, a obtenção de prova digital ocorre, normalmente, na sequência de uma busca, nos termos dos artigos 174.º e seguintes do CPP, onde o perito informático se depara com os sistemas informáticos onde está armazenada a prova e procede à sua recolha.[114] No entanto, o caso mais comum é a fonte não corresponder a um lugar físico, por isso, o rumo da investigação deve ser em sentido inverso em relação à típica recolha em local físico, isto é, o perito informático tem antes de descobrir a localização do agente que praticou determinado ato ilícito e que passa, muitas vezes, pela identificação do endereço IP. A identificação do endereço IP é extremamente importante em sede de obtenção de prova em ambiente digital e apresenta enormes especificidades, pelo que explicitaremos esse processo adiante. De qualquer modo, após a identificação da fonte da prova digital, segue-se a cópia da informação recolhida com vista ao seu armazenamento seguro e facilidade na análise dos dados com pertinência para a investigação.[115] De seguida, o perito informático procede ao exame da prova digital que consiste na apreciação do conjunto dos dados recolhidos, recorrendo aos seus conhecimentos e ferramentas técnicas, com o

---

[113] Cfr. BENJAMIM SILVA RODRIGUES *Da Prova Penal, Tomo IV*, pp. 29 e 30 e Conselho da Europa, *Eletronic Evidence Guide do Conselho da Europa*, pp. 14, 161-162.

[114] Quando a recolha é realizada fisicamente, deve o perito informático registar todo o equipamento informático relevante e o estado em que se encontravam, nomeadamente, se estavam ligados ou não. Pode acontecer que seja necessária a apreensão dos ditos equipamentos, estes devem ser transportados e devidamente colocados num lugar seguro pelas autoridades ou que seja necessária a recolha no local para evitar a perda dos dados mais voláteis, como enuncia DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, pp. 118-120. Pormenorizadamente, Conselho da Europa, *Eletronic Evidence Guide*, pp. 41-76.

[115] DAVID SILVA RAMALHO alerta, e bem, para a possibilidade da cópia do sistema informático poder ser total ou parcial, sendo evidente que a cópia total é muito mais invasiva para o titular do equipamento, podendo as autoridades inclusive deparar-se com conteúdo íntimo que nada releva para a investigação em curso e, por este motivo, este processo deve obedecer ao princípio da proporcionalidade, como de resto todas as diligências de prova, devendo a cópia total ser utilizada apenas nos casos em que é imprescindível, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, pp. 122-124.

intuito de selecionar a informação relevante, passando então para a fase de análise que se traduz na conversão destes dados em prova propriamente dita.[116] Por fim, é elaborado o relatório onde se indica todas as diligências realizadas, explicando o seu fundamento e quais as ferramentas utilizadas.[117] Claro está que a linguagem técnica terá de ser transformada numa linguagem compreensível, tanto para as autoridades judiciais, como para o próprio arguido, uma vez que este precisa de compreender o conteúdo dos atos ilícitos que lhe estão a ser imputados.

Ainda assim, tendo em conta que haverá cada vez mais especialização tecnológica por parte dos cibercriminosos, a investigação criminal enfrentará mais dificuldades com o constante desenvolvimento de técnicas que permitem contornar a lei. É por esse motivo que a codificação da prova digital configura uma característica tão apelativa, porque permite o anonimato do agente do crime, por exemplo, mediante a utilização de uma identidade falsa, mas também da encriptação da própria informação transmitida.[118] Como tal, cabe aqui analisar os mecanismos de codificação utilizadas. Portanto, o anonimato do agente é, muitas vezes, alcançado através da criação de identidades falsas ou da utilização de redes *Wi-Fi* públicas e, ainda, através de pagamentos *online*, mediante moedas virtuais, vulgo criptomoeda, dificultando a identificação do agente do crime.[119] Contudo, existem técnicas bastante mais sofisticadas que são as que causam mais alarme, pois implicam sempre uma modificação de dados informáticos,[120] quer seja pela eliminação, adulteração ou dissimulação de dados. Na eliminação de dados, o agente pretende que as autoridades não consigam recuperar determinado conteúdo, por exemplo, eliminando os ficheiros do disco rígido.[121] No caso da adulteração de dados informáticos, a intenção é a recolha de informação já previamente contaminada, alterando o seu conteúdo original e,

[116] Cfr. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, pp. 127-129 e BENJAMIM SILVA RODRIGUES, *Da Prova Penal, Tomo IV,* pp.

[117] BENJAMIM SILVA RODRIGUES remete este relatório com caráter digital ao regime do relatório pericial tradicional, plasmado no artigo 157.º CPP, *Da Prova Penal, Tomo IV*, p. 513. Já DAVID SILVA RAMALHO pronuncia-se sobre o relatório final dever ser elaborado, preferencialmente, pelo MP ou pelos OPC, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, p. 130.

[118] Cfr. VERA MARQUES DIAS, "A Problemática da Investigação do Cibercrime", *Data Venia, Revista Jurídica e Digital*, Ano 1, n.º 1, Julho-Dezembro 2012, pp. 71-74.

[119] Cfr. MARCO GERCKE *Understanding Cybercrime: A Guide for Developing Countries*, 2009, pp. 33 e DAVID SILVA RAMALHO, falando especificamente sobre *bitcoin*, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, pp. 157-164.

[120] A definição de dados informáticos encontra-se prevista na alínea b) do artigo 2.º da LCib: «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».

[121] Cfr. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, pp. 165-167. O autor esclarece que existem mecanismos através dos quais um perito informático consegue recuperar estes dados eliminados, desde que estes não tenham sido substituídos por outros.

consequentemente, tornando-a inútil para efeitos de investigação criminal.[122] Por último, a dissimulação de dados, que tem como objetivo torná-los impercetíveis para quem os investiga, engloba duas áreas relevantes: a criptografia e a esteganografia. DAVID SILVA RAMALHO define a criptografia como o «conjunto de princípios e técnicas utilizados para converter, de forma reversível, certa informação legível em informação ilegível através da utilização de códigos pré-definidos, de modo a permitir que a mesma apenas seja conhecida pelo seu destinatário», enquanto que a esteganografia corresponde ao «método utilizado para esconder a informação dentro de outros ficheiros digitais, como sejam imagens, vídeos, músicas, ou outro tipo de documentos».[123] Dentro da criptografia, a técnica mais utilizada é a encriptação propriamente dita, ou seja, a cifragem de texto, de ficheiros individuais ou mesmo de todo o disco rígido.[124] Inclusive, a encriptação e a esteganografia podem cumular-se, tornando ainda mais difícil e morosa a investigação.[125]

Por tudo isto, a prova digital surge, não só como o presente e o futuro da criminalidade, mas como um dos grandes desafios do direito penal moderno.

[122] *Id.*, pp. 172-174.
[123] *Id.*, pp. 167-168 e 170. Detalhadamente, Conselho da Europa, *Eletronic Evidence Guide*, pp. 77-79 e 144.
[124] Uma outra técnica de criptografia é o denominado *hashing*, isto é, um algoritmo matemático que transforma os ficheiros numa complexa sequência de números – um *hash value* - que serve como a sua "assinatura" e que pretende salvaguardar a integridade do ficheiro em causa, muito utilizado pelas autoridades, demonstrando assim que a criptografia é algo bastante abrangente e que é utilizada tanto para a investigação criminal, como na cibercriminalidade. Cfr. Conselho da Europa, *Eletronic Evidence Guide*, pp. 134 e 135.
[125] MARCO GERCKE explicita a dificuldade dos *software* de encriptação, acessíveis a todos, significarem um enorme desafio para as autoridades judiciais e policiais, dando o exemplo prático: *«for investigative authorities, it is difficult to distinguish the harmless exchange of holiday pictures and the exchange of pictures with encrypted hidden messages»*, *Understanding Cybercrime*, pp. 77 e 78.

7. A articulação das leis aplicáveis

A prova digital é cada vez mais uma realidade no nosso ordenamento jurídico-penal e o cibercrime constitui o modo mais comum na prática de diversos atos ilícitos. Assim, o legislador viu-se obrigado a compreender estas matérias, que não são tipicamente relacionadas com o Direito, e a introduzir normas específicas no ordenamento jurídico português. Porém, as normas aplicáveis à prova digital e à cibercriminalidade estão longe de ser pacíficas e unânimes, isto porque existem distintos diplomas legais que regulam estas matérias e não são congruentes entre si, gerando muita confusão na doutrina e na jurisprudência.[126] Essencialmente, falamos de três diplomas: o CPP, a Lei n.º 32/2008, de 17.07, e a Lei n.º 109/2009, de 15.09 (doravante LCib).

Ora, o CPP não apresenta quaisquer normas específicas para a prova digital ou para o cibercrime, estando orientado para o ambiente físico e não para o ambiente digital, o que significa que os meios de obtenção aí consagrados são claramente insuficientes na obtenção e valoração de prova digital.[127] Como aponta CONDE CORREIA, o legislador mistura as realidades física e digital quando, ao abrigo do artigo 189.º do CPP, submete o regime das interceções telefónicas e outras comunicações, como as realizadas através do telemóvel, correio eletrónico ou outra forma de transmissão de dados por via telemática, ainda que guardadas em suporte digital.[128] Do mesmo modo, PAULO DÁ MESQUITA critica o legislador por não resolver esta confusão de realidades presente no CPP que, de forma alguma, se pode reportar às formas de comunicação por via telemática, mas é o que acontece no regime do artigo 189.º do CPP.[129]

Quanto à Lei n.º 32/2008, este diploma corresponde à transposição para o direito interno da Diretiva n.º 2006/24/CE, do Parlamento e do Conselho, de 15.03, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações eletrónicas, sendo que a lei nacional regula a conservação e transmissão de dados de tráfego e localização, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de

[126] CONDE CORREIA caracteriza, de forma muito acertada, esta incongruência legislativa relativa à prova digital como «um verdadeiro pântano prático», "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público*, n.º 139, julho-setembro 2014, p. 30.
[127] BENJAMIM SILVA RODRIGUES, *Da Prova Penal, Tomo IV*, p. 502.
[128] Cfr. CONDE CORREIA, *ob. cit.*, pp. 31 e 32.
[129] PAULO DÁ MESQUITA, "Prolegómeno sobre prova eletrónica e interceção de telecomunicações no Direito Processual Penal Português – o Código e a Lei do Cibercrime", *Processo Penal, Prova e Sistema Judiciário*, 2010, pp. 89 e 90.

crimes graves por partes das autoridades competentes.[130] Na prática, esta Lei veio implementar no nosso ordenamento jurídico a obrigatoriedade da conservação de todos os dados de tráfego, de base e de localização,[131] consagrados no artigo 4.º da Lei n.º 32/2008, por parte dos fornecedores de serviços de comunicações eletrónicas,[132] pelo prazo de 1 ano a contar da data da conclusão da comunicação, de acordo com o seu artigo 6.º, independentemente da existência de um processo penal.[133] Já relativamente à transmissão dos dados, o artigo 9.º estipula que só pode ser autorizada por despacho fundamentado do JIC, se existir razões para crer que são indispensáveis para a descoberta da verdade ou que a prova é impossível ou muito difícil de obter de outra forma em sede de investigação, deteção e repressão do catálogo restritivo de crimes previsto neste diploma, sendo que a autorização só pode ser requerida pelo MP ou pelo OPC competente e desde que respeite os princípios da adequação, necessidade e proporcionalidade.[134]

Por último, a LCib constitui o «verdadeiro sistema processual de prova digital».[135] Esta Lei corresponde à transposição para o direito interno da Decisão-Quadro n.º

---

[130] Os crimes graves aqui em causa são os referidos na alínea g) do artigo 2.º da Lei n.º 32/2008.

[131] Os *dados de tráfego* correspondem a uma subcategoria dos já mencionados dados informáticos e definem-se 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», de acordo com a alínea c) do artigo 2.º da LCib.
Os *dados de base* são «na perspetiva dos utilizadores, os elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respetivo serviço: interessa essencialmente o número e os dados através dos quais o utilizador tem acesso ao serviço», conforme a definição do Parece n.º 21/2000 do Conselho Consultivo da PGR, disponível em www.ministeriopublico.pt, como a identificação do utilizador e a morada de acesso à rede.
Os *dados de localização* são «quaisquer dados tratados numa rede de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónica publicamente disponível», de acordo com o artigo 2.º da Diretiva 2002/58/CE, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32002L0058.
Os dados previstos no artigo 4.º da Lei n.º 32/2008 são os chamados *metadados*, ou seja, dados sobre dados, pois não incidem sobre o conteúdo das comunicações.

[132] Os *fornecedores de serviços* correspondem a «qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respetivos utilizadores», ao abrigo da alínea d) do artigo 2.º da LCib. Pense-se, no caso de comunicações através da *internet*, no *Google*, *Facebook*, *Microsoft* e, no caso de operadoras de telecomunicações, na Vodafone, MEO ou NOS, em Portugal. Também conhecidos como *internet service providers*.

[133] Cfr. DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de prova previstos na Lei do Cibercrime*, p. 59.

[134] CONDE CORREIA entende que o legislador duplicou o regime no que respeita a este artigo com as normas gerais do CPP, porque a aquisição e valoração processual penal devia estar estipulada no CPP e a conservação preventiva de dados, pelo contrário, pode ficar reservada à legislação extravagante, correspondendo a conceitos diferentes, *ob. cit.*, pp. 33 e 34.

[135] *Id.*, p. 35.

2005/222/JAI do Conselho, de 24.02,[136] e da Convenção sobre o Cibercrime do Conselho da Europa ou Convenção de Budapeste, no qual o legislador optou por criar um diploma extravagante – e não a inserção no CPP – de normas penais materiais (artigos 3.º a 10.º), processuais (artigos 11.º a 19.º) e de cooperação internacional relativas à cibercriminalidade (artigos 20.º a 26.º), de modo a, num único diploma, deter um regime mais eficaz para a prova digital e satisfazer as exigências europeias e internacionais.

Relativamente à conjugação de todos estes diplomas, confere-se que existe uma grande controvérsia na doutrina e na jurisprudência. Na articulação entre o CPP e as duas restantes leis, a maioria parece defender que o artigo 189.º do CPP foi revogado tacitamente por ambas, ainda que muitas das disposições normativas da LCib remetam para o regime geral do CPP, isto é, os artigos 187.º a 190.º.[137] Mais problemática é a conjugação da LCib e a Lei n.º 32/2008, tendo em conta que o artigo 11.º, n.º 2 da LCib estabelece que «as disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de julho». Portanto, a minoria da doutrina e da jurisprudência defendem uma interpretação literal deste artigo, logo vão no sentido da revogação do regime do artigo 9.º da Lei n.º 32/2008 pelas disposições processuais da LCib.[138] No entanto, a maioria entende que, por força do artigo 11.º, n.º 2, da LCib, os dois regimes encontram-se em complementaridade.[139] Este complementaridade tem uma consequência prática nos crimes contra a liberdade e autodeterminação sexuais, uma vez

---

[136] Cfr. Decisão-Quadro n.º 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005F0222.

[137] Cfr. CONDE CORREIA, *ob. cit.*, p. 36, RITA CASTANHEIRA NEVES, *As Ingerências nas Comunicações Eletrónicas em Processo Penal*, 2011, p. 280 e DUARTE RODRIGUES NUNES, *O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada: contributo para uma adequação do direito português às exigências de uma resposta eficaz à criminalidade organizada em matéria de utilização de métodos "ocultos" de investigação criminal*, 2020, p. 557. Defendendo uma revogação parcial, PAULO DÁ MESQUITA, *ob. cit.*, pp. 104 e 105.

[138] Concordam com esta revogação, CONDE CORREIA, *ob. cit.*, p. 36, PAULO DÁ MESQUITA, *ob. cit.*, pp. 110 e 111 e DUARTE RODRIGUES NUNES apenas quanto aos dados de conservação, *Os Meios de Obtenção de Prova*, pp. 65 e 66. Na jurisprudência, Acórdão do TRE de 06.01.2015, processo n.º 6793/11.2TDLSB-A.E1, relator João Gomes de Sousa, disponível em www.dgsi.pt.

[139] Cfr. BENJAMIM SILVA RODRIGUES, *Da Prova Penal, Tomo II, Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, 1ª edição, 2010, pp. 439 e 440 e *Tomo IV*, p. 519, PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*, p. 549, PEDRO DIAS VENÂNCIO, *ob. cit.*, pp. 100 e 101, CARLOS PINHO, "Os problemas interpretativos resultantes da Lei nº 32/2008, de 17 de julho (Conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações)", *Revista do Ministério Público*, nº 129, Jan-Mar 2012, p. 79, RITA CASTANHEIRA NEVES, *ob. cit.*, pp. 237 e 238 e ÂNGELA PINTO, *ob. cit.*, p. 120. Na jurisprudência, o Acórdão do TRL de 07.03.2017, processo n.º 1585/16.5PBCSC-A.L1-5, relator Artur Vargues e o Acórdão do TRP de 20.11.2019, processo n.º 54/19.6GDSTS-A.P1, relator Borges Martins, disponíveis em www.dgsi.pt.

que estes correspondem à terminologia de criminalidade violenta, presente na alínea j) do artigo 1.º do CPP, que é o mesmo que dizer que se aplica o regime da Lei n.º 32/2008 porque se aplica a crimes graves, mas apenas se for punível com pena de prisão de máximo igual ou superior a 5 anos. Portanto, todos os crimes contra a liberdade e autodeterminação sexuais puníveis com pena inferior seguem o regime do artigo 189.º, n.º 2, do CPP.

No nosso entender, parece existir uma intenção clara por parte do legislador quando redigiu o n.º 2 do artigo 11.º da LCib no sentido da complementaridade, pelo que concordamos com a opinião da maioria da doutrina e jurisprudência, ou seja, que a Lei n.º 32/2008 consagra a obtenção de dados de tráfego e localização nos crimes graves, enquanto a LCib é relativa à investigação de crimes cometidos por meio de um sistema informático ou a crimes cometidos em que seja necessário proceder à recolha de prova em suporte eletrónico. Não quer isto dizer, contudo, que a escolha do legislador seja a mais correta, uma vez que exige um esforço hercúleo do aplicador do direito para conseguir conciliar estes três diplomas, devido às remissões constantes de umas normas para as outras, que se vê sujeito à melhor articulação possível consoante o caso concreto, logo não existe harmonia legislativa, o que gera sempre confusões.[140]

[140] Numa tentativa de simplificar esta conjugação e acabando por concluir desta maneira, a Nota Prática n.º 8/2016, de 18.02, do Gabinete do Cibercrime do MP, disponível em https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_8_pedido_de_info_a_isp.pdf.

7.1. Os meios de obtenção de prova existentes na LCib

A LCib constitui o diploma central em matéria de obtenção e valoração de prova digital, contendo as disposições processuais que regulamentam os meios de obtenção de prova existentes, previstos nos artigos 11.º a 19.º.

O artigo 11.º da LCib começa por determinar que as disposições processuais se aplicam aos crimes previstos nas alíneas do seu n.º 1. Desde logo, esclarecemos que o crime de pornografia de menores constitui um destes crimes, nos termos das alíneas b) e c), devido à crescente transferência deste tipo de criminalidade para o ambiente digital.

