Tribunal da Relação de Évora
Processo nº 355/22.6JGLSB.E1

Relator: FÁTIMA BERNARDES
Sessão: 05 Março 2024
Votação: UNANIMIDADE

METADADOS **DADOS DE TRÁFEGO**

DECLARAÇÃO DE INCONSTITUCIONALIDADE **PROVA PROÍBIDA**

PORNOGRAFIA DE MENORES

Sumário

I - Pese embora o formulário utilizado pelo Ministério Público (invocando como fundamento legal para o pedido o artigo 14º da Lei nº 109/2009 e os artigos 267º, 262º e 164º do C. P. Penal), se os dados solicitados são obtidos a partir de um concreto IP em conexão com uma certa comunicação realizada (e não a partir de uma relação contratual), estamos perante dados conservados pela operadora nos termos do artigo 4º, nº 1, al. a), e nº 2, al. b), da Lei nº 32/2008, de 17/07 (normativo que foi declarado inconstitucional, com força obrigatória geral, pelo Ac. do TC nº 268/2022).
II - Trata-se, por isso, de prova proibida, sendo que a admissão parcial dos factos pelo arguido, não deve, no caso dos autos, ser considerada como forma autónoma e independente de acesso aos factos, sem conexão estreita com a prova proibida, na medida em que é motivada pela apreensão e exame aos equipamentos informáticos onde é descoberta matéria com relevância criminal (que é prova proibida contaminada pela prova proibida original).
III - Por força do “efeito à distância” daquela proibição de prova (prova primária), a apreensão do equipamento/material informático, que teve lugar no âmbito da busca domiciliária realizada, mostra-se “contaminada”, não podendo ser utilizada a prova obtida por esse meio (prova sequencial ou secundária), sendo que, no caso concreto, não ocorre qualquer exceção ou limitação do “efeito à distância” decorrente da assinalada proibição de prova, designadamente a existência de prova sequencial obtida através de uma fonte independente e autónoma da prova inquinada ou a ocorrência da situação de “mácula dissipada”.

Texto Integral

Acordam, em conferência, na Secção Criminal do Tribunal da Relação de Évora:

1. RELATÓRIO
1.1. Neste processo comum, com intervenção do Tribunal Coletivo, n.º 355/22.6JGLSB do Tribunal Judicial da Comarca de Faro – Juízo Central Criminal de Faro – Juiz 3, foi submetido a julgamento o arguido ***(A)***, acusado da prática, como autor material, na forma consumada e em concurso efetivo, de 7872 (sete mil oitocentos e setenta e dois) crimes de pornografia de menores, p. e p. pelos artigos 176º, n.ºs 1, alíneas c) e d) e 5, do Código Penal, agravados, sendo 6842 (seis mil oitocentos e quarenta e dois) crimes pelo n.º 7 e 1030 (mil e trinta) crimes pelo n.º 6, do artigo 177º do Código Penal.
1.2. Realizado o julgamento, foi proferido acórdão, em 16/06/2023, depositado nessa mesma data, no qual se decidiu absolver o arguido da prática de todos os crimes por que vinha acusado.
1.3. Inconformado com o assim decidido, recorreu o Ministério Público para este Tribunal da Relação, extraindo da motivação de recurso apresentada as conclusões que seguidamente se transcrevem:
«1.ª - O inquérito iniciou-se através de uma ação de monitorização na *internet* desenvolvida pela Polícia Judiciária em redes de partilha *Peer-to-peer*.
2.ª - Nessa ação foi detetado que, no dia 3 de Abril de 2022, cerca das 22H11, bem como no dia 3 de Maio de 2022, cerca das 07H31 e 08H48, através do IP (.....), nesses grupos data/hora, se encontravam disponíveis para ser descarregados e partilhados ficheiros de abuso sexual de menores (cf. fls. 2/4).
3.ª - Perante esse circunstancialismo, o Ministério Público solicitou à operadora NOS que fornecesse a identificação completa do utilizador que operou o endereço desse IP na data a horas indicados, datas e horas de início e do termo da ligação que usou aquele endereço de IP, com fundamento no estatuído nos artigos 11.º, n.º 1, alínea b), e 14.º, n.ºs 1 a 4, da Lei do Cibercrime.
4.ª - Apurou-se junto da operadora NOS que o referido IP era utilizado pelo arguido (A), residente na morada sita (.....) (cf. fls. 10/12).
5.ª - Nessa sequência, foram realizadas buscas domiciliárias na residência do arguido (A), em que lhe foram apreendidos aparelhos informáticos, cuja perícia informática revelou que o mesmo, no dia 13/07/2022, tinha a aplicação

DreaMule em funcionamento desde há dez mil cento e dezoito horas (10118,56) – mais de 421 dias – em atividade de *upload* e há sete mil novecentas e sessenta e três horas (7963,49) – mais de 331 dias – em atividade de *download* (computador Acer) e há três mil trezentas e noventa e cinco horas (3395,40) – mais de 141 dias – em atividade de *upload* e há três mil quatrocentas e seis horas (3406,93) – mais de 141 dias – em atividade de *download*, (computador Lenovo), de forma ininterrupta, período durante o qual o arguido (A) descarregou variados ficheiros contendo vídeos e/ou imagens com o teor descrito em 1.º do libelo acusatório e permitindo ao mesmo tempo a partilha a terceiros dos ditos ficheiros.
6.ª - Mais se apurou que o arguido (A), no período compreendido entre 15/01/2022 e o dia 13/07/2022, na sua residência, sita (.....), utilizou a rede da *internet* associada ao contrato da NOS, através do IP (.....), que lhe havia sido fornecido pela operadora NOS, para, através dos referidos programas "DreaMULE", "uTorrent", "Ares" e "aMule", ordenar e proceder à descarga e partilha simultânea de pelo menos 32.687 ficheiros, ocupando um total de espaço em disco superior a 4 TB, na sua maioria ficheiros com designações compatíveis com pornografia de menores, de acordo com critérios de pesquisa habitualmente utilizados para o efeito, tendo os mesmos sido distribuídos/ partilhados, na sua totalidade ou parcialmente, através das referidas aplicações.
7.ª - Em concreto, apurou-se que o arguido Sidney Souza utilizou esses aparelhos para transferir, guardar e partilhar os seguintes ficheiros:
a) No computador Portátil Acer, através dos programas/aplicações de partilha de ficheiros "DreaMULE", "uTorrent", "Ares" e "aMule", o arguido Sidney Souza transferiu e guardou no disco rígido Toshiba pelo menos 1674 ficheiros vídeo de conteúdo sexual explícito, onde crianças surgem em práticas de cariz primordialmente sexual, nomeadamente, de sexo oral, anal, vaginal, atos de masturbação e poses eróticas, total ou parcialmente desnudados, envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 14 anos, tendo sido permitida ao mesmo tempo a partilha dos mesmos com terceiros;
b) No computador Portátil Acer, através dos programas/aplicações de partilha de ficheiros "DreaMULE", "uTorrent", "Ares" e "aMule", o arguido (A) transferiu e guardou no cartão de memória que se encontrava acoplado nesse computador pelo menos 1953 ficheiros de imagem de conteúdo sexual explícito, onde crianças surgem em práticas de cariz primordialmente sexual, nomeadamente, de sexo oral, anal, vaginal, atos de masturbação e poses eróticas, total ou parcialmente desnudados, envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal,