Alguns dos meios de obtenção de prova presentes na LCib são caracterizados como métodos "ocultos" de investigação criminal. Segundo COSTA ANDRADE, os métodos "ocultos" de investigação criminal «representam uma intromissão nos processos de ação, interação e comunicação das pessoas concretamente visadas, sem que estas tenham conhecimento do facto nem dele se apercebam» e, por isso, «levam as pessoas atingidas - normalmente o suspeito - a "ditar" inconscientemente para o processo "confissões" não esclarecidas nem livres».[141]

A ocultação da investigação criminal surge com a crescente dificuldade de obtenção de prova digital. DAVID SILVA RAMALHO alerta, no entanto, que o recurso aos métodos "ocultos" não pode basear-se numa mera dificuldade, mas sim quando se trate de um ilícito tão lesivo que justifica a utilização destes meios mais gravosos para alcançar o sucesso na investigação.[142] Por seu turno, DUARTE RODRIGUES NUNES defende que os métodos "ocultos" não representam uma mudança para um «paradigma de "eficácia quase a todo o custo", mas de adequar um paradigma preexistente que é desadequado e ineficaz para responder a uma forma de criminalidade extremamente danosa para a Sociedade e que ameaça a própria existência do Estado de Direito e é de investigação extremamente difícil».[143]

Todavia, o recurso a métodos "ocultos" de investigação criminal são inerentemente restritivos de direitos fundamentais, pelo que estão sujeitos ao princípio da reserva de lei, ao abrigo do artigo 125.º do CPP, que abrange os meios de obtenção de prova previstos na lei, mas também os meios de obtenção atípicos; ao princípio da

---

[141] COSTA ANDRADE, *"Bruscamente no verão passado"*, pp. 105 e 106.
[142] Cfr. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal*, pp. 204-210.
[143] Aqui DUARTE RODRIGUES NUNES refere-se à criminalidade organizada como exemplo paradigmático da necessidade de recorrer aos métodos "ocultos" de investigação, *O Problema da Admissibilidade dos Métodos "Ocultos" de Investigação Criminal*. p. 430.

proporcionalidade, fazendo a ponderação entre a necessidade da utilização deste método e os direitos fundamentais que restringe, de acordo com o artigo 18.º, n.º 2, da CRP; e, por fim, ao princípio da reserva de juiz, consagrado no artigo 32.º, n.º 4, da CRP, sendo o juiz que tem a competência para autorizar o recurso a estes métodos, salvo algumas exceções consoante o método que esteja em causa.[144] De modo geral, os métodos "ocultos" põe em causa direitos como o direito à intimidade da vida privada, à inviolabilidade das comunicações, à autodeterminação informacional e à confidencialidade, conforme o método utilizado.

No panorama europeu, fala-se, em termos amplos, no direito à privacidade digital que engloba estes direitos fundamentais em contexto de ambiente digital. Na ponderação entre o direito à privacidade digital e a prossecução da investigação criminal, o TEDH utiliza como parâmetro o artigo 8.º da CEDH, que prevê o direito ao respeito da vida privada e familiar, do domicílio e da correspondência, fazendo uma interpretação extensiva para a dimensão digital, para verificar se existe violação deste direito mediante a delimitação de critérios, nos termos do n.º 2 deste artigo, que se não se verificarem, conclui-se pela ilegitimidade da ingerência das autoridades na privacidade digital dos cidadãos.[145] Ainda assim, observam-se posições opostas em relação ao recurso aos métodos "ocultos" de investigação criminal na Europa, desde a sua inadmissibilidade em Itália até à sua admissibilidade na Alemanha.[146]

Em Portugal, o legislador não se expressou diretamente pela sua admissibilidade ou não, pelo que nos encontramos num terreno pantanoso composto por «lacunas e descontinuidades, incongruências e inconsistências e, sobretudo, por insustentáveis contradições e assimetrias normativas, axiológicas e político-criminais».[147] Contudo, indubitavelmente, estes métodos encontram-se dispersos pela legislação, nomeadamente

---

[144] Cfr. COSTA ANDRADE, *"Bruscamente no verão passado"*, pp. 113-117. DAVID SILVA RAMALHO esclarece que não é necessária a criação de novas normas legais habilitantes a cada inovação tecnológica que vai surgindo e que exige uma nova forma de pensar nos métodos de obtenção de prova digital, mas, antes pelo contrário, que este novos métodos de obtenção de prova possam ser reconduzidos a uma previsão legal habilitante, *Métodos Ocultos de Investigação Criminal*, pp. 213-225.

[145] Exemplo de uma decisão do TEDH acerca da ponderação entre a privacidade digital e a ingerência das autoridades públicas nesse direito, com base no artigo 8.º da CEDH, é o Acórdão *Wieser and Bicos Beteiligungen GmbH v. Austria*, de 16.01.2008, disponível em www.hudoc.echr.coe.int. PAULO DE SOUSA MENDES analisou detalhadamente estas questões relacionadas com a privacidade digital, criticando o papel passivo do TEDH por não considerar existirem repercussões da violação deste direito no processo equitativo, de acordo com o artigo 6.º da CEDH, "A privacidade digital posta à prova no processo penal", *Quaestio facti, Revista Internacional sobre Razonamiento Probatorio*, n.º 2, 2021, pp. 227-235.

[146] Cfr. DUARTE RODRIGUES NUNES, *O Problema da Admissibilidade dos Métodos "Ocultos" de Investigação Criminal*, P. 499.

[147] COSTA ANDRADE, "*Bruscamente no verão passado"*, p. 109.

as escutas telefónicas no CPP, mas também a apreensão de correspondência e as ações encobertas na LCib, pois a todos estes métodos de obtenção de prova está subjacente a falta do seu conhecimento pelo visado até ao momento em que já foram consumados.[148]

Apesar disto, a verdade é que o recurso a métodos "ocultos", mesmo com as desvantagens apontadas, vai continuar a fazer parte da investigação criminal e, com o desenvolvimento tecnológico, será cada vez mais uma realidade. Assim, concordamos com COSTA ANDRADE quando incentiva a sua inserção sistemática no CPP, à semelhança do direito alemão, uma vez que levaria a menos situações dúbias e desproporcionais, fruto da arbitrariedade a que estão sujeitos os aplicadores do direito.[149]

7.1.1. Preservação e revelação expedita de dados

Agora, analisaremos as disposições processuais propriamente ditas. Os artigos 12.º e 13.º correspondem às chamadas medidas cautelares da LCib, uma transposição dos artigos 16.º e 17.º da Convenção sobre o Cibercrime, respetivamente, pois têm como objetivo a imposição, pelas autoridades competentes, da conservação de dados informáticos específicos num determinado sistema informático, a quem tiver a sua disponibilidade ou controlo, quando haja receio de que estes possam perder-se, alterar-se ou deixar de estar disponíveis. Portanto, o artigo 12.º da LCib prevê a preservação expedita de dados informáticos, isto é, um "congelamento" ou "*quickfreeze*" destes dados, efetuado através de uma ordem por parte da autoridade judiciária competente ou pelos OPC,[150] nos casos de urgência estipulados no n.º 2, às entidades que tenham a sua disponibilidade ou controlo – normalmente os fornecedores de serviço -,[151] que ficam

[148] Cfr. COSTA ANDRADE, *"Métodos ocultos de investigação: plädoyer para uma teoria geral", Que futuro para o Direito Processual Penal? Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, pp. 532-534, BENJAMIM SILVA RODRIGUES, *Da Prova Penal, Tomo IV*, pp. 532 e 533, RITA CASTANHEIRA NEVES, *ob. cit.*, pp. 95-103 e 196-197.
[149] COSTA ANDRADE, *"Métodos ocultos de investigação"*, p. 540.
[150] DUARTE RODRIGUES NUNES clarifica que a autoridade judiciária competente para emitir a ordem de preservação corresponde ao MP na fase de inquérito, ao JIC na fase de instrução e ao Juiz na fase de julgamento, *Os Meios de Obtenção de Prova*, p. 48.
[151] Não tem de ser necessariamente um fornecedor de serviço, podem ser os cidadãos que disponham ou controlem os dados em causa. Cfr. RITA CASTANHEIRA NEVES, *ob. cit.*, p. 234 e PEDRO VERDELHO, "A nova Lei do Cibercrime", *Scientia Ivridica*, 320, 2009, p. 736.
Além disso, a preservação de dados não tem sempre de configurar um "congelamento", o que é o mesmo que dizer que ficam inacessíveis, podendo os dados ser usados pelos utilizadores legítimos, desde que assim esteja determinado na ordem de preservação, conforme o ponto 159 do Relatório Explicativo da Convenção sobre o Cibercrime, disponível em https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf.

com a obrigação de preservar imediatamente os dados com vista a salvaguardar a produção de prova digital, conforme o n.º 3, tendo em conta que esta é facilmente alterada, danificada ou eliminada. Nos termos dos n.º 3 e 5, a ordem de preservação tem de discriminar, sob pena de nulidade, a natureza dos dados, a sua origem e destino e o período de tempo pelo qual deverão ser preservados até a um máximo de 3 meses, renovável pelo mesmo período até ao limite máximo de 1 ano. É pertinente esclarecer que esta medida pretende a preservação de dados e não o seu arquivo, logo apenas se aplica a dados já previamente recolhidos e arquivados e nunca à sua obtenção em tempo real ou no futuro, mas que incide sobre qualquer tipo de dados.[152]

Por sua vez, o artigo 13.º da LCib consagra a revelação expedita de dados de tráfego que consiste em o destinatário da ordem de preservação expedita de dados informar a autoridade judiciária ou OPC, assim que tiver esse conhecimento, na sequência da ordem de preservação, se existem outros fornecedores de serviço através dos quais a comunicação em causa tenha sido realizada, de modo que também eles possam ser sujeitos a uma ordem de preservação de dados. Este é um meio de obtenção de prova acessório do anterior, uma vez que tem o intuito de garantir a sua eficácia, isto porque é muito comum que uma comunicação seja efetuada mediante vários fornecedores de serviços e que nenhum deles, individualmente, possua todos os dados de tráfego relativos a essa comunicação. Assim, na maioria dos casos, a preservação expedita de dados não é suficiente para identificar a origem ou o destino da comunicação, enquanto que com a complementaridade da revelação expedita de dados de tráfego já armazenados é possível para as autoridades tomarem conhecimento de todo o percurso da comunicação e, deste modo, identificar os indivíduos infratores.[153]

---

[152] De acordo com os pontos 149, 151 e 161 do Relatório Explicativo da Convenção sobre o Cibercrime, onde se estabelece a diferença entre "preservação de dados" e o "arquivo de dados" e, ainda, onde especifica que a incidência sobre todo o tipo de dados pode incluir, exemplificando, sobre registos comerciais, médicos, pessoais ou outros. Cfr. BENJAMIM SILVA RODRIGUES, *Da Prova Penal, Tomo II*, p. 439 e CARLOS PINHO, *ob. cit.*, p. 78.

[153] O Relatório Explicativo da Convenção sobre o Cibercrime explica, ilustrativamente, nos pontos 166 e 167, que a partilha de informação dos fornecedores de serviço através dos quais ocorreu uma determinada comunicação permite que se passe de ter apenas «uma parte do *puzzle*», ou seja, a informação de apenas um dos fornecedores, para possuir toda a informação disponível dos dados de tráfego, completando assim o *puzzle*, dando o exemplo da identificação das pessoas que distribuem produtos de pornografia infantil ao determinar a origem ou o destino de uma dada comunicação. Além disso, no ponto 168, clarifica que a solução de emitir inúmeras ordens de preservação seria demasiado moroso, dando preferência a esta partilha de informação relevante.

7.1.2. Injunção para apresentação ou concessão do acesso a dados

A injunção para apresentação ou concessão do acesso a dados ou "*production order*", plasmada no artigo 14.º da LCib é uma transposição do artigo 18.º da Convenção sobre o Cibercrime, consiste num meio de obtenção de prova através do qual a autoridade competente emite uma ordem à entidade que detém o controlo ou a disponibilidade sobre determinados dados informáticos para, no decurso do processo penal e sempre que se verifique essencial para a descoberta da verdade, os comunique ao processo ou permita o acesso ao sistema informático onde estão armazenados, sob pena de punição por desobediência, nos termos do artigo 348.º do CP *ex vi* n.ºs 1 e 3 do artigo 14.º da LCib.[154]

Ao abrigo do n.º 2 do artigo 14.º, a ordem de injunção deve especificar os dados informáticos a que se pretende aceder ou que sejam fornecidos, de forma a incidir somente sobre dados relevantes para a investigação e não indiscriminadamente. A injunção pode ser dirigida a um cidadão individual ou aos fornecedores de serviços que, em conformidade com o n.º 4, vêem-se obrigados a disponibilizar dados relativos aos seus clientes ou assinantes – frisa-se que os dados aqui em causa são apenas os dados de base e de localização e nunca dados de tráfego ou dados de conteúdo -[155] e que são os dados relativos ao tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço (alínea a), a identidade, morada postal ou geográfica e número de telefone do assinante e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços (alínea b), ou a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviço, mas não dados de conteúdo ou de tráfego (alínea c).[156] No entanto, já não pode ser dirigida a quem não constitua arguido ou suspeito no processo em causa – sob pena de violar o princípio *nemo tenetur se ipsum accusare* ou direito à não autoincriminação, previsto no artigo 61.º, n.º 1, alínea d) do CPP -, a sistemas informáticos utilizados para o exercício da advocacia, de atividades médica, bancária e

[154] PAULO DÁ MESQUITA critica a solução adotada pelo legislador, expressando a sua preferência pela adoção de uma medida compulsória e não sancionatória, por exemplo, através da aplicação de uma sanção pecuniária compulsória, prevista no artigo 829.º-A do Código Civil, por cada dia de atraso no cumprimento da ordem de injunção, assegurando, assim, em tempo útil, a disponibilização dos dados informáticos requeridos, *ob. cit.*, p. 113. DUARTE RODRIGUES NUNES defende a conjugação de ambas, *Os Meios de Obtenção de Prova*, p. 115.

[155] A definição de dados de conteúdo não se encontra prevista na LCib, mas o Relatório Explicativo da Convenção sobre o Cibercrime enuncia, no seu ponto 229, que correspondem ao «conteúdo informativo da comunicação, isto é, o significado ou o teor da comunicação, ou a mensagem ou informação transmitida pela comunicação».

[156] Cfr. Pontos 178 a 181 do Relatório Explicativo da Convenção sobre o Cibercrime.

da profissão de jornalista, tendo em conta o regime de segredo profissional ou de funcionário e de segredo de Estado, previsto no artigo 182.º do CPP, é aplicável com as devidas adaptações, de acordo com os n.º 5, 6 e 7 do artigo 14.º da LCib.[157] Em suma, este meio de obtenção de prova confere uma alternativa menos intrusiva, caracterizando-se por ser um meio mais flexível e menos dispendioso.[158]

Este meio de obtenção de prova apresenta, ainda, uma particularidade que cabe aqui analisar e que é de extrema importância. É frequente que um dos dados mais relevantes que se possam obter na sequência de uma investigação criminal em ambiente digital corresponda ao endereço IP do sujeito infrator. Ora, o IP (*internet protocol*) corresponde, nas palavras de DAVID SILVA RAMALHO, ao «elemento central da comunicação na *internet*», consistindo «num esquema de comunicação que define o modo como os dados são enviados através da rede», atribuindo «um endereço numérico a cada sistema informático ligado à *internet* (o *internet protocol address* ou *IP address*)», o endereço IP.[159] O endereço IP pode ser estático ou dinâmico, sendo que, no primeiro, o número identificador permanece sempre o mesmo, enquanto que, no segundo, este muda consoante a necessidade de atribuição de endereços IP aos muitos dispositivos eletrónicos existentes atualmente em todo o mundo que pretendem conectar-se à rede e tendo em conta que as combinações numéricas que constituem esse endereço são finitas. Porém, o endereço IP dinâmico surge, muitas vezes, associado à data, hora e fuso horário em que o mesmo foi utilizado.

Ainda assim, a identificação do endereço IP não significa que se conhece automaticamente o agente do crime, mas apenas que um certo indivíduo contratou um serviço de *internet*, tendo estabelecido uma ligação à rede em que lhe foi atribuído um determinado IP (no caso de ser dinâmico claro) e, por isso, é comum que esse processo recorra a terceiros, tais como o fornecedor de serviço de acesso à *internet* que regista os

---

[157] RITA CASTANHEIRA NEVES e HÉLDER SANTOS CORREIA refletiram sobre o confronto entre a colaboração do arguido no acesso aos dados informáticos e os meios de obtenção de prova da LCib e, especificamente quanto ao artigo 14.º, consideraram que o legislador ponderou bem os interesses e direitos em causa quando estipulou estas exceções à ordem de injunção, salvaguardando assim o *nemo tenetur* ao não impor uma colaboração ativa do arguido no que poderia, eventualmente, resultar na recolha de prova incriminatória contra si, "A Lei do Cibercrime e a colaboração do arguido no acesso aos dados informáticos", *Actualidad Jurídica Uría Menéndez*, n.º 38, Outubro 2014, p. 148.

[158] ÂNGELA PINTO traz à colação uma questão controversa, mas bastante pertinente, relativamente ao prazo de conservação dos dados de base no âmbito da ordem de injunção, uma vez que a LCib não estabelece qualquer prazo e acaba por concluir que o prazo deve ser 6 meses quando não estiverem em causa os crimes graves da Lei n.º 32/2008, senão o prazo é o estipulado no artigo 6.º desta Lei que corresponde a 1 ano, *ob. cit.*, pp. 122 e 123. Como veremos, as dúvidas adensam devido à recente decisão do TC que declarou inconstitucional o artigo 6.º da Lei n.º 32/2008.

[159] DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal*, p. 52.

endereços IP atribuídos aos seus utilizadores ou a pessoa individual que se viu afetada pela cibercriminalidade cujo sistema informático faz esse registo.[160]

No âmbito da ordem de injunção, a doutrina e a jurisprudência muito têm discutido se o endereço IP corresponde a um dado de base ou um dado de tráfego. Atualmente, a maioria entende que se trata de um dado de base, porque não afeta os dados pessoais e, consequentemente, a privacidade do seu titular, nem revela o percurso da comunicação efetuada, apenas revela o ponto de conexão à rede.[161] Portanto, nos termos do n.º 4 do artigo 14.º da LCib, a ordem de injunção pode incidir sobre a obtenção do IP estático e do IP dinâmico, mas apenas quando as autoridades conhecem o IP dinâmico utilizado, pois implica apenas a identificação do seu utilizador.[162] Por este motivo, a entidade competente para realizar o pedido de identificação do endereço IP é o MP, somente sendo necessária a autorização do Juiz quando se trata de dados de tráfego.[163]

7.1.3. Pesquisa de dados informáticos

O artigo 15.º da LCib estipula a pesquisa de dados informáticos, correspondendo à transposição do artigo 19.º da Convenção sobre o Cibercrime, que nada mais é do que uma verdadeira busca em ambiente digital, isto é, a autoridade judiciária competente autoriza ou ordena a obtenção de dados informáticos específicos e determinados, alojados num certo sistema informático, mediante um despacho que procede à sua pesquisa, com um prazo de validade máximo de 30 dias, sob pena de nulidade, quando se verificar necessária à produção de prova para a descoberta da verdade, devendo a autoridade presidir à diligência sempre que possível, nos termos dos n.º 1 e 2.[164] No n.º 3 determina-se a possibilidade do OPC proceder à pesquisa informática sem a prévia autorização da

[160] *Id.*, p. 120 e ÂNGELA PINTO, *ob. cit.*, p. 123.
[161] No mesmo sentido, CONDE CORREIA, *ob. cit.*, pp. 48 e 49 e ÂNGELA PINTO, *ob. cit.*, p. 123. Na jurisprudência, uma decisão de referência no estabelecimento do endereço IP como um dado de base é o Acórdão do TRL de 19.06.2014, processo n.º 1695/09.5PJLSB.L1-9, relatora Margarida Vieira de Almeida, disponível em www.dgsi.pt.
[162] Fora destes casos, em que se exija o conhecimento de um determinado processo de comunicação para identificar o IP dinâmico, já se trata de um dado de tráfego, estando fora do âmbito deste artigo. Cfr. DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova*, pp. 62 e 63.
[163] Cfr. Notas Práticas n.º 1/2012, de 9.07, e n.º 2/2013, de 3.04, do Gabinete do Cibercrime do MP disponíveis em https://cibercrime.ministeriopublico.pt/notas-praticas?page=1.
[164] O Relatório Explicativo da Convenção sobre o Cibercrime explicita, nos Pontos 184 a 189, que o objetivo deste meio de obtenção de prova foi modernizar e harmonizar os regimes da busca e apreensão tradicionais para os dados informáticos armazenados no âmbito de investigações criminais.

autoridade judiciária nos casos em que existir consentimento documentado de quem tiver a disponibilidade ou o controlo desses dados (alínea a) ou nos casos de crimes que coloquem em causa a vida ou a integridade da pessoa, como o terrorismo, a criminalidade violenta ou altamente organizada (alínea b), com as exceções descritas no n.º 4 que obrigam os OPC a comunicar imediatamente à autoridade judiciária nos casos da alínea b) e, em ambas, deve elaborar-se o devido relatório, ao abrigo do artigo 253.º do CPP.[165] A pesquisa de dados informáticos pode incidir sobre todo o sistema informático, apenas uma parte ou o suporte de armazenamento de dados independentes (como uma *pen drive*).[166]

Já o n.º 5 prevê a extensão da pesquisa informática, bastante útil, porque pode acontecer que, na sequência da pesquisa, os dados procurados se encontrem noutro sistema informático, mas que são legitimamente acessíveis através do sistema informático inicialmente alvo da pesquisa, desde que ocorra mediante autorização ou ordem da autoridade competente. Ora, esta extensão corresponde, no fundo, a uma pesquisa realizada por acesso remoto e apresenta muita utilidade porque facilita a investigação criminal em grande medida, evitando que as autoridades tenham de se dirigir ao local ou mesmo nos casos mais difíceis em que os dados informáticos se encontram no estrangeiro. Contudo, a extensão da pesquisa informática a dados armazenados no estrangeiro suscita bastantes dúvidas.

A propósito da extensão do n.º 5, surge o entendimento de que esta é permissiva em relação às buscas *online* que consiste em «aceder, de forma oculta e à distância, via *internet*, aos dados contidos num computador, observá-los e, sendo caso disso, copiá-los em maior ou menor medida».[167] Existem duas modalidades de busca *online*: a busca que consiste numa única intromissão e a busca que ocorre de forma prolongada no tempo.[168] Ora, este meio de obtenção de prova não se encontra expressamente previsto na lei e, por isso, discute-se a sua admissibilidade no ordenamento jurídico português. Como

---

[165] Se a pesquisa realizada por OPC ocorrer sem o prévio despacho da autoridade judiciária é considerada nula, ao abrigo do n.º 3 do artigo 126.º do CPP. Bastante crítico do n.º 3 do artigo 15.º da LCib, BENJAMIM SILVA RODRIGUES, *Da Prova Penal, Tomo II*, pp. 448 e 449 e *Tomo IV*, pp. 526 e 527.
[166] Cfr. DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova*, p. 87.
[167] COSTA ANDRADE, *"Bruscamente no verão passado", a reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia e devia ter sido diferente*, 2009, p. 153.
[168] A Alemanha prevê a segunda modalidade de busca *online* no artigo §100b da StPO, desde que autorizada por 3 juízes com duração até 1 mês, renovável por igual período, nunca podendo ser obtidas informações subsumíveis à esfera íntima. LUIS GRECO e ORLANDINO GLEIZER explicam os requisitos do regime alemão para proceder à busca *online*, "A infiltração *online* no processo penal – notícia sobre a experiência alemã", *Revista Brasileira de Direito Processual Penal*, Vol. 5, n.º 3, 2019, pp. 1498-1508, disponível em https://revista.ibraspp.com.br/RBDPP/article/view/278/192.

antecipámos, existe a opinião de que a busca *online* é permitida ao abrigo deste n.º 5, uma vez que nada é dito quanto à possibilidade da pesquisa de dados informáticos noutros sistemas informáticos por acesso remoto ser realizada *online*, até porque a exigência da presença da autoridade judiciária competente pode acontecer no local ou *online*, que é o mesmo que dizer no local onde se encontra o sistema informático através do qual se faz a busca *online*, mas apenas nos moldes da primeira modalidade que implica um único acesso.[169] Porém, existem muitas vozes contrárias que acreditam que a busca *online* é um método muito intrusivo, correspondendo a uma violação do domicílio, ainda que não ocorra presencialmente, e da inviolabilidade das telecomunicações e, como não está expressa, ainda do princípio da legalidade.[170]

A nosso ver, a razão encontra-se com quem admite as buscas *online* no ordenamento jurídico português e revemo-nos na totalidade com COSTA ANDRADE quando refere que é um método de obtenção de prova digital muito profícuo «tendo em conta a presença praticamente ubíqua do computador no quotidiano dos cidadãos, em todos os setores e domínios da vida e, portanto, também do lado da preparação, planificação e gestão de meios e recursos do crime» e os «obstáculos técnicos ainda subsistentes e o recurso cada vez mais generalizado a programas de proteção e "blindagem" dos dados».[171]

Por fim, o n.º 6 remete para as normas da execução das buscas previstas no CPP e no Estatuto do Jornalista, com as devidas adaptações, sendo que a consequência mais importante é a diligência ser presidida pelo JIC nos casos em que a pesquisa informática incida sobre determinadas classes profissionais que estão sujeitas a um forte sigilo profissional, assim como a exige a presença do representante profissional do visado.[172] Assim, as disposições sobre buscas do CPP aplicam-se subsidiariamente ao regime das pesquisas informáticas, consagrado no artigo 15.º da LCib.

---

[169] A favor da admissibilidade da busca *online*, DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova*, pp. 227-231, COSTA ANDRADE, *"Bruscamente no verão passado",* pp. 166-180, PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*, p. 502 e CONDE CORREIA, *ob. cit.*, pp. 42-44.

[170] Contra a admissibilidade da busca *online*, CONDE CORREIA, *ob. cit.*, pp. 42-44, RITA CASTANHEIRA NEVES, *ob. cit.*, pp. 196-197 e BENJAMIM SILVA RODRIGUES, *Da Prova Penal, Tomo II*, pp. 471-475.

[171] COSTA ANDRADE, *"Bruscamente no verão passado",* pp. 166 e 167. As buscas *online* estão previstas, no direito espanhol, nos artigos 588 *septies* a, b e c da LEC para certos crimes, como os crimes cometidos contra menores, e apenas por um prazo de 1 mês renovável até ao máximo de 3 meses.

[172] De acordo com os artigos 176.º e 177.º do CPP e 11.º, n.º 6 do Estatuto do Jornalista. Cfr. RITA CASTANHEIRA NEVES, *ob. cit.*, pp. 297 e 298.

7.1.4. Apreensão de dados informáticos

Igualmente uma transposição do artigo 19.º da Convenção sobre o Cibercrime, o artigo 16.º da LCib consagra o regime de apreensão de dados informáticos que consiste na ordem da apreensão de dados ou documentos informáticos já armazenados, necessários à produção de prova, pela autoridade judiciária competente que a autoriza ou ordena mediante despacho, na sequência de uma pesquisa informática ou de outro acesso legítimo a um sistema informático.[173]

O "outro acesso legítimo a um sistema informático", apesar da LCib não indicar quais são esses meios, pode corresponder a um exame ou a uma perícia, mas estas figuras não devem ser confundidas.[174] O exame encontra-se previsto nos artigos 171.º e seguintes do CPP e corresponde a um meio de obtenção de prova que consiste na inspeção de vestígios deixados pela prática de um crime e todos os indícios em relação ao modo ou ao lugar em que este foi praticado e contra ou sobre que pessoas foi cometido que, no caso de prova digital, são os dispositivos eletrónicos e os dados informáticos utilizados para a prática do ilícito. Por seu turno, a perícia consiste na perceção ou apreciação de certos factos, ao abrigo dos artigos 151.º e seguintes do CPP, exigindo, para tal, conhecimentos específicos por parte de quem a realiza, quer sejam técnicos, científicos ou artísticos, no caso de prova digital, realizada por perito informático do laboratório de Polícia Científica da PJ, caracterizando-se como meio de prova, isto é, «visam a deteção de indícios da prática do crime, constituindo um meio de aquisição para o processo de uma prova "preexistente" e, em regra, contemporânea ou preparatória do crime» e consequente «"reprodução" ("avaliação") do facto».[175]

A autoridade competente para ordenar a apreensão de dados é o MP, em sede de inquérito, ou o OPC, sem prévia autorização, quando haja urgência ou perigo na demora, desde que a autorização surja depois no prazo máximo de 72 horas, à luz dos n.º 2 e 4. Os n.º 5 e 6 remetem para o que já abordámos nos n.º 6 e 7 do artigo 14.º da LCib. Relativamente ao n.º 3, a competência para a apreensão tem de ser obrigatoriamente do Juiz, sob pena de nulidade, por estarem em causa dados íntimos ou pessoais, pois restringe

[173] O Relatório Explicativo da Convenção sobre o Cibercrime esclarece, no ponto 199, que a apreensão ou a forma semelhante contém dois objetivos principais: reunir provas mediante a cópia dos dados informáticos apreendidos e confiscar os ditos dados, não permitindo o acesso à sua versão originária ou mesmo removendo-os, mas nunca implica a eliminação definitiva.
[174] DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal*, p. 137 e PEDRO VERDELHO, "A nova Lei do Cibercrime", pp. 740 e 741.
[175] PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*, p. 331.

o direito à privacidade do titular ou de terceiro, devendo ponderar a sua junção aos autos consoante os interesses do caso concreto.[176]

O legislador atendeu ao facto de que os aparelhos eletrónicos dispõem hoje de muita informação pessoal do seu proprietário, tal como afirma CONDE CORREIA, «o computador funciona hoje, muitas vezes, como uma extensão da personalidade», logo «o visado deverá poder exigir que o Estado apenas interfira no conteúdo do seu computador mediante o seu próprio consentimento ou, então, mediante mandado oficial regularmente emitido».[177]

Quanto às formas de execução da apreensão de dados informáticos, as alíneas do n.º 7 estabelecem quatro modos distintos: a apreensão do suporte onde está instalado o sistema ou onde estão armazenados os dados informáticos (alínea a), a realização de uma cópia de dados, em suporte autónomo (alínea b), preservação da integridade dos dados, por meios tecnológicos, sem realização de cópia nem remoção (alínea c) e a eliminação irreversível ou bloqueio do acesso aos dados (alínea d).[178] O critério de aplicação destas formas de execução da apreensão começa, desde logo, pela escolha da medida menos lesiva para os direitos fundamentais dos visados.[179] A forma de execução da apreensão prevista na alínea b) está sujeita, nos termos do n.º 8, a uma cópia em duplicado, sendo uma delas selada e confiada ao secretário judicial dos serviços onde se encontra o processo e, se for preciso, os dados apreendidos são certificados por meio de assinatura digital, de modo a garantir a integridade da prova digital.[180] Também aqui o legislador não impõe que a apreensão dos dados informáticos seja realizada no local, pelo que se depreende que pode ocorrer *online*, à semelhança das buscas *online* do artigo 15.º, n.º 5 da LCib.[181]

---

[176] Defendendo uma proibição absoluta da valoração destes dados, BENJAMIM SILVA RODRIGUES, *Da Prova Penal*, *Tomo II*, p. 451 e *Tomo IV*, p. 529 e PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*, p. 508.

[177] CONDE CORREIA, *ob. cit.*, pp. 51 e 52.

[178] A última forma de execução da apreensão, a eliminação definitiva dos dados e o bloqueio do acesso aos dados, revela-se eficaz nos casos de pornografia de menores, DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de* Prova, p. 138.

[179] Detalhadamente, DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de* Prova, pp. 322-324, RITA CASTANHEIRA NEVES, *ob. cit.*, p. 273 e DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal*, pp. 140 e 141.

[180] BENJAMIM SILVA RODRIGUES defende uma cópia tripartida dos dados apreendidos e discorda da assinatura digital, por entender que a integridade da prova é assegurada através do cumprimento de todas as etapas de obtenção de prova digital, *Da Prova Penal*, *Tomo II*, pp. 452 e 453 e *Tomo IV*, pp. 530 e 531. No mesmo sentido, PEDRO DIAS VENÂNCIO por defender que a assinatura digital corresponde a uma medida de preservação de dados, *ob. cit.*, pp. 114 e 115.

[181] Cfr. DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de* Prova, p. 495.

7.1.5. Apreensão de correio eletrónico e registos de comunicações de natureza semelhante

O legislador português previu especificamente a apreensão de correio eletrónico e registos de comunicação de natureza semelhante no artigo 17.º da LCib, dispondo que o Juiz pode autorizar ou ordenar, por despacho, a apreensão de mensagens de correio eletrónico ou registos de comunicações de natureza semelhantes,[182] armazenados num determinado sistema informático, que configurem grande interesse para a descoberta da verdade ou para a prova, no âmbito de uma pesquisa informática ou outro acesso legítimo, remetendo para o regime da apreensão de correspondência consagrado nos artigos 179.º e seguintes do CPP.

Este artigo não estabelece a diferença entre o correio eletrónico aberto/fechado e lido/não lido, o que tem gerado opiniões diversas na doutrina e jurisprudência. Por um lado, há quem entenda que, à semelhança da correspondência tradicional, também a correspondência eletrónica, após ser recebida e lida pelo seu destinatário, deve ser tratada como mero documento, estando sujeita ao regime geral das apreensões e, por isso, são considerados como dados informáticos e deixam de estar sob o crivo da proteção da correspondência e das telecomunicações, a apreensão realiza-se nos termos do artigo 16.º da LCib, não sendo necessária a intervenção do Juiz, bastando a intervenção do MP.[183] Por outro lado, certos autores defendem que o intuito do legislador foi o de conferir à correspondência eletrónica uma tutela mais garantística em relação à correspondência tradicional, para proteger a privacidade da autodeterminação informacional e, como tal, apenas o Juiz possui competência para autorizar ou ordenar a dita apreensão, nos termos do artigo 179.º do CPP *ex vi* artigo 17.º da LCib.[184]

Não pretendendo alongar-nos muito sobre esta temática, apenas referir que, na nossa opinião, toda esta controvérsia é fruto de um conjunto de confusões suscitadas pelo legislador que decidiu aplicar o regime das apreensões tradicionais à apreensão do correio eletrónico quando estes são fundamentalmente diferentes entre si. Dito isto, entendemos que a questão do correio eletrónico ou mensagens de natureza semelhante lido/não lido

---

[182] Os "registos de comunicações de natureza semelhante" correspondem às mensagens armazenadas em telemóveis, como as SMS, e às plataformas de mensagens, como o *Messenger* ou o *Whatsapp*.
[183] Concordam, CONDE CORREIA, *ob. cit.*, pp. 40 e 41, COSTA ANDRADE, *"Bruscamente no verão passado",* pp. 157-160. Na jurisprudência, o Acórdão do TRL de 22.04.2021, processo n.º 184/12, relator Fernando Estrela, disponível em www.dgsi.pt.
[184] Cfr. RITA CASTANHEIRA NEVES, *ob. cit.*, p. 275. Na jurisprudência, o Acórdão do TRL de 06.02.2018, processo n.º 1950/17, relator João Carrola, disponível em www.dgsi.pt.

como critério de apreensão não faz qualquer sentido, devido, precisamente, às características inerentes à comunicação eletrónica por ser muito difícil ou mesmo impossível determinar quando é que terminou a comunicação e se a mensagem já foi ou não aberta/lida. No entanto, não concluímos que a correspondência eletrónica não é merecedora de tutela de proteção da privacidade, pelo que é necessária a intervenção do Juiz, proferindo despacho a autorizar ou ordenar a apreensão, quando esta for relevante para a descoberta da verdade, aplicando parcialmente o n.º 1 do artigo 179.º do CPP.[185]

Coisa diferente é quem deve ser o primeiro a aceder ao conteúdo das mensagens em causa, sendo que o n.º 3 do artigo 179.º do CPP estabelece que deve ser o Juiz, mas, quando se trata correspondência eletrónica não é, de todo, viável, porque podem estar em causa dezenas ou centenas de mensagens e é preciso proceder à sua abertura, leitura e seleção para determinar quais as mensagens pertinentes para a investigação em curso. Portanto, como esta apreensão ocorre no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, deve ser o OPC ou o MP a ter o primeiro contacto com a correspondência apreendida por possuírem melhor conhecimento sobre a investigação.

[185] Indo de encontro ao Acórdão do TC n.º 403/2015, de 27.08.2015, processo n.º 773/15, relator Lino Rodrigues Ribeiro, que determinou que o âmbito da tutela da inviolabilidade da correspondência, ao abrigo do artigo 34.º da CRP, abrange as mensagens já entregues aos seus destinatários, disponível em www.tribunalconstitucional.pt.

7.1.6. Interceção de comunicações

O artigo 18.º da LCib prevê a interceção de comunicações informáticas,[186] transposição dos artigos 20.º e 21.º da Convenção sobre o Cibercrime, que corresponde à obtenção de dados de conteúdo de comunicações em tempo real e de dados de tráfego, quer seja correio eletrónico, SMS, conversações realizadas nas plataformas de mensagens como o *Messenger*, mas também as comunicações realizadas por VoIP, como o *Skype*.[187]

De acordo com o n.º 1, este meio de obtenção de prova é admissível relativamente aos crimes presentes na LCib (alínea a) e aos crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico quando estes estejam consagrados no artigo 187.º do CPP, remetendo assim para o regime das escutas telefónicas. Além disso, a interceção e o registo de transmissão de dados informáticos só podem ser autorizados durante o inquérito, ao abrigo do n.º 2, se for indispensável para a descoberta da verdade ou se a prova fosse impossível ou muito difícil de obter por outro meio, por despacho fundamentado do JIC e mediante requerimento do MP, sendo que, à luz do n.º 4, este despacho deve ainda conter o seu âmbito quando a interceção tiver como objeto o registo de dados de conteúdo ou de tráfego. Por fim, no n.º 4, o legislador dispôs que, em tudo o que não contrarie este artigo, aplica-se o regime dos artigos 187.º, 188.º e 189.º do CPP, configurando o artigo 18.º da LCib um regime especial. Como tal, a interceção de comunicações está sujeita às formalidades do regime das escutas telefónicas, de realçar, o prazo máximo de 72 horas para a autorização da interceção ser levada ao conhecimento do juiz do processo, bem como o prazo de três meses, renovável pelo mesmo período, da própria interceção, nos termos do n.º 3 e 6 do artigo 187.º *ex vi* o n.º 4 do artigo 18.º da LCib e que, segundo o artigo 188.º do CPP, o OPC pode realizar a interceção de comunicações, desde que lavre

[186] A definição de interceção encontra-se plasmada na alínea e) do artigo 2.º da LCib: «o ato destinado a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros».

[187] DUARTE RODRIGUES NUNES descreve o VoIP como «uma nova forma de comunicar "telefonicamente" através da *internet* mediante a utilização de um *software* específico, permitindo a comunicação sonora e imagética», sendo que «as palavras e imagens trocadas entre ambos são convertidas em sinal digital e esses dados são encriptados pelo sistema *Skype* ou outro», considerando o autor que a instalação do *software* é um ato que está incluído, por natureza, na autorização da realização das escutas, *Os Meios de Obtenção de Prova*, pp. 157 e 158. No mesmo sentido, PEDRO DIAS VENÂNCIO, *ob. cit.*, p. 119 e PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*, p. 544. CARLOS PINHO descreve mesmo a interceção de comunicações como o único meio especial de aquisição processual de dados de tráfego, *ob. cit.*, p. 78.

o devido auto e elabore um relatório e que obedeça aos restantes requisitos descritos neste artigo.[188]

Este meio de obtenção de prova é considerado bastante intrusivo e restritivo dos direitos fundamentais, especialmente porque se pode aceder a dados de conteúdo dos visados. Ainda assim, o Relatório Explicativo da Convenção sobre o Cibercrime indica que se trata de um meio com bastante utilidade numa investigação criminal, uma vez que as comunicações através de sistemas informáticos podem constituir prova de imensos crimes e, tendo em conta a capacidade da tecnologia de transmitir uma grande quantidade de dados em pouco tempo, sendo esses dados bastante voláteis, somente a sua interceção, em tempo real, permite descobrir a natureza ilegal destas comunicações e localizar o infrator mediante a descoberta do percurso da comunicação realizada. Aliás, o Relatório Explicativo utiliza a distribuição de pornografia infantil como caso paradigmático da relevância e eficácia da interceção de comunicações, pois este meio de obtenção de prova possibilita a descoberta dos detalhes das comunicações efetuadas entre o infrator e a vítima, como a data, hora e a origem e destino da comunicação, bem como do seu conteúdo, em tempo real, conseguindo assim descobrir não só o infrator como, a partir daí, até a identificação de outra vítimas ou ligações com cúmplices.[189]

Ademais, alguns autores reconduzem a aplicação das buscas *online* na segunda modalidade – em tempo real e de forma duradoura – a este regime da interceção de comunicações, tendo em conta que ambos são procedimentos igualmente intrusivos e ofensivos dos direitos fundamentais, devendo passar pelo escrutínio da competência do JIC e do princípio da proporcionalidade, ao abrigo do artigo 18.º, n.º 2, da CRP.[190] Esta modalidade já nos parece não ser admissível, pois existindo a alternativa menos intrusiva de uma busca *online* que é direcionada para aquele visado e para aqueles dados informáticos no âmbito da investigação, uma busca duradoura e não direcionada é tão atentadora dos direitos fundamentais do visado que é desconforme à nossa lei.