inequivocamente têm idade inferior a 14 anos, tendo sido permitida ao mesmo tempo a partilha dos mesmos com terceiros;
c) No computador Portátil Acer, através dos programas/aplicações de partilha de ficheiros “DreaMULE”, “uTorrent”, “Ares” e “aMule”, o arguido (A) transferiu e guardou no cartão de memória que se encontrava acoplado nesse computador pelo menos 454 ficheiros de imagem de conteúdo sexual explícito, onde crianças surgem em práticas de cariz primordialmente sexual, nomeadamente, de sexo oral, anal, vaginal, atos de masturbação e poses eróticas, total ou parcialmente desnudados, envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 16 anos, tendo sido permitida ao mesmo tempo a partilha dos mesmos com terceiros;
d) No computador Portátil LENOVO, através dos programas/aplicações de partilha de ficheiros “DreaMULE”, “uTorrent”, “Ares” e “aMule”, o arguido (A) transferiu e guardou no disco rígido/SSD pelo menos 239 ficheiros vídeo de conteúdo sexual explícito, onde crianças surgem em práticas de cariz primordialmente sexual, nomeadamente, de sexo oral, anal, vaginal, atos de masturbação e poses eróticas, total ou parcialmente desnudados, envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 14 anos, tendo sido permitida ao mesmo tempo a partilha dos mesmos com terceiros;
e) No computador Portátil LENOVO, através dos programas/aplicações de partilha de ficheiros “DreaMULE”, “uTorrent”, “Ares” e “aMule”, o arguido (A) transferiu e guardou no disco rígido/SSD pelo menos 30 ficheiros vídeo de conteúdo sexual explícito, onde crianças surgem em práticas de cariz primordialmente sexual, nomeadamente, de sexo oral, anal, vaginal, atos de masturbação e poses eróticas, total ou parcialmente desnudados, envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 16 anos, tendo sido permitida ao mesmo tempo a partilha dos mesmos com terceiros;
f) No disco externo Western Digital, o arguido (A) guardou pelo menos 366 ficheiros vídeo de conteúdo sexual explícito, onde crianças surgem em práticas de cariz primordialmente sexual, nomeadamente, de sexo oral, anal, vaginal, atos de masturbação e poses eróticas, total ou parcialmente desnudados, envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 16 anos, sendo que tais ficheiros foram descarregados pelo arguido no período acima descrito através da aplicação DreaMULE, tendo sido permitida ao mesmo tempo a partilha dos mesmos com terceiros.
8.ª - Consequentemente, assim que o arguido (A) descarregou cada um desses

ficheiros, estes ficaram, automaticamente, disponíveis para partilha através dos mencionados softwares/programa/aplicações de partilha Surfshark, CCleaner, Advanced SystemCare (IObit), Duplicate Cleaner log.txt, Mule, DreaMule, uTorrent e Ares;
9.ª - Acontece, porém, que o Tribunal *a quo* considerou que, à luz do Acórdão do Tribunal Constitucional n.º 268/2022, que julgou inconstitucionais as normas ínsitas nos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17/07, a obtenção dos dados atinentes à identificação e à morada do suspeito (utilizador de um determinado endereço IP, num dado dia e hora) configura uma prova proibida, por contender com direitos fundamentais do suspeito, pelo que tais dados devem ser tratados como se não existissem.
Por essa razão, o Tribunal *a quo* deu como não provada toda a factualidade narrada no libelo acusatório, absolvendo o arguido (A) dos crimes de pornografia de menores na sua forma agravada que lhe foram imputados nessa sede.
10.ª - Salvo o devido respeito, que é muito, o Ministério Público não se conforma com o douto Acórdão ora em crise, porquanto não merece a nossa concordância.
11.ª - Pois, os "metadados das telecomunicações", que são os dados das mesmas que não são comunicados, ou seja, são os dados sobre os dados comunicados, os dados gerados antes e durante o processo de comunicação, que estão na posse dos fornecedores dos serviços de telecomunicações, dividem-se em três categorias essenciais: a) os dados de base, ou seja, os elementos necessários ao acesso à rede: identificação do utilizador, morada, número de acesso e dados através dos quais o utilizador tem acesso ao serviço; b) os dados de tráfego, ou seja, a direção, destino, trajeto e duração da comunicação, bem como a localização dos aparelhos em comunicação; c) e os dados de conteúdo, ou seja, o conteúdo da comunicação: som, imagem, texto, etc.
12.ª - No caso vertente, o Ministério Público solicitou à operadora de telecomunicações NOS que fornecesse aos presentes autos "metadados das telecomunicações" que configuram meros dados de base, a saber:
a) identificação completa do utilizador que utilizou o endereço IP (…..), porto 999, no grupo data/horas do dia 4 de Março de 2022 às 19H58 e às 23H16 e do dia 5 de Março de 2022 às 03H42, 05H37 e às 18H07 (nome, morada de faturação e instalação, posto chamador, equipamento Internet instalado, marca, modelo e endereço MAC; b) datas e horas de início e do termo da ligação que usou aquele endereço de IP; c) IMEI, número de telemóvel e identificação do cliente, caso se trata de acesso por dispositivo móvel.
13.ª - Acontece que a identificação do utilizador de um determinado endereço

IP, num dado dia e hora, nada revela sobre o percurso de qualquer comunicação concreta, pois que se limita a confirmar que uma comunicação (e apenas essa), que já se conhece, foi efetuada através de um determinado número técnico de acesso à internet; portanto, com esta informação, apenas se estabelece a ligação entre uma determinada comunicação, que se conhece já, e a respetiva origem.
14.ª - Tais dados foram legítima e validamente solicitados pelo Ministério Público ao fornecedor de serviços, no caso, a operadora de telecomunicações NOS, ao abrigo do disposto nos artigos 11.º, n.º 1, alínea b), e 14.º, n.ºs 1 a 4, da Lei do Cibercrime, sendo a competência para a obtenção dos dados em apreço do Ministério Público.
15.ª - Essas normais legais, que se mantém em vigor, habilitam o Ministério Público, no âmbito de processos relativos a crimes cometidos por meio de um sistema informático (artigo 11.º, n.º 1, alínea b), da Lei do Cibercrime), a obter os dados acima apontados e solicitados à operadora de telecomunicações NOS (artigo 14.º, n.ºs 1 a 4, da Lei do Cibercrime).
16.ª - Foi, justamente, nessa sequência que o Ministério Público, com fundamento legal, requereu à Instrução Criminal autorização para a realização de buscas domiciliárias.
17.ª - Salvo o devido respeito, que é muito, não podia – nem pode – o Tribunal *a quo* convocar, para este efeito, o regime jurídico da conservação e transmissão de dados dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes, previsto na Lei n.º 32/2008, de 17/07, nem o nicho de normativos legais que foram julgados inconstitucionais, pelo Tribunal Constitucional, no acórdão n.º 268/2022, designadamente os artigos 4.º, 6.ºe 9.º da Lei n.º 32/2008, de 17/07, nem o regime jurídico ínsito em quaisquer outros dispositivos legais atinentes à obtenção de dados de tráfego.
18.ª - De facto, o Tribunal Constitucional, no acórdão n.º 268/2022, que tem um objeto bem delimitado, limitou-se a declarar a inconstitucionalidade dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17/07, não se tendo pronunciado, nem o poderia fazer, no âmbito de tal acórdão, acerca de outros normativos legais que, regendo a matéria da obtenção de “metadados das telecomunicações”, se mantêm em vigor, como é o caso do artigo 14.º, n.ºs 1 a 4, da Lei do Cibercrime, que serviu de base à solicitação feita à operadora NOS, pelo Ministério Público, no caso dos autos.
19.ª - E porque assim é, e porque os dados facultados pela operadora de telecomunicações NOS, atinentes à identificação e à morada do utilizador de