[188] PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*, p. 531.
[189] Cfr. Ponto 218 do Relatório Explicativo da Convenção sobre o Cibercrime.
[190] Neste sentido, DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova*, pp. 231 e 234.

7.1.7. Ações encobertas

O legislador português consagrou, no artigo 19.º da LCib, as ações encobertas enquanto meio de obtenção de prova digital, nos termos previstos na Lei n.º 101/2001, de 25 de agosto, na sequência do inquérito relativo aos crimes presentes na LCib, bem como os crimes cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, uma pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior e, sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos.[191] Existem dois tipos de ação encoberta no nosso ordenamento jurídico: a chamada "clássica" porque é realizada por infiltração de polícia ou de uma pessoa que não pertença a um OPC, mas que esteja a atuar sob a sua direção, prevista na Lei n.º 101/2001, e a realizada em ambiente digital que não implica a infiltração física, apenas no mundo digital, consagrada na LCib. De qualquer modo, ambas as modalidades implicam a existência de um agente encoberto que tenta obter provas concretas para investigação criminal, sem nunca revelar a sua identidade.

Na doutrina, faz-se a distinção entre agente encoberto, agente infiltrado e agente provocador.[192] Em ambiente digital, a função do agente encoberto consiste em frequentar os diversos sítios da *internet*, inclusive a *DarkWeb*, tais como *sites*, *chats* e outros locais que podem ser acessíveis ao público ou de acesso reservado, que pode, dependendo dos casos, necessitar do consentimento dos seus participantes, utilizando um *nickname*, por exemplo, para ocultar a sua verdadeira identidade. DUARTE RODRIGUES NUNES exemplifica, no caso de pornografia infantil, o agente encoberto poderá criar uma página

---

[191] A definição de ações encobertas encontra-se prevista no n.º 2 do artigo 1.º da Lei n.º 101/2001 como «aquelas que sejam desenvolvidas por funcionário de investigação criminal ou por terceiro atuando sob o controlo da PJ para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade», disponível em www.pgdlisboa.pt.
Não se encontram previstas as ações encobertas na Convenção sobre o Cibercrime, pelo que o legislador português consagrou este meio de obtenção de prova por lhe reconhecer uma grande importância na recolha de prova digital, tal como o ordenamento jurídico espanhol que prevê o *agente encubierto informático*, à luz do artigo 282, bis, 6 e 7 do LEC, assim como o direito alemão, de acordo com o artigo §110 do StPO, e no direito francês nos artigos 706-81 a 706-87 do *Code de Procédure Pénale*.

[192] O agente infiltrado é admissível à luz da Lei n.º 101/2001, assim como uma quarta definição que se reporta à figura do "homem de confiança", isto é, o sujeito que não é OPC, mas que atua sob o seu controlo, que não é tão relevante abordar no âmbito da luta contra a proliferação da pornografia infantil. Cfr. PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*, p. 68 e COSTA ANDRADE, *Sobre as Proibições de Prova*, p. 233.

de *internet* para identificar os suspeitos da prática deste crime sem nunca se identificar ou divulgar quaisquer dados sobre si.[193] Em relação ao agente infiltrado, este já tem um papel mais insidioso do que o agente encoberto, uma vez que a sua atuação implica que este se insira no meio criminoso, de forma prolongada, através de uma identidade fictícia, ganhando a confiança dos seus participantes, sendo ativo nos locais determinados da *internet* que está a investigar,[194] podendo até praticar atos preparatórios ou de execução, se assim for necessário, mas nunca incentivando à prática de crimes.[195] Por sua vez, o agente provocador incentiva um determinado sujeito à prática de crimes com a intenção de o sujeitar a um processo criminal, frequentando o mundo digital com esse objetivo, algo que, sem esse seu incentivo, nunca aconteceria, podendo atuar como mero instigador ou mesmo como autor mediato.

Tendo em conta as diferenças existentes entre estas modalidades, há certos autores que entendem que apenas a figura de agente infiltrado se pode reconduzir ao regime das ações encobertas do artigo 19.º da LCib, sendo que o agente encoberto é admissível como meio de obtenção de prova atípico, nos termos do artigo 125.º do CPP.[196] Pelo contrário, existe quem critique a distinção entre as figuras do agente encoberto e do agente infiltrado por considerar que adiciona confusão ao regime, mas distingue em relação ao agente provocador.[197]

A ação encoberta deve obedecer a certas formalidades previstas na Lei n.º 101/2001, tais como, a dependência da prévia autorização pelo MP, sendo comunicada ao JIC no prazo máximo de 72 horas, ou da autorização do JIC, sob proposta do MP, nos termos do artigo 3.º. Além disso, a identidade fictícia é atribuída aos agentes da polícia criminal por despacho do Ministro da Justiça, mediante proposta do Diretor Nacional da PJ, possuindo a validade de 6 meses prorrogáveis por períodos de igual duração, nos termos do artigo 5.º.

Concordamos com FREDERICO PELLUCCI quando critica a solução de remeter o regime das ações encobertas *online* para o das ações encobertas clássicas, «já que uma

---

[193] Cfr. DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova*, p. 440.
[194] Recorrentemente, de forma a poder pertencer à comunidade *online* de partilha de material pornográfico envolvendo menores, no seguimento da ação encoberta, o agente vê-se confrontado com a necessidade do envio prévio deste tipo de conteúdo. Contra, FREDERICO PELLUCCI, "A Atuação dos Agentes Encobertos e Infiltrados nos Canais Abertos e Fechados de Comunicação em Ambiente Informático-Digital", *Novos desafios da prova penal*, 2020, p. 268 e 269.
[195] *Vide* artigo 6.º, n.º 1 da Lei n.º 101/2001 quanto à impunibilidade da conduta do agente encoberto que pratique atos preparatórios ou de execução, desde que atue respeitando o princípio da proporcionalidade.
[196] Neste sentido, DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova*, pp. 201e 202 e FREDERICO PELLUCCI, *ob. cit.*, pp. 260-263.
[197] DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal*, pp. 289-292.

regulamentação autónoma, que deixasse patente a diferença entre a obtenção das provas nas duas realidades intrinsecamente distintas, daria muito mais segurança ao trabalho investigativo, principalmente na atual sociedade informatizada».[198]

De acordo com o n.º 2 do artigo 19.º da LCib, quando for necessário recorrer a meios e dispositivos informáticos, aplicam-se as regras previstas para a interceção de comunicações, com as devidas adaptações, de modo a agilizar a recolha dos dados pertinentes para o processo penal na sequência da ação encoberta relativamente aos conteúdos com que se deparam na *internet*. Face à expressão «sendo necessário o recurso a meios e dispositivos informáticos», tem-se vindo a colocar a hipótese de abranger o chamado uso de *malware*.[199]

O uso de *malware* implica a utilização de meios técnicos e a instalação sub-reptícia em determinado sistema informático de certos programas informáticos que permitem esta infiltração – por exemplo, programas do tipo "Cavalo de Tróia",[200] mas também vírus, *spyware*, entre outros.[201] Portanto, o uso de *malware* corresponde à instalação destes programas de modo a «comprometer as suas funções, contornar os seus controlos de acesso, causar prejuízo ao seu utilizador ou ao sistema informático, monitorizar a sua atividade ou apropriar-se, corromper, eliminar e/ou alterar dados informáticos».[202] Este meio de obtenção de prova digital é particularmente insidioso e restritivo dos direitos fundamentais do visado, porque permite o acesso aos dados informáticos armazenados, bem como dos dados em tempo real e os dados armazenados temporariamente, em particular. Por este motivo, deve sempre ser encarado como uma

---

[198] FREDERICO PELLUCCI, *ob. cit.*, p. 248.

[199] DAVID SILVA RAMALHO opta por rejeitar o conceito de busca *online* por não se tratar de uma verdadeira busca e devido à instalação de *malware* e a recolha de informação por ele permitido não ocorrer *online*, utilizando sempre o termo *malware*, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, pp. 315-318. No entanto, seguimos o entendimento de DUARTE RODRIGUES NUNES ao afirmar que este é um ato preparatório de uma busca *online* ou de uma interceção de comunicações, porque em ambas não está implícito o uso de *malware*, é somente uma das maneiras, "Da Admissibilidade da utilização de *benware* no Direito Português", pp. 15 e 16. PAULO DÁ MESQUITA critica o legislador por criar uma norma tão ampla, *ob. cit.*, p. 127.

[200] No direito italiano prevê-se o uso do *captatore informatico*, um software do tipo "Cavalo de Tróia" como meio de interceção de comunicações nos casos admissíveis, de acordo com o artigo 614 do *Codice Penale.*

[201] DUARTE RODRIGUES NUNES, "Da Admissibilidade da utilização de *benware* no Direito Português", CyberLaw by CIJIC, 2020, p. 13, PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*, p. 502 e COSTA ANDRADE, "*Bruscamente no Verão Passado"*, p. 166.
Definições destes conceitos detalhados em DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, pp. 319-322.

[202] DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, p. 319. Definição de *malware* presente no *Eletronic Evidence Guide* do Conselho da Europa, p. 187.

medida a título excecional e necessária, autorizada pelo JIC mediante requerimento do MP, de acordo com o artigo 18.º, n.º 2, *ex vi* o artigo 19.º, n.º 2, da LCib.[203]

Este método já demonstrou ser bastante eficaz na luta contra a difusão de pornografia infantil na *DarkWeb* – por exemplo, na operação *Darknet* realizada pelo grupo *Anonymous* que desmantelou um fornecedor de serviços, *Freedom Hosting*, que tinha essa finalidade -,[204] pelo que nos revemos na denominação de alguns autores, como DUARTE RODRIGUES NUNES, de *benware*, isto é, o recurso a *software* que seja benigno para a investigação criminal.[205] Por este motivo, seria de extrema importância a sua previsão no nosso ordenamento jurídico que, a nosso ver, não é admissível à luz do artigo 19.º, n.º 2, da LCib porque não nos caber na *ratio* da norma, mas também porque necessita de consagração expressa devido à sua danosidade implícita dos direitos fundamentais.

[203] DAVID SILVA RAMALHO retira da letra da lei que o uso de *malware* apenas deve ser admitido no contexto das ações encobertas, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, pp. 354-346. Novamente, concordamos com DUARTE RODRIGUES NUNES que defende que pode ser utilizado noutros meios de obtenção de prova, como a interceção de comunicações, "Da Admissibilidade da utilização de *benware* no Direito Português", pp. 31-33.
[204] Cfr. DAVID SILVA RAMALHO, "Investigação Criminal na *Dark Web*", pp. 383 e 384.
[205] DUARTE RODRIGUES NUNES, "Da Admissibilidade da utilização de benware no Direito Português", p. 14.

7.1.8. Cooperação internacional

Recordando que uma das características da prova digital é a sua transnacionalidade, a LCib consagra medidas específicas relativamente à cooperação internacional no âmbito da obtenção de prova digital nos seus artigos 20.º a 35.º, uma transposição dos artigos 23.º a 25.º da Convenção sobre o Cibercrime.

O Relatório Explicativo da Convenção sobre o Cibercrime explicita que a cooperação internacional deve funcionar para efeitos de investigação ou de procedimentos relativos a infrações penais relacionadas com sistemas e dados informáticos ou para a recolha de prova digital sempre que estes dados se encontrem em território estrangeiro, baseando-se no auxílio mútuo entre os Estados em matéria de medidas cautelares mediante a elaboração de um pedido de acesso a esses dados.[206] Desde logo, o artigo 20.º da LCib estabelece que as autoridades nacionais competentes devem cooperar com as autoridades estrangeiras competentes para efeitos de investigação ou procedimentos relativos a crimes relacionados com sistemas ou dados informáticos e da recolha de prova de um crime, em suporte eletrónico, remetendo para as normas sobre transferência de dados pessoais previstas na Lei n.º 59/2019, de 8.08. Em relação às medidas previstas na LCib, encontra-se prevista a possibilidade de proceder à preservação e revelação expeditas de dados informáticos em Portugal, bem como ao acesso a dados informáticos e a interceção de comunicações e respetiva reprodução, nos termos dos artigos 22.º, 24.º, 25.º e 26.º da LCib.[207]

Contudo, a nosso ver, a medida mais inovadora e eficaz prevista na LCib corresponde à criação do ponto de contacto permanente para efeitos de cooperação internacional, isto é, a Rede 24/7 da PJ, definido no n.º 1 do artigo 21.º, transposição da Decisão-Quadro n.º 2005/222/JAI do Conselho, de 24.02, pois promove a prestação de assistência imediata e permanente no combate à prática de crimes em ambiente digital

[206] Cfr. Pontos 242 e seguintes do Relatório Explicativo da Convenção sobre o Cibercrime. Existem apenas duas situações em que um Estado pode aceder unilateralmente a dados informáticos que se encontram noutro território que são as determinadas no artigo 32.º da Convenção sobre o Cibercrime, isto é, o acesso a dados informáticos acessíveis ao público e se existir consentimento legal e voluntário da pessoa com legitimidade para divulgar esses dados através do sistema informático.

[207] Com base no regime previsto na LCib, pode concluir-se que o acesso transfronteiriço não constitui qualquer proibição de prova, nos termos do n.º 3 do artigo 126.º do CPP. Porém, DAVID SILVA RAMALHO questiona-se sobre a validade da recolha de prova diretamente de Estado terceiro para subsequente envio para Portugal – que corresponde a uma carta rogatória, à luz da alínea b) do n.º 3 do artigo 111.º do CPP – e acaba por concluir que o Estado português não possui competência para realizar diretamente a recolha de prova a partir de território estrangeiro, sendo que essa prova é proibida, *Métodos Ocultos de Investigação Criminal*, pp. 87-91.

entre vários pontos de contacto, nos termos do n.º 2. No caso de pedido de cooperação, a assistência imediata é prestada de acordo com o n.º 3, sendo que quando se trate da preservação expedita de dados, da recolha de prova ou da localização de suspeitos e prestação de informações de caráter jurídico, a PJ dá notícia e remete relatório imediatamente para o MP, ao abrigo do artigo 253.º do CPP, e, por sua vez, de modo a responder prontamente a estes pedidos, o MP assegura a disponibilidade de Magistrados e meios técnicos, como estabelece o n.º 5.

Além disso, em Portugal, a PGR elaborou protocolos de cooperação internacional no âmbito da investigação da cibercriminalidade e da obtenção de prova digital, pretendendo agilizar o procedimento dos pedidos de dados aos fornecedores de serviços. Esses protocolos são compostos por um conjunto de formulários elaborados para simplificar e acelerar os pedidos de colaboração do MP aos fornecedores de serviços, sejam pedidos de preservação de dados ou pedidos de informação, por exemplo, na sequência de uma injunção do artigo 14.º da LCib. Se o fornecedor de serviço se encontrar em território nacional, como a MEO ou a NOS, utilizam-se os formulários disponíveis no SIMP que são enviados por correio ou *e-mail*.[208] Mas, se o fornecedor se encontrar no estrangeiro, tendo em conta que o pedido de cooperação internacional pode tornar-se muito moroso,[209] especialmente nos EUA onde se encontra a maioria, a PGR criou protocolos com os fornecedores mais utilizados - como a *Microsoft*, o *Google*, o *Facebook* – através dos quais o MP solicita determinados dados sobre um titular de uma conta destes serviços, de modo muito mais eficiente.[210]

---

[208] Como consagrou a Circular n.º 12/2012, de 25.09.2012 da PGR disponível em https://www.ministeriopublico.pt/iframe/circulares e os ditos formulários estão disponíveis no sistema do SIMP.

[209] Este pedido é realizado por carta rogatória, nos termos do artigo 21.º da LCib e dos artigos 145.º e seguintes da Lei n.º 144/99, de 31.08, a Lei da Cooperação Judiciária Internacional em Matéria Penal, disponível em www.pgdlisboa.pt.

[210] As Notas Práticas n.º 3/2014, de 12.06, e 4/2014, de 22.12, do Gabinete do Cibercrime do MP concretizam esta cooperação sem recurso a carta rogatória, ou seja, uma cooperação "informal", cujos formulários também se encontram disponíveis no *site* do SIMP. Nem todos os fornecedores de serviços permitem o recurso a esta cooperação "informal", exigindo que o pedido seja realizado através do procedimento de cooperação judiciária internacional, como o *Yahoo!* e o *Twitter*, exceto quando se tratem de situações urgentes, funcionam como os restantes fornecedores que dispõem de canais mais expeditos, utilizando a Rede 24/7 como ponto de contacto através do seu endereço de *e-mail*. Especificamente em relação ao *Google* e à *Microsoft, vide* Notas Práticas n.º 14/2019, de 20.12, e n.º 21/2021, de 15.01, do Gabinete do Cibercrime, respetivamente.
ÂNGELA PINTO alerta, ainda, para o facto de certos países, como os EUA, não preverem um período de armazenamento de dados, pelo que a prática generalizada desse país é armazenar os dados pelo período de 90 dias, pelo que o pedido de informação deve ser realizado atempadamente, sob pena do MP já não poder ter acesso aos dados informáticos que pretende para a investigação em curso *ob. cit.*, p. 125.

8. As especificidades da *DarkWeb*

Atendendo a todas as noções e características inerentes à prova digital, acresce o conceito de *DarkWeb*, uma realidade cada vez mais comum na cibercriminalidade. Ora, a *internet* pode apresentar-se sob duas formas distintas: a *Surface Web* e a *Deep Web*, sendo que a primeira corresponde à *internet* acessível a todos através de motores de busca como o *Google* ou o *Yahoo!*, e a partir dos quais temos acesso ao conjunto de páginas que compõem a *Web*, enquanto a segunda consiste no conjunto de páginas não indexadas, ou seja, não acessíveis pelos normais motores de busca, permitindo a quem possui conhecimentos sobre o procedimento de navegação aceder às mesmas. A *Deep Web* é, ainda, composta por três camadas: na primeira camada estão presentes os *sites* não indexados, cujo acesso exige a pré-existência de credenciais; na segunda camada encontram-se os *sites* não indexados e encriptados, tendo acesso restrito; e na última camada, o acesso aos *sites* implica a existência de registo e palavra-passe.[211] À medida que se vai aprofundando as camadas da *Deep Web*, maior é o grau de anonimato e encriptação.

Contudo, com o desenvolvimento tecnológico, surgiram camadas ainda mais profundas na *Deep Web*, a chamada *DarkWeb*, que corresponde à *internet* que somente pode ser acedida mediante a instalação de um *software* por parte do utilizador em conjugação com a exigência de determinadas autorizações dentro da própria rede.[212] Neste enquadramento, surge o conceito de *Darknet* que consiste numa «rede virtual estabelecida entre vários utilizadores, inacessível a terceiros e que funciona através de uma rede de telecomunicações pública, neste caso a *internet*, que visa a partilha de informações e ficheiros em formato digital sem, contudo, permitir que, quer os endereços de IP dos seus membros, quer o teor das comunicações entre si estabelecidas, possam ser descobertos».[213]

---

[211] A *Deep Web* foi criada pelos EUA na década de 90 com o intuito dos membros da Marinha poderem comunicar sem interceções de terceiros, logo a ideia era a existência de um local *online* no qual as mensagens surgiam cifradas, mas rapidamente começou a ser utilizada para outros fins, nomeadamente para a prática de atos ilícitos, sendo atualmente um grande meio para a cibercriminalidade, ELIANA PEREIRA, "Crime de Abuso Sexual de Menores com Recurso à Internet – Darknet – Os desafios da investigação", *Trabalhos Temáticos de Direito e Processo Penal, Volume I*, CEJ 2016, pp. 164 e 165 e DAVID SILVA RAMALHO, "A investigação criminal na *Dark Web*", *Revista da Concorrência e Regulação*, Ano IV, n.º 14/15, Abril/Setembro 2013, pp. 385 e 386

[212] DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova*, p. 39 e Conselho da Europa, *Eletronic Evidence Guide*, pp. 110.

[213] DAVID SILVA RAMALHO distingue entre *Dark Web* e *Darknet*, "A investigação criminal na *Dark Web*", p. 394. Pelo contrário, o Conselho da Europa não distingue estes conceitos, assumindo-os como sinónimos, e explicita a grande diferença entre a *Deep Web* e a *Darknet*, *Eletronic Evidence Guide*, p. 111.

Além disso, o *software* mais comum para a prática de atos ilícitos na *DarkWeb* é o *Tor*, pois corresponde a um sistema que impede a interceção de comunicações e do seu conteúdo, assim como a determinação da sua origem e do seu destinatário por terceiros. O *Tor* é um sistema que permite, assim, a anonimização das comunicações, baseando-se num complexo sistema através do qual os dados em tráfego se encontram encapsulados em camadas de encriptação e são transmitidos entre um conjunto de elos de ligação (*nodes*) até chegar ao destinatário final, onde aparecem desencriptados.[214] Isto é, «conecta-se a diversos distribuidores de conexão que criptografam e recriptografam as informações».[215] DAVID SILVA RAMALHO explica que «um dado utilizador que queira aceder a um *website* através do *Tor*, liga-se automaticamente à rede de retransmissores *Tor* e esta cria um "túnel" que transporta aleatoriamente a comunicação através da rede *Tor* até ao seu destinatário final - daí que, quanto maior o número de utilizadores, mais difícil será a identificação de cada um» e quando «a comunicação finalmente atinge o portal de saída do "túnel", isto é, quando a comunicação parte do último retransmissor da rede *Tor* (o chamado *exit node*) para o fornecedor de serviço, encontrar-se-á já desprovida de qualquer camada de cifragem».[216] A grande vantagem da comunicação via *Tor* é o facto de cada elo de ligação apenas conhecer o elo de ligação imediatamente anterior e posterior, impedindo descobrir o trajeto da comunicação efetuada, de onde partiu e para onde vai. Resumidamente, o processamento da comunicação do *Tor* permite a dissimulação da identificação do endereço IP dos seus utilizadores, bem como do conteúdo transmitido, dando azo a comunicações praticamente impercetíveis.

Deste modo, o uso da *DarkWeb* é muito atrativo para a cibercriminalidade, uma vez que permite o completo anonimato, inclusive do próprio IP dos seus utilizadores, dificultando bastante a obtenção de prova digital por parte das autoridades judiciárias, como é o caso dos grupos existentes para a partilha de conteúdo pedopornográfico, composto por indivíduos de todo o mundo, que ali se juntam de forma anónima para aquele fim, comunicando livremente através de uma rede de partilha exclusiva e "escapando", assim, à alçada das autoridades.[217]

Aqui distinguimos os conceitos, mas acabamos por nos referir, de forma geral, apenas a *DarkWeb* por razões sistemáticas.

[214] Camadas estas que se assemelham às de uma cebola, daí o nome *Tor*, que significa *The Onion Routing*.

[215] DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova*, p. 39.

[216] DAVID SILVA RAMALHO, "A investigação criminal na *Dark Web*", p. 391.

[217] *Ibid.* No mesmo sentido, ELIANA PINTO, *ob. cit.*, p. 158.

IV. Dificuldades de obtenção e valoração de prova digital no crime de pornografia de menores

Analisadas as questões relativas ao crime de pornografia de menores e da prova digital, reunimos aqui condições para examinar as dificuldades de obtenção e valoração de prova digital no crime de pornografia de menores, relacionando com o que foi abordado acima.

JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO afirmam, acertadamente, que a característica mais prejudicial da transferência do crime de pornografia de menores para o mundo digital tem que ver com «a tutela da imagem do menor, que se vê gravemente afetada, atento o elevado grau de disseminação e a quase impossibilidade prática de apagar totalmente o "rasto" digital na *internet*».[218] Assim, os grandes objetivos da investigação criminal serão a identificação das vítimas, a cessação da prática dos atos ilícitos, a perseguição criminal dos agentes do crime e a repressão da divulgação de conteúdo pedopornográfico.[219]

Efetivamente, os avanços tecnológicos revelaram-se muito propícios para a perpetuação deste tipo de criminalidade que, através da *internet*, mas especialmente da *DarkWeb*, é facilmente difundido globalmente, com a agravante da capacidade de comunicar quase sem possibilidade de deteção, por isso, é dificultada a tarefa de identificar e localizar os agressores. Ademais, o combate à pedopornografia é uma das grandes prioridades das autoridades judiciárias por todo o mundo, mas defronta-se com um grande obstáculo: a tecnologia desenvolve-se a uma velocidade tal que os ordenamentos jurídicos não conseguem atualizar-se atempadamente. Por isso, deparamo-nos com a insuficiência dos regimes, assim como a falta de especialização e de recursos das autoridades policiais e judiciárias.

Ora vejamos as principais dificuldades da investigação criminal na obtenção e valoração de prova digital no crime de pornografia de menores.

[218] JOSÉ MOURAZ LOPES e TIAGO CAIADO MILHEIRO, *ob. cit.*, p. 267.
[219] Cfr. ELIANA PEREIRA, *ob. cit.*, p. 167 e ANA PAULA RODRIGUES, *ob. cit.*, pp. 275 e 276.

9. A identificação dos agressores e da vítima e da sua idade

Uma das grandes dificuldades atinentes à prática do crime de pornografia de menores na *internet* prende-se com a identificação e idade da vítima, assim como da identificação dos seus agressores. Relativamente aos agressores, a questão relaciona-se com as características da prova digital, que dificultam a sua identificação e localização. Quanto à vítima, as autoridades judiciárias deparam-se, muitas vezes, somente com imagens ou vídeos de crianças, sem qualquer tipo de contexto, ou seja, desconhecendo a sua identidade, a sua idade, a sua localização, mas também se o conteúdo pedopornográfico é atual ou não (e se já não se tratará de um menor à data da recolha do material) e se a criança em causa já se encontra sinalizada como vítima.

No que diz respeito à identificação dos agressores, o ordenamento jurídico português dispõe de legislação expressa, a Lei n.º 103/2015, de 24.08, que corresponde à transposição da Diretiva n.º 2011/93/UE, de 13.12.2011, e criou um sistema de registo de identificação criminal de condenados pela prática de crimes contra a autodeterminação sexual e a liberdade sexual do menor.[220] Estas normas permitem facilitar a investigação criminal relativamente à identidade dos agressores sexuais portugueses ou não nacionais residentes em território nacional. Contrariamente aos EUA, o acesso a esta base de dados não é público, sendo apenas permitida às entidades estipuladas no artigo 16.º da Lei.[221]

Em relação à descoberta da idade do menor, esta é extremamente importante para se perceber se o agente do crime verá a sua pena agravada em razão da idade do menor afetado, de acordo com os critérios dos n.º 6 e 7 do artigo 177.º do CP.[222] Naturalmente, a idade relevante corresponde à idade do menor à data da consumação do crime. Este apuramento da idade é difícil, pois a maioria das vezes não se possui a identificação da criança, logo as autoridades judiciárias recorrem à opinião de peritos do INMLCF, nos termos dos artigos 151.º e seguintes do CPP, que realizam um juízo sobre a idade provável

[220] Discordando do regime estabelecido na Lei por implicar graves consequências aos condenados, como a obrigação da inscrição numa base de dados e as obrigações que daí advêm, PAULO DUARTE TEIXEIRA, "A (R)evolução Silenciosa do Sistema Penal Português", *Revista Julgar*, n.º 33, 2017, pp. 193-197. Porém, esta opção legislativa portuguesa vai ao encontro da jurisprudência do TEDH que considera que a obrigação de inscrição numa base de dados, ainda que por muitos anos, não comina numa violação dos artigos 7.º e 8.º da CEDH, como no Acórdão Gardel v. France de 17.03.2010, disponível em www.hudoc.echr.coe.int.

[221] O FBI em parceria com o *Department of Justice* disponibilizam publicamente a base de dados dos agressores sexuais, informando sobre a sua identidade e localização. Esta informação encontra-se disponível em https://www.fbi.gov/scams-and-safety/sex-offender-registry.

[222] No entanto, o Acórdão do TRE de 17.03.2015 processo n.º 524/13.0JDLSB.E1, relator Carlos Jorge Berguete, estabelece que a concreta identificação de vítimas não constitui elemento do tipo quando estiver em causa a mera detenção e/ou a divulgação de material pedopornográfico, desde que sejam menores de idade, disponível em www.dgsi.pt.

da criança presente no conteúdo pedopornográfico em questão. Contudo, esta prova pericial pode ser inconclusiva ou mesmo errada, por exemplo, nos casos em que os menores aparentam ter mais ou menos idade do que realmente possuem, o que significa que não é uma prova exatamente fidedigna e, consequentemente, podendo sempre invocar-se o princípio *in dubio pro reo* quando não se consiga comprovar a idade concreta.[223] Ademais, a dificuldade da identificação da idade é acrescida nas situações de criminalização por representação realista aparente de menor, uma vez que se tratam de pessoas maiores de idade com aspeto de menor, o que torna esta tarefa ainda mais árdua e equívoca.

Na tentativa de dirimir as dificuldades na identificação da vítima e de agilizar o reconhecimento de crianças sujeitas a prévios abusos pelas autoridades judiciárias, surgiram várias ferramentas, especialmente internacionais, baseadas na ideia de cooperação, que têm demonstrado bons resultados. A Interpol criou uma base de dados de imagens que configuram situações de exploração sexual de crianças - o *International Child Sexual Exploitation database* (ICSE) – com a finalidade de facilitar a identificação destas crianças e da sua localização mediante a utilização de um *software* que permite aos investigadores especializados de todo o mundo comunicar entre si e partilhar conteúdo de forma a evitar a duplicação de esforços e, assim, tornar a investigação bastante mais eficaz.[224] Igualmente, a Europol tem vindo a criar várias *taskforces – Europol's Victim Identification Taskforce* (VIDTF) - com o mesmo objetivo de identificar crianças utilizadas em conteúdo pedopornográfico (e os seus agressores) através da parceria de especialistas de vários países.[225] Nesta senda, é também de realçar o trabalho do *National Center for Missing & Exploited Children* (NCMEC), uma organização não lucrativa, localizada nos EUA, que se dedica a encontrar crianças desaparecidas e a prevenir a sua exploração sexual, que trabalha diretamente com as autoridades policiais americanas, que rapidamente contactam as autoridades dos países onde ocorra uma situação de risco.[226] Esta tarefa tem sido ainda mais dificultada pelo recurso aos *sites* de *streaming* e da *DarkWeb* para consumo ou divulgação de pornografia de menores.

---

[223] Cfr. INÊS FERREIRA LEITE, "A tutela penal da liberdade sexual", p. 58 e ANA PAULA RODRIGUES, *ob. cit.*, p. 276.

[224] Segundo o *site* da Interpol, esta base de dados já ajudou a identificar 27.733 crianças globalmente, mas também os seus agressores, disponível em https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database.

[225] Disponível em https://www.europol.europa.eu/media-press/newsroom/news/global-europol-taskforce-identifies-18-child-victims-of-sexual-abuse#:~:text=The%20VIDTF%20is%20a%20Europol,in%20child%20sexual%20abuse%20material.

[226] Disponível em https://www.missingkids.org/HOME

Até à data, Portugal não prevê legislação expressa relativamente à identificação da vítima criança e da sua idade, mas tem sido complacente nas operações internacionais. No entanto, em 2021, criou um Protocolo de procedimentos de atuação destinado à prevenção, deteção e proteção de crianças vítimas de tráfico de seres humanos, que inclui o tráfico para fins de exploração sexual, nomeadamente a produção, promoção e distribuição de pornografia que envolva crianças, bem como o seu uso em espetáculos de sexo.[227]

A nosso ver, este Protocolo constitui uma grande evolução no sentido das nossas autoridades judiciárias tomarem um papel mais ativo na luta contra esta criminalidade, caminhando gradualmente para entidades mais competentes e para uma investigação mais eficiente.

[227] Este Protocolo também se pronuncia sobre os procedimentos para a aferição da idade da criança, determinando que a realização dos exames periciais não deve ser uma diligência obrigatória, devendo dar-se primazia a outros mecanismos, como as declarações da criança ou, se possível, dos seus documentos, sempre protegendo ao máximo os direitos da criança, disponível em https://www.cig.gov.pt/wp-content/uploads/2021/05/TSH_Book_M06.pdf.

10. A ineficácia dos meios de obtenção de prova previstos na LCib face às especificidades da *DarkWeb*

O crime de pornografia de menores representa um dos grandes desafios mundiais da investigação criminal, sendo muito complicado a obtenção de prova, especialmente quando se trata de grandes redes de distribuição de material pedopornográfico, uma vez que tanto os produtores como os consumidores comunicam entre si essencialmente através da *DarkWeb*.[228] Assim, os meios de obtenção de prova digital previstos na LCib nem sempre serão eficazes na obtenção desta prova nem no combate a este tipo de criminalidade. Ora vejamos.

Relativamente à preservação e revelação expeditas de dados, consagradas nos artigos 12.º e 13.º da LCib, revelam-se pouco eficazes quando o crime ocorre com recurso à *DarkWeb*, porque este método de obtenção de prova consiste na preservação e revelação por parte dos fornecedores de serviços dos dados de tráfego referentes a um determinado cliente e a uma dada comunicação. Contudo, na *DarkWeb*, nomeadamente num sistema como o *Tor*, é praticamente impossível obter estas informações, visto que a intenção é mesmo impedir que estes dados sejam descobertos e, mais importante, que o trajeto da comunicação realizada seja revelado. Além disso, também é muito comum a informação encontrar-se encriptada, sendo constantemente modificada na sua transmissão entre os diferentes utilizadores, pelo que o acesso aos dados de tráfego pelas autoridades pode traduzir-se numa mera revelação da hora a que um sistema informático se conectou a outros sistemas.[229] Por estes motivos, a investigação criminal na *DarkWeb* recorrendo a estes métodos de obtenção de prova revela ter pouca utilidade perante os obstáculos que apresentam, podendo as autoridades não obter qualquer informação.

Quanto à injunção para apresentação ou concessão do acesso a dados, presente no artigo 14.º da LCib, de forma semelhante, corresponde a um método de obtenção de prova digital pouco eficaz quando o agente do crime recorre à *DarkWeb*. Ademais, se a injunção for ordenada ao fornecedor de serviço que o agente do crime utilizou, nos termos do n.º

[228] Um exemplo notório da complexidade da redes de pornografia de menores, que contou com a participação de Portugal, corresponde ao caso *Wonderland*, cuja rede era composta por um presidente, um secretário e um comité executivo, assim como o seu acesso era muito exclusivo. Além disso, continha muita informação encriptada que as autoridades nunca conseguiram desvendar por completo. Cfr. INÊS FERREIRA LEITE, *Pedofilia*, pp. 15 e 16 e MANUEL MAGRIÇO, *A Exploração Sexual de Crianças no Ciberespaço - Aquisição e Valoração de Prova Forense de Natureza Digital*, 2013 pp. 5 e 6.

[229] Como nos explica DAVID SILVA RAMALHO, "A investigação criminal na *Dark Web*", pp. 398 e 399, mas também ELIANA PEREIRA, *ob. cit.*, p. 170 e DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova*, pp. 82 e 83.

1, é improvável que as autoridades venham a descobrir o local de armazenamento do conteúdo ilícito, a não ser que tenham acesso aos dados de conteúdo por terem sido transmitidos para o fornecedor de serviço, o que não acontece porque estes dados são, usualmente, transmitidos diretamente entre os utilizadores da *DarkWeb*, sem nunca passar pelo fornecedor de serviço. Por outro lado, se a injunção for apresentada nos termos do n.º 4, em que se obriga o fornecedor de serviço a revelar os dados de base e de localização relativos a um determinado cliente ou assinante que recorreu à *DarkWeb*, implica que terá de se conhecer o sistema informático a partir do qual se efetuou o acesso e a consequente comunicação, o que não é presumível que aconteça quando se recorre a estes meios. Por último, se a injunção for ordenada ao administrador da rede informática a que o suspeito recorreu para aceder à *DarkWeb*, só terá relevância se se souber a sua identificação, assim como da origem da comunicação, que também não é provável. Se o agente do crime utilizar o *Tor*, acontece precisamente o que referimos a propósito da preservação e revelação expeditas de dados, visto que pretende exatamente prejudicar o rastreamento da comunicação.[230] Como explicita DAVID SILVA RAMALHO, este meio de obtenção de prova apenas poderá ter sucesso se o visado for descuidado na sua navegação na *DarkWeb*, por exemplo, se tiver procedido ao *download* de ficheiros com conteúdo pedopornográfico, sem ter efetuado a cifragem ou não tenha eliminado os dados após a utilização.[231]

A propósito da pesquisa e apreensão de dados informáticos e da apreensão de correio eletrónico e registo de comunicações de natureza semelhante, ao abrigo dos artigos 15.º a 17.º da LCib, exige-se novamente que as autoridades possuam conhecimento sobre o sistema informático onde se encontram armazenados os dados e a partir do qual se acedeu à *DarkWeb* para que a recolha de prova digital seja eficaz.[232] Do mesmo modo, muitas vezes pressupõe a obtenção de credenciais de acesso aos *websites* não publicamente acessíveis ou à *DarkWeb*, ou seja, do nome de utilizador e a palavra-passe, que apenas ocorre se o investigador tiver a sorte destas serem divulgadas ou as

[230] Cfr. DAVID SILVA RAMALHO, "A investigação criminal na *Dark Web*", pp. 400 e 401, ELIANA PEREIRA, *ob. cit.*, p. 171 e DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova*, pp. 116 e 117.

[231] *Ibid.*

[232] Portanto, implica que as autoridades tenham recorrido a outros métodos de obtenção de prova digital, previamente, tais como, uma ação encoberta ou de uma busca *online*, ou então da imprudência do suspeito, DAVID SILVA RAMALHO, "A investigação criminal na *Dark Web*", p. 402. DUARTE RODRIGUES NUNES relembra que a pesquisa de dados informáticos presencial é dificilmente eficaz nas situações em que se recorra à *DarkWeb* devido à exigência de se conhecer a localização do sistema informático utilizado, mas a busca *online* já demonstra ser eficaz, *Os Meios de Obtenção de Prova*, pp. 159-160 e 503.

obter na sequência da investigação criminal, que não será, decerto, a maioria das situações. Se estas questões forem ultrapassadas, é necessária a consequente apreensão do sistema informático onde os dados se encontram armazenados ou a partir do qual se acedeu, tendo em conta estes dados estão frequentemente cifrados e são muito voláteis, nos termos do n.º 7 do artigo 16.º da LCib.[233] A recolha desses dados deve ser realizada remotamente, ou seja, através da busca *online*, e é dificultada pelo facto dos utilizadores poderem facilmente eliminar os ficheiros da rede, uma vez que, no contexto da *DarkWeb*, é habitual existirem meios de verificar se a rede está a ser invadida por terceiros e, nesses casos, procedem à eliminação dos dados. Adicionalmente, a *DarkWeb* torna ainda mais difícil a recolha de prova digital graças aos programas que permitem o anonimato dos seus utilizadores e da sua localização associados à sua utilização.[234] Deste modo, a pesquisa e apreensão de dados informáticos serão apenas métodos de obtenção de prova digital eficazes no âmbito da *DarkWeb* se as autoridades tiverem informação prévia sobre o sistema informático utilizado e das credenciais de acesso, que implica o recurso a outros métodos de obtenção de prova.[235]

Para proceder eficazmente à interceção de comunicações, prevista no artigo 18.º da LCib, verifica-se a necessidade da identificação do suspeito ou de terceiro intermediário, de acordo com o artigo 187.º, n.º 4, do CPP *ex vi* do artigo 18.º, n.º 4, da LCib. Como temos vindo a mencionar, esta identificação é extremamente difícil na *DarkWeb*, visto que os dados de conteúdo se encontram cifradas e não podem ser conhecidas senão pelo destinatário final. No caso do *Tor*, poderá existir a hipótese de ter acesso a estes dados apenas e só se o destinatário final, no *exit node*, a quem a informação chega decifrada, não proceder às devidas precauções de cifragem da informação quando esta atinge o seu sistema informático, podendo aí ocorrer uma interceção bem sucedida. Porém, tendo em conta a improbabilidade desta situação, este método de obtenção de prova apresenta pouca ou mesmo nenhuma utilidade.[236]

Em relação às ações encobertas do artigo 19.º da LCib, este meio de obtenção de prova digital tem-se mostrado muito eficaz nos casos de crime de pornografia de menores

[233] ELIANA PEREIRA, *ob. cit.*, pp. 171 e 172.
[234] DAVID SILVA RAMALHO, "A investigação criminal na *Dark Web*", p. 404.
[235] *Id.*, p. 405. Especificamente em relação à apreensão de correio eletrónico, entendemos não ter tanto relevo atualmente, por existirem outros meios muito mais propícios à divulgação de pornografia infantil e, face aos problemas que a *DarkWeb* confere à investigação criminal, este não configura um dos seus maiores obstáculos.
[236] Cfr. DAVID SILVA RAMALHO, "A investigação criminal na *Dark Web*", pp. 406 e 407, ELIANA PEREIRA, *ob. cit.*, pp. 172 e 173 e DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova*, pp. 365 e 366.

online, inclusive na *DarkWeb*. Esta eficácia deve-se ao facto do agente encoberto conseguir, muitas vezes, diretamente, solicitar a respetiva identificação e localização dos utilizadores de uma determinada comunidade *online* que se dedica à partilha de material pedopornográfico, através da confiança que consegue obter por se encontrar nestes meios e simulando o mesmo interesse nestes conteúdos. A única situação em que a ação encoberta não é eficiente sucede nos casos em que os *websites* são destinados à mera visualização ou *download* - condutas a que nos referimos a propósito do tipo legal de crime - sem que ocorra comunicação entre os consumidores de material pedopornográfico.[237]

Manifestamente, os meios de obtenção de prova previstos na LCib são ineficazes na recolha de prova digital, com exceção da busca *online* e das ações encobertas, que demonstram alguma eficácia na deteção e repressão do crime de pornografia de menores.[238] Tal situação é incomportável perante a gravidade deste crime, pelo que o Direito deve atualizar-se à medida da evolução tecnológica e o legislador deve repensar os meios da LCib.