um determinado IP, num concreto lapso temporal, foram legitima, válida e oportunamente solicitados e obtidos, tais dados configuram prova legal, porquanto não proibida.
20.ª - Em consequência, o aresto em crise não merece a concordância do Ministério Público, pois que, através da prolação do aresto em crise, o Tribunal *a quo* violou as disposições legais ínsitas nos artigos 125.º e 126.º, ambos do Código de Processo Penal e 11.º, n.º 1, alínea b), e 14.º, n.ºs 1 a 4, ambos da Lei do Cibercrime.
21.ª - Aliás, esta discordância do Ministério Público goza de respaldo jurisprudencial nas instâncias superiores, designadamente no Tribunal da Relação de Évora e, inclusivamente, no Supremo Tribunal de Justiça (*vide* Acórdão do Tribunal da Relação de Évora, datado de 28 de Março de 2023, relatado pelo Ex.º Juiz Desembargador, Dr.º Artur Vargues, publicado na *internet* em *www.dgsi.pt*; Acórdão do Tribunal da Relação de Évora, datado de 9 de Maio de 2023, relatado pela Ex.º Juiz Desembargadora, Dr.ª Fátima Bernardes, publicado na *internet* em *www.dgsi.pt*; Acórdão do Supremo Tribunal de Justiça datado de 2 de Fevereiro de 2023, relatado pelo Ex.º Juiz Conselheira Maria Carmo Silva Dias, publicado na *internet* em *www.dgsi.pt*; Acórdão do Supremo Tribunal de Justiça, datado de 13 de Abril de 2023, relatado pelo Ex.º Juiz Conselheiro, Dr.º Orlando Gonçalves, publicado na *internet* em *www.dgsi.pt*).
Nestes termos, deve ser concedido provimento ao recurso interposto, mediante revogação do acórdão proferido nos autos e, concomitantemente, ser substituído por outro que admita os dados facultados pela operadora de telecomunicações NOS, atinentes à identificação e à morada de utilizador do IP referenciado, associados ao arguido (A), como prova válida e legítima, e, consequentemente, condenando-o pela perpetração dos crimes de pornografia de menores na forma agravada, imputados em sede de libelo acusatório, a uma pena única não inferior a 8 anos de prisão ou, em alternativa, o reenvio dos autos à primeira instância para renovação integral dos meios de prova indicados no libelo acusatório e apuramento das condições pessoais do arguido para efeitos de determinação da medida concreta da pena.
V. Exas. farão, como sempre, JUSTIÇA!»

1.4. O recurso foi regularmente admitido.
1.5. O arguido não apresentou resposta ao recurso.
1.6. Subidos os autos a este Tribunal da Relação, a Exm.ª Procuradora-Geral Adjunta emitiu parecer sem que concluísse pela procedência ou improcedência do recurso.
1.7. Cumprido o disposto no n.º 2 do artigo 417º do Código de Processo Penal,

não foi exercido o direito de resposta.
1.8. Feito o exame preliminar e colhidos os vistos legais, realizou-se a conferência, cumprindo agora apreciar e decidir:

2. FUNDAMENTAÇÃO
2.1. **Delimitação do objeto do recurso**
Em matéria de recursos, que ora nos ocupa, importa ter presente as seguintes linhas gerais:
O Tribunal da Relação tem poderes de cognição de facto e de direito – cf. artigo 428º do CPP.
As conclusões da motivação do recurso balizam ou delimitam o respetivo objeto – cf. artigos 402º, 403º e 412º, todos do CPP.
Tal não preclude o conhecimento, também oficioso, dos vícios enumerados nas alíneas a), b) e c), do nº. 2 do artigo 410º do C.P.P., mas tão somente quando os mesmos resultem do texto da decisão recorrida por si só ou em sua conjugação com as regras da experiência comum (cf. Ac. do STJ nº. 7/95 – *in* DR I-Série, de 28/12/1995, ainda hoje atual), bem como das nulidades principais, como tal tipificadas por lei.
No caso vertente, atentas as conclusões extraídas pelo recorrente da motivação de recurso apresentada, são as seguintes as questões suscitadas:
- Validade/legalidade da prova obtida através dos dados facultados pela operadora de telecomunicações NOS, atinentes à identificação e à morada do utilizador de um determinado IP, num concreto lapso temporal, com a indicação das datas e horas de início e termo da ligação, ao abrigo do disposto nos artigos 11º, n.º 1, alínea a) e 14º, n.ºs 1 a 4, da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro).
- Sequente validade das apreensões efetuadas no âmbito da busca domiciliária realizada na morada do arguido e da perícia realizada ao equipamento/ material informático apreendido;
- Consequente condenação do arguido pela prática dos crimes de pornografia de menores, na forma agravada, que lhe são imputados no libelo acusatório.

2.2. O **acórdão recorrido**, nos segmentos que relevam para a apreciação do mérito do recurso, é do seguinte teor:

«(…)
II – FUNDAMENTAÇÃO
1. **Factos Provados**
Produzida a prova e discutida a causa, resultaram provados os seguintes factos com pertinência para a decisão da mesma:

Inexistem factos provados

2. **Factos não Provados**

Não se provou:

1. Que no dia 13/07/2022, na sua residência sita (.....), o arguido detinha no seu quarto os seguintes objetos:

- Um computador portátil de marca Acer Modelo N15K1, com o s/n NXMVHEB024541057237600, contendo no seu interior, como parte integrante, um Disco Rígido 2,5", Toshiba, modelo: MQ01ABD100, S/N: 95LDC230T, com 1 TB (Terabyte) de capacidade, e onde se encontrava acoplado um cartão de memória (SDHC-Card), Voigtländer, S/N: 1021WG1408G, com 4 GB (Gigabyte) de capacidade.
- Um computador portátil LENOVO, modelo IDEAPAD 3 15ADA05, com o S/N:PF2NWY6E contendo no seu interior, como parte integrante, um SSD (Solid State Drive) M2 (NVMe) PCIe, modelo MTFDHBA512QFD, 512GB.
- Um disco externo da marcha Toshiba com capacidade de 2TB, com o N/S 17QETC2WTMAE.
- Um disco externo da marca WD elements, com o N/S WXA1A(?) 1HY.
- Um disco externo da marca WD elements, com 4TB de capacidade e com o S/N WDC87LJ84, o qual se encontrava ligado ao computador ACER.