[237] Cfr. DAVID SILVA RAMALHO, "A investigação criminal na *Dark Web*", pp. 407-410, ELIANA PEREIRA, *ob. cit*., p. 174 e DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova*, p. 433.
[238] Cfr. DUARTE RODRIGUES NUNES, *O Problema da Admissibilidade dos Métodos "Ocultos" de Investigação Criminal*, pp. 814-817. Defendendo que o único meio que parece revelar-se eficaz são as ações encobertas, FREDERICO PELLUCCI, *ob. cit.*, p. 238.

11. O regime desadequado da cooperação internacional

Já mencionámos brevemente que a cibercriminalidade e a consequente obtenção e valoração de prova digital vieram inviabilizar o conceito clássico da aplicação da lei penal no espaço que, no ordenamento jurídico português, é definido pelo princípio da territorialidade, previsto no artigo 4.º do CP. Este princípio determina que a lei penal portuguesa é aplicável a factos praticados no território nacional, independentemente da nacionalidade do agente, uma vez que a prova digital é inerentemente dispersa e transnacional, ocorrendo frequentemente situações em que o agente do crime e a vítima são cidadãos nacionais, mas os dados informáticos que comprovam o cometimento do crime encontram-se armazenados em território estrangeiro. Contudo, também pode acontecer que o local onde se encontram os dados informáticos não considera o ato praticado como crime, normalmente implicando a recusa da cedência desses dados, o que impede a continuação do procedimento criminal. Em princípio, não será um problema para o crime de pornografia de menores pela sua gravidade e os diferentes países tentam coordenar-se no combate desta criminalidade.[239]

Assim sendo, a territorialidade como fator de conexão de competência jurisdicional já demonstrou ser insuficiente e, como tal, tem-se apontado o poder de disposição ou *power of disposal* sobre os dados informáticos como o correto fator de conexão, pois elimina a dificuldade do conhecimento da localização dos dados. O critério da disposição permite obter certos dados informáticos localizados no estrangeiro, de forma legítima, pelas autoridades judiciárias, desde que no âmbito de um procedimento criminal.[240]

Para colmatar as desvantagens da transnacionalidade da prova digital, a Convenção sobre o Cibercrime criou disposições acerca da cooperação judiciária internacional e, mais tarde, o chamado *Transborder Group* do Comité da Convenção sobre o Cibercrime do Conselho da Europa (T-CY), um subgrupo *ad-hoc* com o fundamento de desenvolver um instrumento, como um protocolo ou uma recomendação, sobre jurisdição e regulação do acesso transfronteiriço de dados, mas ainda sem qualquer solução legal concreta.[241]

---

[239] MANUEL MAGRIÇO, *ob. cit.*, p. 113.
[240] PEDRO VERDELHO, "Obtenção de prova *online*", p. 443.
[241] Disponível em https://rm.coe.int/16802e79e8.

Porém, a grande controvérsia neste âmbito tem sido a admissibilidade do acesso transfronteiriço unilateral de dados informáticos localizados no estrangeiro, estipulado no seu artigo 32.º. Ao nível da LCib, sabe-se que é permitido às autoridades estrangeiras acederem livremente a dados informáticos armazenados nos sistemas informáticos localizados em Portugal, ao abrigo do seu artigo 25.º. PEDRO VERDELHO afirma que este artigo é «o contraponto à autorização concedida às autoridades portuguesas pelo Artigo 32º da Convenção sobre o Cibercrime – diretamente aplicável na ordem jurídica interna».[242]

Existe alguma norma na LCib que admita o acesso transfronteiriço unilateral de dados informáticos localizados fora do país? DAVID SILVA RAMALHO e DUARTE RODRIGUES NUNES entendem que sim, recorrendo ao regime do n.º 5 do artigo 15.º da LCib como a fixação da intenção do legislador de possibilitar este acesso, sem qualquer notificação ao Estado onde se encontram os dados informáticos acedidos, ou seja, sem recorrer aos mecanismos de cooperação judiciária internacional e, consequentemente, a prova digital obtida por este mecanismo é valorada por encontrar previsão legal, logo é admissível nos termos do artigo 125.º do CPP.[243]

Todavia, há diversos entendimentos desfavoráveis quanto ao acesso transfronteiriço unilateral. RUI SOARES PEREIRA é veemente contra. Mesmo admitindo a insuficiência da Convenção sobre o Cibercrime de dar uma resposta rápida e eficiente perante as crescentes dificuldades na recolha de prova digital, defende que a solução não pode residir num acesso que fuja às regras da cooperação judiciária internacional, pelo menos enquanto não se legislar noutro sentido, por isso, o acesso transfronteiriço deve ser realizado conforme as regras estipuladas, não podendo desconsiderar o sistema processual do território onde se encontram os dados informáticos pretendidos como faz a LCib. Aliás, o autor pronuncia-se mesmo pela inconstitucionalidade da norma do artigo 15.º, n.º 5, da LCib. Portanto, na sua opinião, a prova digital obtida mediante um acesso transfronteiriço unilateral pode não vir sequer a ser valorada por falta de norma habilitante que o justifique, sendo reconduzível ao regime de proibição de prova do artigo 126.º da CPP. [244] Resumidamente, nas palavras do autor, o acesso transfronteiriço de dados informáticos deve sempre obedecer ao sistema de

[242] PEDRO VERDELHO, "Lei do Cibercrime", *Enciclopédia de Segurança*, 2015, p. 263.
[243] Cfr. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal*, pp. 83-90 e 274-277 e DUARTE RODRIGUES NUNES, *Os Meios de Obtenção de Prova*, pp. 234-244.
[244] Cfr. RUI SOARES PEREIRA, pp. 249-270.

cooperação judiciária internacional, porque o artigo 15.º, n.º 5, da LCib não apresenta suficiente «densidade normativa e a qualidade de lei necessárias, que são ainda exigências constitucionais de legitimação à luz do princípio da legalidade e do princípio da reserva de lei» e «a soberania e a territorialidade (ou jurisdição) devem ser entendidas como fazendo parte e assumindo um papel relevante no sistema (interno) de proteção de direitos fundamentais de cada Estado, pelo que, tendo em conta este cenário, sempre se poderia considerar ocorrer, por via do acesso transfronteiriço, uma violação indireta dos direitos fundamentais passível de enquadramento nas proibições de prova».[245]

Para VÂNIA COSTA RAMOS, a obtenção de prova transfronteiriça deve obedecer a três requisitos: a prova solicitada no estrangeiro seria admissível também em Portugal; a exigência do cumprimento das formalidades; a valoração da prova obtida apenas ocorre se não violar as regras de proibição de prova portuguesas, do país a quem se solicitou o acesso ou supranacionais, quer seja por solicitação, quer seja espontaneamente.[246]

Independentemente da aceitação ou não do acesso transfronteiriço unilateral de dados informáticos, existe a opinião generalizada: é com a maior urgência que se deve proceder à articulação do direito interno dos diversos países com as novas exigências de uma cooperação internacional eficaz em matéria de cibercriminalidade e recolha de prova digital.

Enquanto esse debate não ocorre, parece-nos que a razão se encontra com a admissibilidade do acesso transfronteiriço unilateral por duas grandes razões. A primeira razão prende-se com o facto deste acesso ser permitido expressamente pelo artigo 32.º da Convenção sobre o Cibercrime, desde que com o consentimento da pessoa com legitimidade para divulgar esses dados através do sistema informático ou caso os dados informáticos estiverem acessíveis ao público, mas também pelo artigo 15.º, n.º 5, da LCib mediante a interpretação de «tais dados são legitimamente acessíveis a partir do sistema inicial», existindo assim norma habilitante. A segunda razão tem que ver com a atual insuficiência da cooperação judiciária internacional para dar resposta aos muitos pedidos

[245] *Id.*, pp. 261 e 269.

[246] VÂNIA COSTA RAMOS, "Notas sobre novos desafios da cooperação judiciária internacional em matéria penal", *Revista de Estudios Europeos*, n.º extraordinario monográfico, 1-2019, p. 198. Nas páginas seguintes, a autora critica a falta de consenso nos Estados-Membros acerca da consequência da ilicitude na obtenção de prova, incluindo quando viola direitos fundamentais, e a clara insuficiência da jurisprudência do TEDH, mas também estabelece que o regime de proibições de prova português implica o respeito pelo artigo 8.º da CEDH, por imposição do artigo 32.º, n.º 8, da CRP que prevê o direito ao processo justo e equitativo, logo qualquer obtenção de prova que viole direitos fundamentais previstos na CEDH deve ser considerada excluída.

que recebe dos diferentes países e, por isso, devem repensar-se os mecanismos tradicionais da cooperação internacional – dando prioridade a mecanismos mais diretos de cooperação, por exemplo, os pedidos aos fornecedores de serviço como já referimos anteriormente. Esta permissividade tem especial sentido quando nos referimos à criminalidade aqui em causa, tendo em conta a gravidade do crime de pornografia de menores, que pensamos nenhum Estado irá contestar, podendo então dar primazia à obtenção de prova digital mediante acesso transfronteiriço unilateral quando isso significar o sucesso da investigação criminal e o combate da disseminação de pornografia infantil. Caso contrário, os Estados encontram-se à mercê da boa vontade dos fornecedores de serviços em permitir o acesso a certos dados informáticos, que tem vindo a diminuir.[247]

Inclusive certos países já adotaram medidas de acesso transfronteiriço nos seus ordenamentos jurídicos, tais como, a Bélgica que previu a possibilidade da pesquisa informática noutros Estados quando haja suspeita dos dados informáticos se encontrarem armazenados fora do território, sendo estes copiados e não eliminados, e desde que o Estado cujos dados são acedidos seja informado da dita pesquisa, bem como em Espanha se consagrou a possibilidade da realização de pesquisas informáticas a grandes sistemas de armazenamento de dados informáticos localizados no estrangeiro.[248]

Em conclusão, para nós, a solução passaria sempre por atingir um consenso entre os diversos países, que terminasse com as incongruências do regime da cooperação internacional. A solução belga parece-nos ser a mais acertada, por não deixar de permitir o acesso transfronteiriço de dados, não impedindo a realização da investigação, mas, simultaneamente, exige que se avise o Estado onde se está a proceder a este acesso, que traz alguma harmonia ao direito internacional. Entretanto, enquanto nada acontece, as investigações criminais não podem ficar frustradas pela passividade dos legisladores e pela resistência dos Estados em abdicar da sua soberania em prol do sucesso das investigações.

---

[247] Comité da Convenção sobre o Cibercrime do Conselho da Europa (T-CY), *Transborder access to data and jurisdiction: Options for further action by the T-CY*, 2014, p. 12 disponível em https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726e.

[248] DAVID SILVA RAMALHO considera que o legislador português adotou uma solução mais ousada que a belga, "A recolha de prova digital através de pesquisas informáticas transfronteiriças", *CEJ E-book – prova digital*, 2018, pp. 68 e 69. A norma habilitante belga corresponde ao artigo 39bis e espanhola é o artigo 588 *sexies* dos respetivos CPP.

12. O problema da *cloud* ou *nuvem*

Uma das maiores e mais recentes dificuldades de obtenção e valoração de prova digital relaciona-se com um recente meio de armazenar dados em ambiente digital, a chamada *cloud* ou *nuvem*, e que se tornou na forma principal de armazenamento de dados informáticos na *internet*. Contudo, devido à *cloud* constituir um conceito relativamente novo para o Direito - que não tem capacidade para se atualizar à medida dos avanços tecnológicos - não se encontra expressa na lei.[249] Assim sendo, tem a maior utilidade compreender este conceito e as consequências na investigação criminal.

A *cloud* ou *nuvem* corresponde ao «serviço de disponibilização de recursos informáticos em rede destinados ao armazenamento de dados e/ou à utilização ou desenvolvimento de *software* a partir de servidores, com recurso às capacidades de memória e de processamento destes»,[250] como é o caso da *Dropbox, Google Drive* ou *iCloud*, mas também os *webmails* como o *Gmail* ou o *Hotmail*, que são serviços de correio eletrónico acedidos diretamente na *internet*, cujos e-mails ficam armazenados na *nuvem* e não no computador.[251] O uso da *cloud* apresenta a facilidade de armazenar dados e aplicações numa grande quantidade, que podem ser acedidos a qualquer momento, quer seja por uma pessoa ou por várias, consoante o objetivo, por qualquer dispositivo ligado à *internet*, sem ser necessário ocupar todo o espaço de memória do dispositivo.

Pese embora as vantagens para os seus utilizadores, a *cloud* configura um grande obstáculo à recolha de prova digital. Desde logo, como enuncia DAVID SILVA RAMALHO, a *nuvem* pode ser utilizada para a prática de atos ilícitos de três modos, podendo corresponder ao objeto material do crime, ao local virtual do crime e/ou ao instrumento do crime.[252] Portanto, a crescente utilização da *cloud* veio trazer mais complexidade à dispersão da informação por diferentes servidores, localizados em vários pontos do mundo, conforme o fornecedor de serviços *cloud* em causa, o que significa que

[249] DAVID SILVA RAMALHO realça que, à data da feitura da Convenção sobre o Cibercrime, a regra de armazenamento de dados informáticos era nos sistemas informáticos, designadamente computadores, *tablets, smartphones*, pelo que não se previu a recolha de prova digital no caso da *cloud* ou *nuvem*, *Métodos Ocultos de Investigação Criminal*, p. 76.
[250] DAVID SILVA RAMALHO, "A Recolha de Prova Penal em Sistemas de Computação em Nuvem", *Revista de Direito Intelectual*, n.º 2, 2014, p. 126. O Conselho da Europa define *cloud* como «*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*», *Eletronic Evidence Guide*, p. 177.
[251] *Id.*, p. 129 e ÂNGELA PINTO, *ob. cit.*, p. 130.
[252] *Id.*, pp. 130 e 131.

o facto da informação se encontrar deslocalizada está sujeita a vários ordenamentos jurídicos. Esta característica acarreta a instabilidade e volatilidade dos dados armazenados em *nuvem*, pois estes podem ser alterados ou eliminados pelo seu utilizador ou mesmo automaticamente pelos fornecedores de serviço *cloud* para evitar a sobrecarga de informação nos seus servidores, uma vez que estes dados não se encontram, muitas vezes, armazenadas num único servidor, mas sim repartidos por um conjunto de servidores.

Como tal, importaria que as autoridades judiciárias conhecessem a localização do servidor onde a informação pretendida se encontra armazenada, na sequência de uma determinada investigação criminal, mas é uma noção irrealista, visto que, por vezes, nem os fornecedores de serviços *cloud* têm conhecimento sobre qual o servidor em que determinados dados se encontram armazenados, por se tratar de uma repartição automática, assim como não possuem a capacidade de recuperar esses dados no caso do utilizador os ter eliminado da *cloud* sem nunca os ter armazenado no seu computador pessoal.[253]

Assim sendo, com a legislação existente, encontramo-nos novamente perante uma situação incomportável de morosidade face às características da prova digital, com a especificidade desta se encontrar armazenada num serviço *cloud*, cujo armazenamento encontra-se maioritariamente em servidores localizados em países estrangeiros, logo as autoridades judiciárias portuguesas vêem-se obrigadas a recorrer aos mecanismos de cooperação judiciária internacional, de modo a não contrariar a Convenção sobre o Cibercrime, que já vimos não ser a melhor opção quando está em causa tamanha volatilidade. Denota-se que o recurso à cooperação judiciária internacional, bem como o seu critério da territorialidade estão completamente ultrapassados, devido ao desconhecimento da localização dos dados armazenados em *nuvem*, pelo que o poder de disposição parece ser a melhor opção, pois releva sim a localização de quem possui a disponibilidade dos dados informáticos,[254] devendo ser admissível o seu acesso transfronteiriço.

[253] Cfr. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal*, pp. 76 e 77 e "A Recolha de Prova Penal em Sistemas de Computação em Nuvem", pp. 153 e 154, PEDRO VERDELHO, "Obtenção de prova online", *Cibercrimen - Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet*, Vol. 1, 2016, p. 444 e Conselho da Europa, *Eletronic Evidence Guide*, p. 88.
[254] PEDRO VERDELHO, "Obtenção de prova *online*", pp. 443 e 446.

Então, o acesso remoto e transfronteiriço nos sistemas *cloud* pode realizar-se ao abrigo dos artigos 15.º, n.º 5 e 6 e 16º, n.º 7, da LCib, porque estes artigos parecem permitir a pesquisa e apreensão de dados informáticos num qualquer sistema informático, independentemente da sua localização, incluindo um serviço *cloud*. No caso dos *webmails*, aplica-se o artigo 17.º da LCib nos mesmos termos que os artigos mencionados.[255] Um dos entraves na recolha de prova digital no âmbito da pesquisa e apreensão dos dados armazenados na *nuvem* corresponde a certos requisitos de acesso, como a palavra-passe da conta de utilizador do visado, que precisa de ser fornecida pelo próprio mediante o seu consentimento, caso contrário, deve ser solicitada a conservação dos dados ao fornecedor de serviço *cloud*. O mesmo acontece com a *password* de um *webmail*, mas a recolha do conteúdo das mensagens para futura apreensão é realizada através da sua cópia para um sistema informático e mediante autorização judicial, por imposição do próprio artigo 17.º da LCib.[256] Porém, em vez de ser dirigida ao titular dos dados, a autoridade judiciária pode antes dirigir-se ao fornecedor de serviços *cloud*, que nem sempre tem acesso ao conteúdo dos dados nem tão-pouco à palavra-passe da conta em questão. Mais, como já referimos, a sede dos serviços *cloud* não costuma ter a disponibilidade dos dados, restando dúvidas sobre a que entidade deve a autoridade judiciária dirigir-se.[257]

À falta de melhor solução perante este grande problema da recolha de prova digital em serviços *cloud*, tendo em conta que o legislador nada previu, cabe ao aplicador do Direito realizar «as necessárias adaptações», de acordo com o n.º 6 do artigo 15.º da LCib.

Esta solução instável traduz-se num catalisador para a prática de crimes devido à elevada dificuldade de recolha dos dados armazenados na *cloud* que podem conter inúmeros ficheiros de pornografia infantil sem nunca as autoridades conseguirem proceder à obtenção de prova digital com êxito.

[255] Concordam, PEDRO VERDELHO, "Obtenção de prova *online*", pp. 444-448 e ÂNGELA PINTO, *ob. cit.*, pp. 130 e seguintes.
[256] Cfr. ÂNGELA PINTO, *ob. cit.*, p. 130 e DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal*, p. 278.
[257] DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal*, pp. 273-275 e PEDRO VERDELHO, "Obtenção de prova *online*", p. 445.

13. O recente Acórdão sobre metadados e a discussão dos direitos fundamentais afetados

Uma das grandes dificuldades na obtenção e valoração de prova digital tem que ver com a conservação e transmissão dos metadados, devido ao grande conflito entre a descoberta da verdade material e o direito à segurança e a proteção da privacidade e da inviolabilidade das comunicações.

O recente Acórdão do TC n.º 268/2022 veio demonstrar isso mesmo ao pronunciar-se sobre a inconstitucionalidade dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, na sequência da declaração de invalidade da Diretiva n.º 2006/24/CE no Acórdão *Digital Rights Ireland Ltd e outros*, de 08.04.2014 do TJUE, e que trará, inevitavelmente, alterações à articulação das leis aplicáveis pela desaplicação destas normas. Esta decisão tem muitas implicâncias práticas, pelo que é necessário compreender os fundamentos invocados pelo TC.

Ora vejamos. A Diretiva n.º 2006/24/CE regula a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, isto é, os Estados-Membros foram obrigados a tomar medidas para a conservação de metadados – os mencionados dados de tráfego e dados de localização – que, apesar de não incluírem o conteúdo das comunicações, permitem «desenhar o historial do próprio ato comunicacional».[258] O TJUE determinou a invalidade da dita Diretiva, com efeito retroativo, por esta restringir, desproporcionalmente, os direitos pelo respeito pela vida privada e familiar e pela proteção de dados pessoais, previstos nos artigos 7.º e 8.º da CDFUE. Essencialmente, as razões invocadas pelo TJUE no Acórdão *Digital Rights Ireland* para a declaração de invalidade da Diretiva foram: o âmbito de aplicação da medida de conservação dos dados é excessiva, não estabelecendo um critério definido; a inexistência de requisitos quanto ao acesso aos dados conservados pelas autoridades; o prazo de conservação estabelecido não respeita o princípio da proporcionalidade, na vertente da necessidade; a ausência de garantias na segurança na conservação e transmissão de dados; a falta de estipulação da conservação dos dados na União Europeia.[259] Contudo, esta declaração de invalidade não implica a invalidade automática da Lei n.º 32/2008, mas sim apenas um dever de não

[258] RITA CASTANHEIRA NEVES, *ob. cit.*, p. 75.
[259] Acórdão do TJUE *Digital Rights Ireland*, de 08.04.2014, processos C-293/12 e C-594/12, disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A62012CJ0293.

aplicação da Diretiva por parte dos Estados-Membros.[260] Ainda assim, certos Estados-Membros optaram pela total desaplicação da Diretiva, existindo assim uma grande disparidade de legislações, o que impossibilita uma cooperação judiciária eficaz.[261]

Além disso, mais tarde, o Acórdão do TJUE *Tele2 Sverige AB* e *Watson*, de 21.12.2016, veio determinar que a opção pela previsão legal da conservação de dados nas legislações nacionais implica a existência de disposições legais quanto ao acesso das autoridades competentes aos dados conservados pelos prestadores de serviços de comunicações eletrónicas.[262]

A nível nacional, a Lei n.º 32/2008 permaneceu em vigor após a declaração de invalidade da Diretiva. Apesar de a lei nacional não apresentar alguns dos vícios apresentados à Diretiva n.º 2006/24/CE pelo TJUE, a verdade é que também não é exímia. Já DAVID SILVA RAMALHO e JOSÉ DUARTE COIMBRA tinham alertado que a Lei n.º 32/2008, mesmo sendo mais exigente e garantística do que a própria Diretiva no que concerne à conservação de dados, abrange todos os indivíduos que utilizam serviços de comunicações eletrónicas, em qualquer lugar e pelo prazo de 1 ano, o que se traduz na conservação de dados de sujeitos sobre os quais não há indícios da prática de atos ilícitos, ou seja, a lei nacional é censurável por permitir a conservação contínua e indiscriminada de dados de tráfego de quase todos os indivíduos que residem em Portugal, concluindo que a aplicação da Lei n.º 32/2008 é contrária ao entendimento do direito europeu.[263] Pelo contrário, DUARTE RODRIGUES NUNES defende que a Lei n.º 32/2008 não viola o direito comunitário, visto que o prazo de conservação de 1 ano não é excessivo quando está em causa a investigação de crimes graves e que só ocorre uma verdadeira lesão dos direitos fundamentais a partir do momento em que o processo penal obriga a identificação da pessoa cujos dados foram conservados porque, antes desse momento, apenas se sabe «que aquele aparelho ou cartão realizou ou recebeu uma comunicação de um outro aparelho ou cartão ou se encontra num dado local».[264]

---

[260] Cfr. Acórdão do TC n.º 403/2015, disponível em www.tribunalconstitucional.pt .
[261] Cfr. CONDE CORREIA, *ob. cit.*, p. 38 e ÂNGELA PINTO, *ob. cit.*, p. 121.
[262] Cfr. Ponto 79 do Acórdão do TJUE *Tele2 Sverige AB* e *Watson*, de 21.12.2016, processos C-203/15 e C-698/15, disponível em https://curia.europa.eu.
[263] DAVID SILVA RAMALHO e JOSÉ COIMBRA, "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves", *O Direito*, 147, 2015, pp. 1037-1039. Por sua vez, CARLOS PINHO entende que o legislador nacional foi mais além do âmbito da Diretiva ao estabelecer na Lei n.º 32/2008 um regime específico de obtenção de dados de tráfego, não harmonizando com as normas do CPP, *ob. cit.*, p. 72.
[264] DUARTE RODRIGUES NUNES, *O Problema da Admissibilidade dos Métodos "Ocultos" de Investigação Criminal*, pp. 561-563. No mesmo sentido, a Nota Prática n.º 7/2015, de 30.12, do Gabinete do Cibercrime do MP, esclareceu que, pelo facto das exigências invocadas pelo TJUE já se verificarem

Apreciando a fundamentação do TC no referido Acórdão, a conjugação dos artigos 4.º e 6.º da Lei n.º 32/2008 foi considerada inconstitucional pela violação do direito à reserva da intimidade da vida privada e do direito à autodeterminação informativa, previstos nos artigos 26.º e 35.º da CRP, respetivamente, em conjugação com o n.º 2 do artigo 18.º da CRP. O direito à autodeterminação informativa corresponde à «proteção das pessoas perante o tratamento de dados pessoais informatizados», isto é, «o objeto de proteção do direito à autodeterminação comunicativa reporta-se a comunicações individuais efetivamente realizadas ou tentadas e só essas é que estão a coberto pelo sigilo de comunicações».[265] Por sua vez, o direito à reserva da intimidade da vida privada, neste contexto, constitui uma dimensão mais ampla do desenvolvimento da personalidade, que se traduz na «faculdade de comunicar com segurança e confiança e o domínio e autocontrole sobre a comunicação, enquanto expressão e exteriorização da própria pessoa».[266]

Assim sendo, é preciso que haja garantias efetivas da proteção destes direitos. De acordo com os parâmetros definidos pelo TEDH, em conformidade com os artigos 7.º e 8.º da CDFUE, estas garantias passam pela notificação dos cidadãos do acesso aos seus dados, do conhecimento de como estes foram controlados e tratados e, em caso de utilização indevida, a possibilidade de poderem recorrer aos tribunais competentes.[267] Ademais, a efetividade dos dados passa pelo local de conservação dos dados pertencer a um dos Estados-Membros da União Europeia, de modo a existir compatibilização quanto ao exercício das garantias constitucionais de proteção, cumprindo com o estipulado no n.º 3 do artigo 8.º da CDFUE. Por isso mesmo, a conservação de metadados, pelo período de 1 ano, de todos os assinantes, ou seja, sem qualquer diferenciação, exceção ou ponderação face ao objetivo perseguido, ainda que o TJUE tenha admitido que a conservação possa ser considerada adequada e necessária para fins de interesse público,[268] não deixa de ser desproporcional, configurando uma agressão muito intensa à intimidade

---

consagradas no direito interno, a decisão europeia não afetaria a validade da lei nacional e a Lei n.º 32/2008 continuaria em vigor, disponível em https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_7_retencao_de_dados.pdf.

[265] Retirado do ponto 13 do Acórdão do TC n.º 403/2015, disponível em www.tribunalconstitucional.pt.

[266] *Ibid.*

[267] Estes parâmetros encontram-se explanados detalhadamente no Acórdão do TEDH *Big Brother Watch and others v. UK*, de 13.09.2018, disponível em www.hudoc.echr.coe.int.

[268] Ponto 49 do Acórdão do TJUE *Digital Rights Ireland* a propósito da conservação de dados ser adequada para a prossecução de investigações penais, conforme os objetivos da Diretiva n.º 2006/24/CE, disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A62012CJ0293.

da vida privada ao permitir identificar, a todo o tempo, a posição e os movimentos dos utilizadores e, como tal, o TC declarou a inconstitucionalidade nos termos enunciados.

Por último, quanto à transmissão de metadados, prevista no artigo 9.º da Lei n.º 32/2008, reporta-se novamente para a questão da notificação do acesso aos dados às pessoas abrangidas pelas autoridades nacionais competentes, visto que a falta de notificação implica a restrição do direito do titular dos dados quanto ao seu tratamento e controlo, bem como do direito de aceder aos tribunais para o exercício do controlo judicial de acessos abusivos ou ilícitos dos dados, limitando desproporcionalmente o direito a uma tutela jurisdicional efetiva, nos termos do n.º 1 do artigo 20.º da CRP, e do direito à autodeterminação informativa, pelo que o TC decidiu pela inconstitucionalidade deste artigo na parte em que não se prevê a notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros, pela violação do disposto no n.º 1 do artigo 35.º e do n.º 1 do artigo 20.º, em conjugação com o n.º 2 do artigo 18.º da CRP.

Portanto, este Acórdão vem alterar a articulação das leis aplicáveis à prova digital e gerar controvérsia, tendo um impacto enorme na investigação criminal. Tanto assim é que, após a decisão do TC, a PGR elaborou um pedido de nulidade desta decisão.[269] Uma das vozes mais prementes é a de RUI CARDOSO ao afirmar que o TC deu prevalência aos direitos da privacidade e da autodeterminação informativa em detrimento dos direitos à segurança e outros eventuais direitos que podem vir a ser afetados pelos crimes cometidos, que, na sua opinião, sairão impunes devido à impossibilidade de realizar a investigação criminal em muitos dos tipos legais de crime. Porém, a sua grande crítica parece ser a de que «a retenção de dados de telecomunicações pode ser feita para acautelar a faturação dessas empresas, mas não para investigar e punir crimes graves», demonstrando incoerência na fundamentação utilizada.[270]

Do mesmo modo, na declaração de voto de Lino Ribeiro presente no Acórdão, são enunciadas essas mesmas incongruências, sendo que discorda da decisão porque reconhece que «a disponibilidade de dados históricos para a investigação criminal só é

[269] O TC rapidamente rejeitou o pedido de nulidade da PGR por entender que carece de legitimidade processual e constitucional para suscitar a nulidade do dito Acórdão, retirado de um artigo do Jornal Diário de Notícias do dia 13.05.2022, disponível em https://www.dn.pt/sociedade/metadados-tc-rejeita-pedido-de-nulidade-da-pgr-14855240.html.

[270] Ideias retiradas do artigo de opinião do Procurador da República RUI CARDOSO publicada no Jornal Expresso, no dia 2.05.2022, disponível em https://expresso.pt/opiniao/2022-05-02-O-Tribunal-Constitucional-entre-o-real-e-o-surreal-e0e48418.

possível se eles forem temporariamente retidos pelos operadores de telecomunicações. Ou seja, a conservação de dados é estritamente necessária para as finalidades da investigação, porque só assim é possível obter dados historicamente determinados», dando primazia ao direito à liberdade e à segurança em prol do direito à autodeterminação informativa, que deve mesmo ser restringida se o inverso significar terreno fértil para a prática de crimes graves.[271] Inclusive, dá nota da decisão do TC alemão não considerar a conservação generalizada de metadados desconforme à sua Constituição quando nem prevê normas tão exigentes como as da nossa CRP, desde que apresente um regime adequado de segurança na conservação e transmissão destes dados.

Apesar da conservação de dados não ocorrer no âmbito de uma investigação criminal, de forma discriminada, o que pode ser potencialmente restritivo da privacidade, será que se sobrepõe ao direito à segurança dos cidadãos perante a prática de crimes graves? Será esta decisão uma cedência a algumas pressões europeias? Entendemos que a decisão do TC foi muito radical, tendo em conta que nenhum destes direitos pode ser encarado como absoluto. Face à cibercriminalidade, é inaceitável que as autoridades não consigam, de todo, fazer investigação criminal em certas circunstâncias. Parece-nos que uma boa solução encontra-se no regime alemão por conter como critério um sistema adequado de segurança, pelo que esperamos que a controvérsia se resolva correta e atempadamente, sob pena da impunibilidade de muitos crimes graves, como possivelmente o crime de pornografia de menores.

[271] Na realidade, na sua feitura, a CRP desconhecia todos os perigos que viriam relacionados com o uso da *internet* e a interpretação destes artigos deve ter isso em conta.

V. Possíveis soluções

O recurso à *internet* para a prática do crime de pornografia de menores tem gerado bastantes dificuldades à investigação criminal devido às características inerentes à prova digital que consistem em terreno fértil para a cibercriminalidade, especialmente mediante o anonimato e a possibilidade de apagar o rasto digital. As dificuldades de obtenção e valoração de prova digital neste tipo de criminalidade geram consequências muito graves para todas as crianças, que continuarão a sofrer destes abusos, pois a ineficácia da investigação criminal incentiva à perpetuação da prática destes atos ilícitos. Quais serão as soluções possíveis para contornar estas dificuldades de modo a proteger as nossas crianças?

Primeiro que tudo, o primeiro passo passa pela prevenção, isto é, a consciencialização para o problema da pornografia infantil e para os perigos da *internet* junto das crianças e dos seus pais, fomentando assim o aumento da literacia informática, por parte do Governo, da comunicação social, do sistema educativo, entre outros. De seguida, já indicámos diversas vezes a importância da especialização das nossas autoridades judiciárias e policiais, porque os conhecimentos técnicos podem constituir elemento crucial para o sucesso das investigações criminais. Seria interessante considerar a criação de *task forces* policiais a nível nacional, à semelhança da EUROPOL, altamente especializadas na cibercriminalidade, em especial na *DarkWeb* e perante mecanismos como a encriptografia. Muitas vezes, os Estados pecam por não investirem nestas iniciativas e, por isso, a falta de recursos e de ferramentas atuais não conseguem fazer frente à alta tecnologia das grandes redes criminosas, como as de pornografia infantil.

Uma ideia muito curiosa para dirimir a difusão de conteúdo pedopornográfico é a apontada por DAVID SILVA RAMALHO que corresponde a um *software* de nome *PhotoDNA* desenvolvido pela *Microsoft* e por uma universidade nos EUA que permite detetar as piores imagens de pornografia infantil que se encontrem *online* e a sua eliminação através de características únicas de cada fotografia, ou seja, este programa reconhece automaticamente uma determinada fotografia já antes divulgada na *DarkWeb* pelos seus elementos característicos, mesmo quando tenha sofrido alterações, e elimina-a de modo a impedir que seja copiada e divulgada outra vez, até na *Surface Web*, por

exemplo, no *Facebook* ou no *Whatsapp* e, em alguns casos, pode até descobrir-se a identidade de quem partilhou através dos seus servidores e das suas contas.[272]

Além disso, a harmonização da lei seria um enorme avanço no combate à pornografia de menores e na obtenção e valoração de prova digital. Como vimos, os meios de obtenção de prova consagrados na LCib são, na sua maioria, ineficazes para este tipo de cibercriminalidade, particularmente, quando recorrem à *DarkWeb*, e os que são minimamente eficazes correspondem a imensuráveis restrições dos direitos fundamentais, como o direito à privacidade, ou não se encontram sequer plasmados na lei. Então, a legislação nacional beneficiaria de uma alteração legislativa no sentido de incluir disposições processuais expressas e coerentes sobre recolha de prova digital no CPP, como muitos autores defendem, mas também a clarificação de certos regimes dúbios na LCib que o legislador não esclarece na letra da lei, mas parece abrir hipóteses para a aplicação, como são os casos da busca *online* e o uso de *malware/benware*, que não se encontram diretamente previstas, mas as normas parecem ir no sentido da sua admissibilidade. Na realidade, essa admissibilidade levaria ao êxito de muitas investigações criminais na cibercriminalidade que, se bem reguladas pelo legislador, diminuiria a lesão dos direitos fundamentais do lesado, ao mesmo tempo que as autoridades conseguiam proceder à investigação atempadamente.

Neste seguimento, pretendemos reiterar a possibilidade dos OPC, no decurso da ação encoberta, praticarem atos preparatórios ou de execução, tendo em conta que o acesso às comunidades *online* que se dedicam à distribuição e consumo de material pedopornográfico está dependente, regularmente, da cedência deste tipo de material como "moeda de troca para pertencer à dita comunidade como algo que deveria estar melhor regulado. Não obstante a gravidade da prática de crimes pelo OPC, vemo-nos obrigados a concordar com a sua admissibilidade em prol do sucesso da investigação criminal, que pode ficar completamente vedada se assim não acontecer, porque acreditamos que a capacidade de desmantelar estas redes de pornografia infantil mediante a identificação dos seus participantes é imprescindível para ajudar não apenas uma criança, mas quiçá dezenas ou milhares de crianças.[273]

[272] Cfr. DAVID SILVA RAMALHO, "A investigação criminal na *Dark Web*", pp. 420-422.

[273] Não descuramos que a cedência deste material é limitadora da dignidade da criança, mas se o sucesso da ação encoberta significar a destruição das grandes redes de pedofilia infantil ou somente de plataformas na *DarkWeb* destinadas à perpetuação da divulgação deste material, a prática do crime pelo OPC sobrepõe-se porque pode significar a preservação da dignidade de muitas crianças. DUARTE RODRIGUES NUNES, *O Problema da Admissibilidade dos Métodos "Ocultos" de Investigação Criminal*, pp.841-895.

A questão controversa dos metadados deve ser resolvida urgentemente, constituindo uma das maiores problemáticas atuais no nosso ordenamento jurídico, novamente estando em causa o atrito existente entre a investigação criminal bem sucedida e os direitos fundamentais do visado. Esta incerteza jurídica apenas leva a mais criminalidade, devendo a lei ser revista no sentido de garantir maior segurança na preservação e transmissão de dados.

Outro assunto premente corresponde à necessidade de legislar sobre a *cloud* ou *nuvem*, por configurar a principal forma de armazenar dados informáticos com os benefícios que já apontámos *supra*.

Na nossa opinião, uma das soluções mais eficazes seria o maior investimento na cooperação internacional, porque apenas a ação coordenada entre os países vai permitir o combate eficiente do crime de pornografia de menores e da sua divulgação, eliminando os «paraísos cibernéticos».[274] Uma cooperação internacional concisa tem a capacidade de, através da criação de Convenções e outros diplomas, uniformizar as diversas legislações de forma a conseguir que a recolha de prova digital ocorra rápida e competentemente e, simultaneamente, caminhando num sentido de congruência e paz jurídica na proteção dos direitos fundamentais. O caso paradigmático da cooperação internacional é o acesso transfronteiriço que é um método bastante competente no que toca à recolha de prova digital, mas que apresenta falhas, resultando no impedimento da prossecução da investigação criminal conforme o local onde se encontrem os dados informáticos, isto é, se lá for admissível ou não.

Porventura, avizinham-se caminhos mais frutíferos para a cooperação internacional entre Estados-membros e entre estes e países terceiros na luta contra o cibercrime que se tornará mais simplificada, enquanto se assegura uma maior proteção dos direitos fundamentais para os visados e da sua privacidade digital. Este é o mote do Conselho da Europa para o segundo Protocolo adicional à Convenção do Cibercrime que pretende melhorar a cooperação entre as autoridades dos diferentes países e entre estas e os fornecedores de serviço diretamente, prevendo procedimentos de assistência mútua urgente.[275] Paralelamente, este ano, a Comissão Europeia propôs nova legislação europeia para combater abusos sexuais a crianças com recurso à *internet* para fazer face ao

[274] Expressão interessante de VERA MARQUES DIAS, *ob. cit.*, p. 78.
[275] Disponível em https://www.consilium.europa.eu/en/press/press-releases/2022/04/05/access-to-e-evidence-council-authorises-member-states-to-sign-international-agreement/.

aumento da prática desta criminalidade durante a pandemia COVID-19,[276] pretendendo a criação de uma entidade independente – *EU Centre on Child Sexual Abuse* – que deverá, entre outras, supervisionar os relatórios dos fornecedores de serviços e enviá-los para as autoridades competentes nacionais para agilizar o processo.[277]

Expectavelmente será uma solução para muitos dos problemas e das dúvidas existentes na matéria da prova digital e melhorará a investigação criminal nos casos de pornografia de menores *online*.