2. Todos os equipamentos acima descritos pertencem e foram utilizados no período acima referido pelo arguido para armazenamento e partilha de vídeos e imagens, de conteúdo sexual explícito, onde menores surgem em práticas de cariz eminentemente sexual, nomeadamente, de sexo oral, anal, vaginal, actos de masturbação e poses eróticas, sendo que alguns menores tinham idade inferior a 14 anos e outros tinham idade inferior a 16 anos.

3. Para esse efeito, o arguido instalou e utilizou nos referidos equipamentos informáticos os seguintes ficheiros e softwares/programas/aplicações de partilha de ficheiros:

a) No Disco Rígido 2,5", da marca Toshiba, com 1 TB de capacidade (Computador Portátil Acer)

i. Surfshark
ii. CCleaner
iii. Advanced SystemCare (IObit)
iv. Um ficheiro denominado de Duplicate Cleaner log .txt, contendo informações, relativas a operações de limpeza do suporte de armazenamento (eliminação de duplicados, copia de arquivos para outra localização)
v. aMule
vi. DreaMule
vii. uTorrent
viii. Ares

b) No SSD (Solid State Drive) M2 (NVMe) PCIe, modelo MTFDHBA512QFD, 512GB (Computador Portátil LENOVO)
ix. DreaMule
x. Express VPN
4. Os aludidos programas/aplicações de partilha de ficheiros “DreaMULE”, “uTorrent”,“Ares” e “aMule”, estavam configurados para iniciar automaticamente assim que o computador fosse ligado, permanecendo depois ligados e em permanente funcionamento e assim que o arguido dava ordem para descarregar cada ficheiro, o mesmo ficava, automaticamente, disponível para partilha e descarga com e por terceiros, permitindo o arguido tal opção através do acionamento da opção de autorização de partilha a terceiros existente nesses programas.
5. Entre 15 de janeiro de 2022 até ao dia 13 de julho de 2022, através dos mencionados softwares/aplicações/programas, os quais utilizam um protocolo “*peer-to-peer*” (ponto-a-ponto), sempre que o arguido fez a descarga dos vídeos e imagens que pretendeu, o arguido permitiu a imediata partilha desses ficheiros ou de partes dos mesmos, contendo o teor acima descrito, proporcionando através dos referidos programas o acesso por terceiras pessoas, de diversas imagens e filmes de índole pornográfica, de conteúdo de índole sexual com menores, com o conteúdo supra descrito.
6. No dia 13/07/2022, a aplicação DreaMule encontrava-se em funcionamento desde há dez mil cento e dezoito horas (10118,56) – mais de 421 dias – em atividade de *upload* e há sete mil novecentas e sessenta e três horas (7963,49) – mais de 331 dias – em atividade de *download* (computador Acer) e há três mil trezentas e noventa e cinco horas (3395,40) – mais de 141 dias – em atividade de *upload* e há três mil quatrocentas e seis horas (3406,93) – mais de 141 dias – em atividade de *download*, (computador Lenovo), de forma ininterrupta, período durante o qual o arguido descarregou variados ficheiros contendo vídeos e/ou imagens de conteúdo sexual explícito onde menores de 16 e 14 anos surgem em práticas de sexo oral, anal, vaginal, atos de masturbação e poses eróticas e permitindo ao mesmo tempo a partilha a terceiros dos ditos ficheiros.
7. No aludido período e na morada indicada em 1.º, utilizando a rede da *internet* associada ao contrato da NOS e através do IP (…..) que lhe havia sido fornecido por esta operadora, através dos referidos programas “DreaMULE”, “uTorrent”, “Ares” e “aMule”, o arguido deu ordem e procedeu à descarga e partilha simultânea de pelo menos 32.687 ficheiros, ocupando um total de espaço em disco superior a 4 TB, na sua maioria ficheiros com designações compatíveis com pornografia de menores, de acordo com critérios de pesquisa habitualmente Utilizados para o efeito, tendo os mesmos sido

distribuídos/partilhados, na sua totalidade ou parcialmente, através das referidas aplicações.
8. Em concreto:
a) No computador Portátil Acer, através dos programas/aplicações de partilha de ficheiros “DreaMULE”, “uTorrent”, “Ares” e “aMule”, o arguido transferiu e guardou no disco rígido Toshiba pelo menos 1674 ficheiros vídeo de conteúdo sexual explícito, onde crianças surgem em práticas de cariz eminentemente sexual, nomeadamente, de sexo oral, anal, vaginal, actos de masturbação e poses eróticas, total ou parcialmente desnudados, envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 14 anos, tendo sido permitida ao mesmo tempo a partilha dos mesmos com terceiros.
b) No computador Portátil Acer, através dos programas/aplicações de partilha de ficheiros “DreaMULE”, “uTorrent”, “Ares” e “aMule”, o arguido transferiu e guardou no cartão de memória que se encontrava acoplado nesse computador pelo menos 1953 ficheiros de imagem de conteúdo sexual explícito, onde crianças surgem em práticas de cariz eminentemente sexual, nomeadamente, de sexo oral, anal, vaginal, atos de masturbação e poses eróticas, total ou parcialmente desnudados, envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 14 anos, tendo sido permitida ao mesmo tempo a partilha dos mesmos com terceiros.
c) No computador Portátil Acer, através dos programas/aplicações de partilha de ficheiros “DreaMULE”, “uTorrent”, “Ares” e “aMule”, o arguido transferiu e guardou no cartão de memória que se encontrava acopolado nesse computador pelo menos 454 ficheiros de imagem de conteúdo sexual explícito, onde crianças surgem em práticas de cariz eminentemente sexual, nomeadamente, de sexo oral, anal, vaginal, atos de masturbação e poses eróticas, total ou parcialmente desnudados, envolvendo menores que pela sua fisionomia estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 16 anos, tendo sido permitida ao mesmo tempo a partilha dos mesmos com terceiros.
d) No computador Portátil LENOVO, através dos programas/aplicações de partilha de ficheiros “DreaMULE”, “uTorrent”, “Ares” e “aMule”, o arguido transferiu e guardou no disco rígido/SSD pelo menos 239 ficheiros vídeo de conteúdo sexual explícito, onde crianças surgem em práticas de cariz eminentemente sexual, nomeadamente, de sexo oral, anal, vaginal, atos de masturbação e poses eróticas, total ou parcialmente desnudados, envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 14 anos, tendo sido permitida

ao mesmo tempo a partilha dos mesmos com terceiros.
e) No computador Portátil LENOVO, através dos programas/aplicações de partilha de ficheiros “DreaMULE”, “uTorrent”, “Ares” e “aMule”, o arguido transferiu e guardou no disco rígido/SSD pelo menos 30 ficheiros vídeo de conteúdo sexual explícito, onde crianças surgem em práticas de cariz eminentemente sexual, nomeadamente, de sexo oral, anal, vaginal, atos de masturbação e poses eróticas, total ou parcialmente desnudados, envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 16 anos, tendo sido permitida ao mesmo tempo a partilha dos mesmos com terceiros.
f) No disco externo Western Digital, o arguido guardou pelo menos 366 ficheiros vídeo de conteúdo sexual explícito, onde crianças surgem em práticas de cariz eminentemente sexual, nomeadamente, de sexo oral, anal, vaginal, atos de masturbação e poses eróticas, total ou parcialmente desnudados, envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 16 anos, sendo que tais ficheiros foram descarregados pelo arguido no período acima descrito através da aplicação DreaMULE, tendo sido permitida ao mesmo tempo a partilha dos mesmos com terceiros.
9. Assim que o arguido descarregou cada ficheiro, o mesmo ficou, automaticamente, disponível para partilha e descarga com e por terceiros.
10. Assim, tais ficheiros encontravam-se disponíveis para partilha e foram efetivamente partilhados com terceiros, alguns na sua totalidade e outros parcialmente.
11. Em concreto:
a) No computador Portátil Acer, através do programa/aplicação de partilha de ficheiros “aMule”, dos referidos vídeos, o arguido partilhou pelo menos 4 desses vídeos com terceiros, num total de 27 partilhas, vídeos esses envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 14 anos.
b) No computador Portátil Acer, através do programa/aplicação de partilha de ficheiros “aMule”, dos referidos vídeos, o arguido partilhou pelo menos 2 desses vídeos com terceiros, num total de 4 partilhas, vídeos esses envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 16 anos.
c) No computador Portátil Acer, através do programa/aplicação de partilha de ficheiros“DreaMule”,dos referidos vídeos o arguido partilhou pelo menos 124 desses vídeos com terceiros, num total de 2119 partilhas, vídeos esses envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 14 anos.

d) No computador Portátil Acer, através do programa/aplicação de partilha de ficheiros “DreaMule”, dos referidos vídeos, o arguido partilhou pelo menos 14 desses vídeos com terceiros, num total de 97 partilhas, vídeos esses envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 16 anos.
e) No computador Portátil LENOVO, através do programa/aplicação de partilha de ficheiros “DreaMule”, dos referidos vídeos, o arguido partilhou pelo menos 251 desses vídeos com terceiros, num total de 830 partilhas, vídeos esses envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 14 anos.
f) No computador Portátil LENOVO, através do programa/aplicação de partilha de ficheiros “DreaMule”, dos referidos vídeos, o arguido partilhou pelo menos 19 desses vídeos com terceiros, num total de 79 partilhas, vídeos esses envolvendo menores que pela sua fisionomia e estrutura anatómica e desenvolvimento corporal, inequivocamente têm idade inferior a 16 anos.
12. Desde o dia 15/01/2022 e até ao dia 13/07/2022, o arguido manteve os seus dois computadores portáteis sempre em funcionamento, permitindo a partilha a terceiros dos ficheiros de pornografia infantil que tinha na sua posse.
13. Para ocultar a existência dos aludidos ficheiros nos seus equipamentos informáticos, por diversas vezes, o arguido utilizou os programas de VPN e programas para apagar a memória e para efectuar a limpeza dos ficheiros, nomeadamente os programas Express VPN, Surfshark, CCleaner e Advenced System Care (IObit).
14. No dia 13/07/2022, aquando da realização da busca domiciliária, no diretório “.....”, que é utilizado por definição do DreaMule 3.2 para guardar os arquivos completos, o arguido tinha descarregado um ficheiro com a designação “.....”, contendo um filme de conteúdo sexual explícito onde menores de 16 e 14 anos surgem em práticas de sexo oral, anal, vaginal, atos de masturbação e poses eróticas.
15. No dia 13/07/2022, na sequência da realização de perícia informática aos equipamentos informáticos do arguido, foi possível apurar que:
- A pasta de receção dos ficheiros descarregados, pelo programa DreaMULE encontra-se neste equipamento e tem o caminho: C:\Users/papay/Downloads/eMule/Incoming, ou seja, sempre que o arguido dava ordem para descarregar ficheiro do seu interesse os mesmos ficavam alojados na pasta referida;
- Na pasta “*C:\Users\papay\Downloads\eMule\Temp*” foram identificados 29.181 ficheiros, ocupando um total de espaço em disco rígido de 3,41 TB, na sua maioria ficheiros com designações compatíveis com pornografia de

menores, de acordo com critérios de pesquisa habitualmente utilizados para o efeito, tendo os mesmos sido distribuídos/partilhados, na sua totalidade ou parcialmente, através da aplicação DreaMULE versão 3.2.
- Os ficheiros de "Download" (descargas) e Upload (partilha) estavam direcionados para a seguinte pasta: “.....”, possibilitando a partilha com os outros utilizadores da aplicação DreaMULE.
- No que concerne ao disco externo que estava ligado ao computador e referido supra no ponto 1 al. e), o arguido tinha no seu interior 29.181 ficheiros, ocupando um total de espaço em disco de3,41TB,contendo ficheiros de filmes de conteúdo sexual explícito onde menores de 16 e 14 anos surgem em práticas de sexo oral, anal, vaginal, atos de masturbação e poses eróticas, sendo que tais ficheiros tinham sido descarregados pelo arguido no período acima descrito através da aplicação DreaMULE, tendo sido permitida ao mesmo tempo a partilha dos mesmos com terceiros.
- No diretório “.....” foram identificadas 14.476 partes de ficheiros recebidos, num total de 411,34 GB, as quais constituem segmentos de ficheiros contendo imagens e vídeos de conteúdo sexual explícito onde menores de 16 e 14 anos surgem em práticas de sexo oral, anal, vaginal, atos de masturbação e poses eróticas, sendo que, aquando da realização da busca, as partes de ficheiros que se encontravam na pasta “Temp” estavam a ser partilhadas com terceiros.
16. Sabia o arguido, que as referidas aplicações/programas “DreaMULE”, “uTorrent”, “Ares” e “aMule”, se tratavam de programas, que visam a partilha de ficheiros e que se encontravam a guardar nos seus equipamentos informáticos os aludidos ficheiros e a partilhar tais ficheiros com terceiros, através dos seus computador, e dos programas de partilha neles instalados, e o arguido quis, como conseguiu, guardar para si, visualizar, divulgar na Internet os ficheiros de filmes e imagens acima descritos ,que exibiam diversas fotografias, imagens e filmes pornográficas de menores de idades inferiores a 14 anos e a 16 anos de idade.
17. O arguido bem sabia ainda que os vídeos e as imagens pornográficas expunham menores, com idades inferiores a 14 e 16 anos e que, por tal circunstância, estava proibida a sua detenção, exibição, cedência, ou partilha, o que não o coibiu de agir da forma descrita, como quis e conseguiu.
18. O arguido tinha perfeito conhecimento de que as referidas imagens e filmes de teor pornográfico com utilização de crianças são proibidas e não se inibiu de as exibir, ceder, divulgar, partilhar e de as deter nos seus suportes informáticos, que se encontravam na sua posse, o que não o impediu de agir do modo descrito, como quis e conseguiu.
19. Fê-lo, assim, bem sabendo que as imagens pornográficas expunham menores com idades inferior a 16 e 14 anos e que, por tal circunstância,