[276] O aumento desta criminalidade durante a pandemia foi reportada num relatório da EUROPOL, disponível em https://www.europol.europa.eu/publications-events/publications/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic.

[277] Disponível em https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2976?fbclid=IwAR0boRf1lbP6g3LdX8Pa1kIC6cvXAMpLA_8p_DZnzsDCd2dixrkouFVSdWI.

VI. Conclusão

O crime de pornografia de menores continua a causar preocupação nas autoridades policiais e judiciárias mundiais, apesar dos grandes esforços para combater a sua prática ao longo dos anos. O recurso à *internet* tem gerado bastantes dificuldades à investigação criminal devido às características inerentes à prova digital que consistem em terreno fértil para a cibercriminalidade, especialmente mediante o anonimato e a possibilidade de apagar o rasto digital. As dificuldades de obtenção e valoração de prova digital nesta criminalidade geram consequências muito graves para todas as crianças, que continuarão a sofrer destes abusos, pois a ineficácia da investigação criminal incentiva à perpetuação da prática destes atos ilícitos.

Portanto, a análise do crime de pornografia de menores, consagrado no artigo 176.º do CP, permite-nos concluir que esta preocupação crescente leva o legislador a criminalizar toda e qualquer conduta relacionada com conteúdo pedopornográfico, incluindo a representação realista de menor e a mera detenção ou visualização deste material, densificando ainda mais a complexidade desta criminalidade. Não entendemos que a solução passe pela incriminação, como parece ser a tendência atual, mas sim pela previsão de mecanismos que obtenham resultados na cibercriminalidade. O rumo da cibercriminalidade será a crescente especialização e sofisticação dos seus participantes, o que torna cada vez mais exigente a investigação criminal, sendo necessário combater este fenómeno.

Assim sendo, defendemos que, através do estudo das características da prova digital e do funcionamento da *DarkWeb*, assim como dos meios de obtenção e valoração de prova digital presentes na LCib, a prioridade deve ser mesmo a uniformização da legislação entre os países, revendo critérios antiquados e desadequados que não se aplicam à prova digital e a atualização das normas jurídicas conforme os avanços tecnológicos, porque uma cooperação internacional coesa melhoraria, em larga medida, a investigação criminal dos casos de pornografia de menores. Além disso, as dificuldades inerentes à recolha de prova implicam que os Estados invistam mais na especialização das suas autoridades policiais e judiciárias, de modo que a investigação criminal seja eficaz.

Bem sabemos que a recolha de prova digital está associada, muitas vezes, a medidas de obtenção de prova intrusivas e violadoras dos direitos fundamentais dos visados, direitos estes que devem imperiosamente ser protegidos. No entanto, os direitos

fundamentais destas crianças também estão a ser violados ao serem sujeitas a estes abusos e somente uma investigação criminal eficiente levará à sua proteção. Dito isto, reiteramos que a luta contra a pornografia infantil beneficiaria de regimes jurídicos mais completos e concretos dos métodos de obtenção de prova digital que efetivamente funcionam, inclusive na *DarkWeb*, como as buscas *online*, o uso de *malware/benware*, o acesso transfronteiriço unilateral e, ainda, dos metadados.

Em suma, concluímos através do presente estudo que o combate ao crime de pornografia de menores continua a ser muito urgente, pois são muitas as dificuldades e complexidades existentes na obtenção e valoração de prova digital, pelo que o regime jurídico deve ser todo repensado e atualizado perante os desafios que o recurso à *internet* impinge e continuará a impingir à investigação criminal, exigindo que esta seja cada vez mais eficiente com vista a combater esta criminalidade.

VII. Bibliografia

ALBERGARIA, Pedro Soares de e LIMA, Pedro Mendes, "O Crime de Detenção de Pseudopornografia infantil – evolução ou involução?", *Revista Julgar,* n.º 12, Coimbra, Coimbra Editora, 2010.

ALFAIATE, Ana Rita, *A Relevância Penal da Sexualidade dos Menores*, Coimbra, Coimbra Editora, 2009.

ALBUQUERQUE, Paulo Pinto de, *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª edição atualizada, Lisboa, Universidade Católica Editora, 2021.

- *Comentário do Código Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª edição atualizada, Lisboa, Universidade Católica, 2011.

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

- *Consentimento e Acordo em Direito Penal*¸ Coimbra Editora, Coimbra, 1991.

- *Sobre as Proibições de Prova em Processo Penal*, Coimbra Editora, Coimbra, 1992.

- "Métodos ocultos de investigação: plädoyer para uma teoria geral", *Que futuro para o Direito Processual Penal? Simpósio em homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, Mário Ferreira Monte et al. (coord.), Coimbra, Coimbra Editora, 2009.

ANTUNES, Maria João e SANTOS, Cláudia, *Comentário Conimbricense do Código Penal, Tomo I, anotação ao artigo 176º*, Figueiredo Dias (dir.), 2ª edição, Coimbra, Coimbra Editora, 2012.

ANTUNES, Maria João e SOUSA, Susana Aires de, "Da relevância da identificação do bem jurídico protegido no crime de pornografia de menores", *Revista Portuguesa de Ciência Criminal*, Ano 29, N.º 2, Maio-Agosto 2019.

ANTUNES, Maria João, "Crimes contra a Liberdade e a Autodeterminação Sexual de Menores", *Revista Julgar,* n.º 12, 2010 (especial).

COCCO, Giovanni, "Può constituire reato la detenzione di pornografia minorile?", *Rivista Italiana di Diritto e procedura penale*, Anno XLIX, Fasc. 3 Luglio-Settembre, 2006.

CORREIA, João Conde, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público*, N.º 139, julho-setembro 2014.

DIAS, Jorge de Figueiredo, *Comentário Conimbricense do Código Penal, Tomo I, anotação ao artigo 172º*, Figueiredo Dias (dir.), Coimbra, Coimbra Editora, 1999.

- *Direito Penal, Parte Geral, Tomo I, Questões Fundamentais, A Doutrina Geral do Crime*, Maria João Antunes et al. (colab.), 3 ª edição, Coimbra, Gestlegal, 2019.

DIAS, Maria do Carmo Saraiva de Menezes da Silva, "Notas Substantivas Sobre Crimes Contra a Liberdade e Autodeterminação Sexual", *Revista do Ministério Público*, Nº 136, 2013.

DIAS, Vera Marques, "A Problemática da Investigação do Cibercrime", *Data Venia, Revista Jurídica e Digital*, Ano 1, n.º 1, Julho-Dezembro 2012.

GARCIA, M. Miguez e RIO, J. M. Castela, *Código Penal Anotado, Parte geral e especial com notas e comentários*, Coimbra, Almedina, 2014

LEITE, André Lamas, "As alterações de 2015 ao Código Penal em matéria de crimes contra a liberdade e autodeterminação sexuais – Nótulas esparsas", *Revista Julgar*, N.º 28, 2016.

LEITE, Inês Ferreira, *Pedofilia – Repercussões das Novas Formas de Criminalidade na Teoria Geral da Infração*, Coimbra, Almedina, 2004.

- "A tutela penal da liberdade sexual", *Revista Portuguesa de Ciência Criminal*, Ano 21, N.º 1, Coimbra, Janeiro-Março 2011.

LOPES, José Mouraz e MILHEIRO, Tiago Caiado, *Crimes Sexuais – Análise Substantiva e Processual*, 3ª edição, Coimbra, Almedina, 2021.

MAGRIÇO, Manuel Eduardo, *A Exploração Sexual de Crianças no Ciberespaço - Aquisição e Valoração de Prova Forense de Natureza Digital*, Sinapsis Editores, 2013.

MENDES, Paulo de Sousa, "A privacidade digital posta à prova no processo penal", *Quaestio facti, Revista Internacional sobre Razonamiento Probatorio*, n.º 2, 2021.

MESQUITA, Paulo Dá, "Prolegómeno sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal Português – O Código e a Lei do Cibercrime", *Processo Penal, Prova e Sistema Judiciário*, Coimbra, Coimbra Editora, 2010.

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

NEVES, Rita Castanheira e CORREIA, Hélder Santos; "A Lei do Cibercrime e a colaboração do arguido no acesso aos dados informáticos*", Actualidad Jurídica Uría Menéndez*, n.º 38, Outubro 2014.

NUNES, Duarte Rodrigues, *Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime*, 2ª edição, Coimbra, Gestlegal, 2021.

- *O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada: contributo para uma adequação do direito português às exigências de uma resposta eficaz à criminalidade organizada em matéria de utilização de métodos "ocultos" de investigação criminal*, Coimbra, Gestlegal, 2020.

- "Da Admissibilidade da utilização de *benware* no Direito Português", *CyberLaw by CIJIC*, Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, Eduardo Vera-Cruz Pinto (dir.), Edição n.º X, Setembro de 2020.

PATTO, Pedro Maria Godinho Vaz, "Pornografia Infantil Virtual", *Revista Julgar*, n.º 12, Coimbra Editora, 2010.

PELLUCCI, Frederico, "A Atuação dos Agentes Encobertos e Infiltrados nos Canais Abertos e Fechados de Comunicação em Ambiente Informático-Digital", Novos desafios da prova penal / coord. Paulo de Sousa Mendes, Rui Soares Pereira; autores Alexssandra Muniz Mardegan, Analu Peixoto Barbosa, António Camilo Alberto de Brito... [et al.], Almedina, Coimbra, 2020.

PEREIRA, Eliana, "Crime de Abuso Sexual de Menores com Recurso à Internet – *Darknet* – Os desafios da investigação", *Trabalhos Temáticos de Direito e Processo Penal*, Volume I, CEJ, 2016.

PEREIRA, Rui Soares, "O Acesso (Unilateral e sem recurso a mecanismos de cooperação judiciária internacional) a dados armazenados em sistemas informáticos localizados no estrangeiro", *Revista de Estudios Europeos*, n.º extraordinario monográfico, 1-2019.

PINHO, Carlos, "Os problemas interpretativos resultantes da Lei nº 32/2008, de 17 de julho (Conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações)", *Revista do Ministério Público*, nº 129, Jan-Mar 2012.

PINTO, Ângela, "Crime de Abuso Sexual de Menores com Recurso à Internet – Enquadramento jurídico, prática e gestão processual", *Trabalhos Temáticos de Direito e Processo Penal,* Volume I, CEJ, 2016.

RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Lisboa, Almedina, 2017.

- "Investigação Criminal na Dark Web", *Revista da Concorrência e Regulação*, Ano IV, n.º 14/15, Abril/Setembro 2013.

- " A recolha de prova penal em sistemas de computação em nuvem", *Revista de Direito Intelectual,* n.º 2, 2014.

- "A recolha de prova digital através de pesquisas informáticas transfronteiriças*", CEJ E-book, Prova Digital*, 2018.

RAMALHO, David Silva e COIMBRA, José, "A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves", *O Direito*, 147, 2015.

RAMOS, Vânia Costa, "Notas sobre novos desafios da cooperação judiciária internacional em matéria penal", *Revista de Estudios Europeos*, n.º extraordinario monográfico, 1-2019.

RAPOSO, VERA, "Da moralidade à liberdade: o bem jurídico tutelado na criminalidade sexual", Costa Andrade e outros (org.), *Liber Discipulorum para Figueiredo Dias*, Coimbra, Coimbra Editora, 2003.

RODRIGUES, Ana Paula, "Pornografia de menores: novos desafios na investigação e recolha de prova digital", *Revista do CEJ,* n.º 15, 1º semestre, 2011.

RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo II, Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal*, 1ª edição, com prefácio da Dra. Sara Antunes, Lisboa, Rei dos Livros, 2010

- *Da Prova Penal, Tomo IV, Da prova eletrónico-digital e da criminalidade informático-digital*, 1º edição, com prefácio da Dra. Catarina dos Santos Gomes, Lisboa, Rei do Livros, 2011

ROXIN, Claus, *Derecho penal. Parte general*, Tomo I, Trad. Diego-Manuel Luzón Peña, Miguel Díaz y Garcia Conlledo e Javier Vicente Remesal Madrid, Civitas, 1997.

- "O conceito de bem jurídico como padrão crítico da norma penal posto à prova", *Revista Portuguesa de Ciência Criminal*, Ano 23, N.º 1, 2013.

TEIXEIRA, Paulo Duarte, "A (R)evolução Silenciosa do Sistema Penal Português", *Revista Julgar*, n.º 33, Coimbra Editora, 2017.

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

VERDELHO, Pedro, "A nova lei do cibercrime", *Scientia Ivridica*, 320, 2009.

- "Lei do Cibercrime", *Enciclopédia de Segurança*, 2015.

- "Obtenção de prova online", *Cibercrimen - Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet*, Daniela Dupuy (dir.) e Mariana Kiefer (coord.), Vol. 1, 1ª edição, Montevideo, Editorial B de F, 2016.

Documentos online:

Conselho da Europa, *Electronic Evidence Guide – A basic guide for police officers, prosecutors and judges*, 2013, disponível em https://rm.coe.int/16803028af.

CRESPO, Álvaro E., "La pornografía infantil en el marco de los delitos informáticos y del llamado "derecho penal de las sociedades de riesgo". Cuestiones problemáticas", *Derecho Penal Online*, 2010, disponível em https://derechopenalonline.com/la-pornografia-infantil-en-el-marco-de-los-delitos-informaticos-y-del-llamado-derecho-penal-de-las-sociedades-de-riesgo-cuestiones-problematicas/.

EUROPOL, *Exploiting Isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic*, 2020, disponível em https://www.europol.europa.eu/cms/sites/default/files/documents/europol_covid_report-cse_jun2020v.3_0.pdf.

EUROPOL, *Internet Organised Crime Threat Assessment* (IOCTA), Publications Office of the European Union, 2021, disponível em https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf.

GERCKE, Marco, *Understanding Cybercrime: A Guide for Developing Countries*, Genebra, ITU, 2009, disponível em https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

Relatório Explicativo sobre a Convenção do Cibercrime, disponível em https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf.

GRECO, Luís e GLEIZER, Orlandino, "A infiltração *online* no processo penal – Notícia sobre a experiência alemã", *Revista Brasileira de Direito Processual Penal*, Volume 5, N.º 3, Setembro-Dezembro 2019, disponível em https://revista.ibraspp.com.br/RBDPP/article/view/278/192.

Jornal Diário de Notícias do dia 13.05.2022, disponível em https://www.dn.pt/sociedade/metadados-tc-rejeita-pedido-de-nulidade-da-pgr-14855240.html

Jornal Expresso, no dia 2.05.2022, disponível em https://expresso.pt/opiniao/2022-05-02-O-Tribunal-Constitucional-entre-o-real-e-o-surreal-e0e48418

Legislação estrangeira:

Decisão-Quadro n.º 2004/68/JAI do Conselho, de 22 de dezembro de 2003, relativa à luta contra a exploração sexual de crianças e a pornografia infantil, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32004F0068&from=HU.

Decisão-Quadro n.º 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005F0222.

Diretiva n.º 2006/24/CE, do Parlamento e do Conselho Europeu, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32006L0024&from=FI.

Convenção sobre o Cibercrime ou Convenção de Budapeste, assinada em 23 de novembro de 2001, disponível em https://rm.coe.int/16802fa428.

Diretiva n.º 2011/93/UE, do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32011L0093.

Jurisprudência consultada:

Acórdão do TC n.º 426/91, de 06.11.1991, processo n.º 183/90, relator José de Sousa e Brito, disponível em www.tribunalconstitucional.pt.

Acórdão do TC n.º 867/2021, de 10.11.2021, processo n.º 867/19, relator Lino Rodrigues Ribeiro, disponível em www.tribunalconstitucional.pt.

Acórdão do TC n.º 403/2015, processo n.º 773/15, relator Lino Rodrigues Ribeiro, disponível em www.tribunalconstitucional.pt.

Acórdão do TC n.º 268/2022, processo n.º 828/2019, relator Afonso Patrão, disponível em www.tribunalconstitucional.pt.

Acórdão do STJ de 22.01.2013, processo n.º 182/10.3TAVPV.L1.S1, relator Santos Cabral, disponível em www.dgsi.pt.

Acórdão do STJ de 17.05.2017, processo n.º 194/14.8TEL.SB.S1, relator Pires da Graça, disponível em www.dgsi.pt.

Acórdão do STJ de 13.03.2019, processo n.º 3910/16.0T9PRT.P1.S1, relator Vinício Ribeiro, disponível em www.dgsi.pt.

Acórdão do STJ de 16.01.2020, processo n.º 283/17.7JDLSB.L1.S1, relatora Helena Moniz, disponível em https://jurisprudencia.csm.org.pt.

Acórdão do STJ de 19.02.2020, processo n.º 4883/15.1TDLSB.L1.S1, relator Nuno Gonçalves, disponível em https://jurisprudencia.csm.org.pt.

Acórdão do TRC de 11.11.2020, processo n.º 28/16.9PAACB.C1, relatora Elisa Sales, disponível em www.trc.pt.

Acórdão do TRE de 06.01.2015, processo n.º 6793/11.2TDLSB-A.E1, relator João Gomes de Sousa, disponível em www.dgsi.pt.

Acórdão do TRE de 17.03.2015, processo n.º 524/13.0JDLSB.E1, relator Carlos Jorge Berguete, disponível em www.dgsi.pt.

Acórdão do TRE de 14.07.2020, processo n.º 649/19.8TELSB-A.E1, relator Renato Barroso, disponível em www.dgsi.pt.

Acórdão do TRE de 21.09.2021, processo n.º 1144/17.5PBSTB.E1, relator Moreira das Neves, disponível em www.jurisprudência.pt.

Acórdão do TRL de 19.06.2014, processo n.º 1695/09.5PJLSB.L1-9, relatora Margarida Vieira de Almeida, disponível em www.dgsi.pt.

Acórdão do TRL de 07.03.2017, processo n.º 1585/16.5PBCSC-A.L1-5, relator Artur Vargues, disponível em www.dgsi.pt.

Acórdão do TRL de 06.02.2018, processo n.º 1950/17, relator João Carrola, disponível em www.dgsi.pt.

Acórdão do TRL de 22.04.2021, processo n.º 184/12, relator Fernando Estrela, disponível em www.dgsi.pt.

Acórdão do TRP de 07.06.2017, processo n.º 481/14.5JABRG.P1, relator Cravo Roxo, disponível em www.dgsi.pt.

Acórdão do TRP de 20.11.2019, processo n.º 54/19.6GDSTS-A.P1, relator Borges Martins, disponíveis em www.dgsi.pt.

Acórdão do TRP de 22.04.2020, processo n.º 573/18.1JAAVR.P1, relator José Piedade, disponível em www.dgsi.pt.

Jurisprudência estrangeira:

Acórdão *Ashcroft, Attorney General, et. al. v. Free Speech Coalition et. al* do Supreme Court of the United States, de 16.04.2002, disponível em https://www.law.cornell.edu/supct/pdf/00-795P.ZS.

Acórdão *R. v. Sharpe, do* Supreme Court of Canada de 21.01.2001, disponível em https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1837/index.do.

Acórdão do TJUE *Digital Rights Ireland*, de 08.04.2014, processos C-293/12 e C-594/12, disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A62012CJ0293.

Acórdão do TJUE *Tele2 Sverige AB* e *Watson*, de 21.12.2016, processos C-203/15 e C-698/15, disponível em https://curia.europa.eu.

Acórdão do TEDH *Wieser and Bicos Beteiligungen GmbH v. Austria*, de 16.01.2008, disponível em www.hudoc.echr.coe.int.

Acórdão do TEDH *Gardel v. France*, de 17.03.2010, disponível em www.hudoc.echr.coe.int.

Acórdão do TEDH *Big Brother Watch and other v.* UK, de 13.09.2018, disponível em www.hudoc.echr.coe.int.