estava proibida a sua exibição, cedência, partilha, distribuição, posse e detenção, o que não o impediu de agir do modo descrito, como quis e conseguiu.
20. O arguido quis assim deter, nos referidos equipamentos informáticos, imagens de menores utilizados em filmes e gravações pornográficos de conteúdo sexual, para satisfazer a sua libido, o que conseguiu, bem sabendo que a sua detenção era proibida.
21. O arguido tinha perfeito conhecimento de que as referidas imagens e filmes de teor pornográfico com utilização de crianças, induzem a exploração efetiva dessas crianças, utilizadas para a realização dos filmes e fotografias em causa, não obstante, não se inibiu de os partilhar e ceder, a terceiros e de as deter em discos e computadores, que se encontravam na sua posse, desta forma promovendo e expandindo este mercado de exploração infantil.
22. O arguido difundiu os referidos dados através da Internet, pelo menos, a partir da sua residência divulgando assim as imagens de pornografia infantil através da Internet, que seguramente foram vistas por um grande número de pessoas em todo o mundo.
23. O arguido agiu sempre livre, deliberada e conscientemente, bem sabendo que as referidas condutas eram proibidas e punidas por lei, e tendo capacidade de determinação, ainda assim não se inibiu de as realizar.

*

Foram deliberadamente omitidos os factos conclusivos (artigos 1.º, 5.º, 6.º, 7.º e 8.º da acusação) e os factos atinentes às condições pessoais e aos antecedentes criminais do arguido, na medida em que não se apuraram quaisquer factos que permitam concluir pela culpabilidade do mesmo (artigo 369.º, n.º 1 do Código de Processo Penal).
*
3. **<u>Motivação da decisão quanto à matéria de facto</u>**
A convicção do Tribunal acerca da matéria de facto dada como provada e não provada assentou no conjunto da prova produzida em audiência recorrendo às regras de experiência e fazendo-se uma apreciação crítica da mesma nos termos do disposto no artigo 127.º do Código de Processo Penal.
Os presentes autos, tal como decorre do teor do auto de notícia de fls. 2 a 4, iniciam-se com uma ação de monotorização na *internet* por parte da PJ, em redes de partilha P2P (*peer-to-peer*), com foco na descarga de ficheiros com assinatura digital específica relacionados com pornografia de menores e onde foi detetado um determinado IP que disponíveis para partilha, naquele momento, alguns desses ficheiros.
A partir desse IP, e como decorre de fls. 9 (frente e verso) foi solicitado pelo

Ministério Público à operadora de comunicações NOS o envio de todos os elementos de identificação do utilizador do IP identificado a fls. 6 nos grupos data/hora e fuso horário indicados.
O que veio acontecer como decorre da informação da NOS de fls. 12.
Todavia, da conjugação do teor de fls. 9 e 12 decorre igualmente que a informação foi prestada por referência às comunicações estabelecidas nos grupos data/hora indicados a fls. 6 e não por referência a informações conservadas para fins comerciais ou inerentes a elementos contratuais.
Donde, salvo melhor entendimento, e pese embora o formulário utilizado pelo Ministério Público para solicitar as informações às operadoras não o invoque expressamente, impõe-se no caso, invocar o regime da Lei 32/2008, de 17.07, e, por consequência, o Acórdão do Tribunal Constitucional n.º 268/2022, que declarou "a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4.º da Lei n.º 32/2008, de 17 de julho, conjugada com o artigo 6.º da mesma Lei" e "a inconstitucionalidade, com força obrigatória geral, da norma do artigo 9.º da Lei n.º 32/2008, de 17 de julho, relativa à transmissão de dados armazenados às autoridades competentes para a investigação, deteção e repressão de crimes graves, na parte em que não 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 a integridade física de terceiros".
Com efeito, pese embora o formulário utilizado pelo Ministério invoque como fundamento legal para o pedido o artigo 14.º da Lei 109/2009 e os artigos 267.º, 262.º e 164.º do Código de Processo Penal, os dados solicitados são obtidos a partir de um concreto IP em conexão com uma certa comunicação realizada (as indicadas a fls. 6) e não a partir de uma relação contratual. Por conseguinte, dúvidas não restam que se tratam de dados conservados pela operadora nos termos do artigo 4.º, n.º 1, al. a), n.º 2 al. b) i) da Lei 32/2008.
Ou seja, dados que integram as categorias dos dados que devem ser conservados nos termos do artigo 4.º da Lei 32/2008 e que foi declarada inconstitucional com fundamento na violação do disposto nos números 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o artigo 18.º, n.º 2 da Constituição da República Portuguesa, por se considerar que a conservação de tais dados relativos às comunicações realizadas interfere com o direito de acesso aos seus dados pessoais informatizados e à proibição de acesso por terceiros e com o direito à reserva da intimidade da vida privada e ao livre desenvolvimento da personalidade.
Os metadados são, em si, meios de prova, designadamente prova documental, e a sua admissibilidade como tal não foi objeto de qualquer juízo de

inconstitucionalidade.
Como refere Rui Cardoso, *in* "A Conservação e a utilização probatória de metadados de comunicações eletrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…", artigo publicado na Revista do Ministério Público, 172, Outubro: Dezembro 2022, "Questão diferente é a da sua obtenção para o processo, para que possam ser utilizados como meios de prova. Podem ser juntos (artigo 164.º, n.º 1, do CPP), mas, quando corpóreos, são objectos susceptíveis de servir a prova e por isso podem ser apreendidos (artigo 178.º, n.º 1, do CPP), apreensão que é um meio de obtenção de prova. Para a apreensão pode ser necessário utilizar outros meios de obtenção de prova, como a revista e a busca – artigos 174.º a 177.º do CPP. Se forem documentos informáticos, prevê a LCC que a sua obtenção de faça através da injunção/concessão de acesso a dados (artigo 14.º, que infra se analisará) e/ou pesquisa e apreensão (artigos 15.º, 16.º e 17.º). Questão ainda diferente é a do regime de conservação dos metadados na posse dos FS e do seu acesso no processo. Aí estamos perante conservação de (possível) meio de prova".
Com efeito, a conservação de dados não se confunde com o acesso aos dados, sendo que o fundamento legal invocado pelo Ministério Público a fls. 9 diz respeito ao acesso e não à conservação dos dados.
Relativamente à conservação de dados apenas dois diplomas podiam ser convocados. A Lei 32/2008, de 17 de julho e a Lei 41/2004, de 18 de agosto, relativa à proteção de dados pessoais e à privacidade nas telecomunicações. A Lei 41/2004, de 18.8 visou e visa a proteção de dados pessoais e a privacidade nas telecomunicações e aplica-se ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicação públicas como se determina no seu artigo 1.º, n.º 2. Citando ainda o mesmo autor (ob. cit.) "(…) É proibida a escuta, a instalação de dispositivos de escuta, o armazenamento ou outros meios de intercepção ou vigilância de comunicações e dos respectivos dados de tráfego por terceiros sem o consentimento prévio e expresso dos utilizadores, com excepção dos casos previstos na lei – artigo 4.º, n.º 2, da Lei 41/2004. Um dos casos de excepção previstos na lei é o que respeita aos dados de tráfego – artigo 6.º dessa lei. No n.º 1 deste artigo determina-se que, sem prejuízo do disposto nos números seguintes, os dados de tráfego relativos aos assinantes e utilizadores tratados e armazenados pelas empresas que oferecem redes e ou serviços de comunicações electrónicas devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação. Os n.ºs 2 e 3 permitem (mas não obrigam) o tratamento de dados de tráfego necessários à facturação dos assinantes e ao pagamento de

interligações (exemplificando alguns tipos de dados) até final do período durante o qual a factura pode ser legalmente contestada ou o pagamento reclamado, que é hoje de seis meses (artigos 10.º, n.º 1, e 1.º, n.º 2, alínea d), da Lei 23/96). Outra excepção era a prevista, aí como obrigatória, nos artigos 4.º e 6.º da Lei 32/2008, declarados inconstitucionais com força obrigatória geral pelo Ac. TC 268/2022. Ou seja, quando a lei excepcionalmente o permite, os metadados são guardados, são conservados, são retidos, não são eliminados, fugindo ao regime regra. É disso que se deve falar quando se fala da conservação ou retenção de metadados".

Declarada a inconstitucionalidade dos artigos 4.º e 6 da Lei 32/2008, permanece apenas em vigor, no que à conservação de dados diz respeito, a Lei 41/2004.

Todavia, este diploma afasta expressamente do seu âmbito de aplicação a prevenção, investigação e repressão de infrações penais, as quais são definidas em legislação especial, como se refere no nº 4 do artigo 1º, esclarecendo ainda no artigo 6º, n.º 7 o seguinte: «O disposto nos números anteriores não prejudica o direito de os tribunais e as demais autoridades competentes obterem informações relativas aos dados de tráfego, nos termos da legislação aplicável, com vista à resolução de litígios, em especial daqueles relativos a interligações ou à faturação".

Desta forma, tem-se entendido que a aplicação desta lei se restringe à relação contratual, não sendo lícito lançar mão dela para efeitos de investigação criminal – neste sentido, os Acórdãos do Tribunal da Relação de Coimbra datados de 18 de maio de 2022 (Pº 171/21.2GGCBR-A.C1) e de 12 de outubro de 2022 (P.º 538/22.9JALRA.C1).

No que respeita ao acesso a dados conservados, existiam três normativos possíveis. O artigo 189.º, n.º 2 do Código de Processo Penal, o artigo 14.º da Lei do Cibercrime (Lei109/2009, de 15.9) e artigo 9.º da Lei 32/2008, esta última também julgada inconstitucional, o que, só por si, não eliminou nem afetou as restantes formas de acesso.

A questão não se centra, todavia, no acesso, mas sim na ilegitimidade da conservação dos dados e que é prévia à questão do acesso. Motivo pelo qual não nos merece concordância o recente acórdão do Supremo Tribunal de Justiça de 2 de fevereiro de 2023, relatado pela Conselheira Maria do Carmo Silva Dias.

A questão que ao caso interessa é a de saber a que título estavam os dados fornecidos pela operadora conservados. E, no caso, em face do já supra exposto, não temos dúvidas tratarem-se de dados conservados ao abrigo da Lei 32/2008.

Ora, por força da declaração, com força obrigatória geral, de

inconstitucionalidade, foram expurgadas do ordenamento jurídico as normas constantes do artigo 4.º, conjugado com o artigo 6.º e o artigo 9.º, todos da Lei 32/2008, de 17.7, ou seja, tais normas foram eliminadas, com efeito retroativo, do sistema jurídico português, como se nunca tivessem existido.
E, pelos fundamentos já invocados – a exceção à regra da eliminação dos dados é ditada apenas por razões de cobrança e não de prevenção, investigação e repressão de infrações penais-fica igualmente excluído (até porque a ele não se faz qualquer referência no pedido de dados à operadora), no caso concreto, o recurso ao artigo 6.º, n.º 1 e 3 da Lei (conjugado com o artigo 10.º, n.º 1 da Lei 23/96, de 26.7), ainda que no caso não se mostrasse ultrapassado o prazo.
Por conseguinte, a conservação dos dados em causa deixou de ter suporte legal e, consequentemente, de permitir, por via dela, a restrição dos direitos fundamentais previstos nos artigos 26.º e 35.º da Constituição da República Portuguesa, nos termos do n. 2 do mesmo diploma.
O que, desde logo, convoca o regime estabelecido no artigo 126.º, n.º 3 do Código de Processo Penal, segundo o qual "ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular".
Dispõe o artigo 32º, n.º 8 da Constituição da República Portuguesa que "São nulas todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações". Subjacente à regra do n.º 8, do artigo 32º da C.R.P., que unanimemente se entende que consagra o princípio das proibições de prova, está a ideia de que sendo a eficácia da justiça, também, um valor que deve ser perseguido, mas porque numa sociedade livre os fins nunca justificam os meios, aquela eficácia só é aceitável quando alcançada lealmente, pelo engenho e arte, nunca pela força bruta, pelo artifício ou pela mentira, que degradam quem os sofre, mas não menos quem os usa. Por isso o repúdio absoluto pela obtenção de provas mediante tortura, coação, e ofensa da integridade física ou moral da pessoa, cuja inviolabilidade é primariamente garantida nos artigos 24.º e 25.º da Constituição, e a limitação aos casos expressamente previstos na lei, em conformidade com a Constituição (artigos 26º e 34º), da obtenção de provas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações.
O que está em causa não é a proibição do uso de meios proibidos na obtenção de elementos de prova, mas essencialmente a utilização das provas obtidas por tais meios.
Há uma proibição absoluta de utilizar essas provas no processo pois seria

intolerável que para realizar a justiça fossem utilizados elementos de prova obtidos por meios vedados pela Constituição e incriminados pela lei.
A realização da justiça do caso é um valor constitucional, mas não é um valor absoluto, que possa ser perseguido por qualquer forma. Quando os meios utilizados para a obtenção das provas forem proibidos ou condicionados pela Constituição para salvaguarda de outros valores, os elementos probatórios por essa forma obtidos não podem ser utilizados em circunstância alguma; ficam radicalmente inquinados do vício de inconstitucionalidade e o sistema não pode tolerar que a Justiça seja prosseguida por meios inconstitucionais» - vide Jorge Miranda, Rui Medeiros, Constituição Portuguesa Anotada, Tomo I, 2ª Edição, Coimbra Editora, págs. 736 e 737.
O que aliás, desde logo decorreria do artigo 32.º, n.º 1 da Constituição, onde se estabelece que o processo criminal assegura todas as garantias de defesa, sendo que entre esses direitos de defesa se considera incluído o de ver excluídas do processo (tornadas ineficazes, inválidas ou nulas) as próprias provas ilegais reportadas a valores constitucionalmente relevantes.
Independentemente da questão da distinção entre nulidades e proibições de prova [decorre desde logo do artigo 118º, n.º 3 do C.P.P. que "as disposições do presente título não prejudicam as normas deste código relativas a proibições de prova] é hoje aceite que estas últimas têm autonomia face ao regime das nulidades, quer dogmática e de regime, embora não de forma pacífica quanto a este último aspeto [desde logo, pela aplicação às proibições de prova do regime previsto no artigo 122.º, n.º 1 do C.P.P.].
Assim, e para que não se confundam com as nulidades, dir-se-á que as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações são inutilizáveis, não podem ser utilizadas no processo, é como se não existissem.
E, por via do disposto no artigo 32.º, n.º 8 da C.R.P., do ponto de vista da proibição de valoração – ou seja, do ponto de vista da "sanção" legalmente imposta para a violação da proibição de produção de prova –estabeleceu-se uma relação de total identidade entre os n.ºs 1 e 3 do artigo 126º do Código de Processo Penal. A diferença entre as proibições de prova previstas no n.º 1 e as previstas no n.º 3 do citado preceito, não se situa ao nível da consequência jurídica (nulidade/proibição de valoração), mas ao nível da hipótese legal.
O n.º 1 do artigo 126º proíbe e sanciona os atentados mais graves e intoleráveis da dignidade e integridade pessoais. E proíbe-os sempre, independentemente do consentimento da pessoa concretamente atingida, sendo aqui, um tal consentimento, tido como pura e simplesmente irrelevante,

pois as proibições em causa (v.g. da tortura) não se revestem apenas de uma valência pessoal-individual. Elas valem também como “instituições” irrenunciáveis do processo penal do Estado de Direito e são, por isso, indisponíveis. Nas hipóteses previstas do n.º 3, o consentimento afasta a proibição: tanto a proibição de produção como a respetiva consequência. Consequência que continua a mesma - nulidade/proibição de valoração - se não houver consentimento, perante a intromissão e devassa que se configurem em manifestações arbitrárias de investigação e perseguição.
Assim, e em conclusão, na hipótese legal do n.º 3 do artigo 126º, as provas obtidas fora dos casos admitidos pela lei e sem o consentimento do respetivo titular, mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações, não podem ser utilizadas, e o seu conhecimento é oficioso, porque afronta diretamente a Constituição – neste sentido, veja-se o acórdão do Tribunal do Tribunal da Relação do Porto de 18 de junho de 2014 (Proc. 35/08.5JAPRT.P1).
Posto isto.
No caso, ainda que retroativamente, estaremos perante uma proibição de prova e que, naturalmente, se traduz numa proibição de valoração da mesma, por se tratar de informação (dados conservados) obtida com base na intromissão não tolerada de direitos fundamentais, em face da ausência de norma que a sustentasse.
Poderia questionar-se a existência de um conflito entre dois direitos fundamentais, por um lado os direitos fundamentais da pessoa e por outro o da realização da justiça. Todavia, não havendo lei que habilite a restrição de direitos fundamentais para a utilização probatória dos dados conservados, não há que fazer qualquer ponderação de interesses conflituantes, pois não se permite a realização da justiça com recurso a meios de prova proibidos.
Partindo deste pressuposto, de que estamos perante uma prova proibida, decorre da doutrina do efeito à distância da prova proibida que essa proibição de valoração se transmite às provas derivadas (secundárias) obtidas com base na prova proibida (primária).
Sobre esta questão, seguimos de perto, o Acórdão do Tribunal Constitucional 198/2004, de 24 de março de 2004 e que versou sobre a correta interpretação do artigo 122.º, n.º 1 do Código de Processo Penal [naquele caso, entendido como autorizando, face à nulidade/invalidade de interceções telefónicas realizadas, a utilização de outras provas, distintas das escutas e a elas subsequentes, quando tais provas se traduzam nas declarações dos próprios arguidos, designadamente quando tais declarações sejam confessórias].
A concretização do direito penal material, a averiguação da existência de um crime e a determinação das consequências jurídicas deste, alcançam-se

através de um procedimento (o processo penal) que podemos definir como "um complexo de actos juridicamente ordenado de tratamento e obtenção de informação que se estrutura e desenvolve sob a responsabilidade de titulares de poderes públicos e serve para a preparação da tomada de decisões" [Gomes Canotilho, Tópicos de um Curso de Mestrado sobre Direitos Fundamentais, Procedimento, Processo e Organização, no Boletim da Faculdade de Direito, Vol. LXVI, Coimbra, 1990, pág. 163].
A questão reside em saber se o valor negativo de um desses atos afeta o que cronologicamente aparece depois, abrangendo-o com a mesma consequência jurídica decorrente do valor negativo detetado no ato anterior. O que assume particular importância no caso das proibições de prova, pois quando retrospetivamente se diz, encarando globalmente certo processo crime, que determinada prova não é valida, retirando-se como consequência que a mesma, embora tenha existido, deve ser tratada como se não existisse (não tivesse existido), há que determinar complementarmente se essa inexistência abrange ou não atos processuais (factos ou provas) posteriores que apresentem alguma conexão com o que foi considerado inexistente. Essa ligação é o que doutrinariamente se qualifica como «efeito-à-distância», indagando este "da comunicabilidade ou não da proibição de valoração aos meios secundários de prova tornados possíveis à custa de meios ou métodos proibidos de prova" [Manuel da Costa Andrade, Sobre as Proibições de Prova em Processo Penal, Coimbra 1992, pág. 61].
Já antes do Código de Processo Penal atual, Figueiredo Dias, afirmava a inteira vigência entre nós da "doutrina que os alemães cognominaram do *Fernwirkung des Beweisverbots* e os americanos do *fruit of the poisonous tree* " (Para Uma reforma Global do Processo Penal Português, *in* Para uma Nova Justiça Penal, Coimbra, 1983, pág. 208).
E, é aceite que o sentido de uma norma que prescreve que a invalidade do ato nulo se estende aos que deste dependerem ou que ele possa afetar (como é o artigo 122º, nº 1 do CPP) é o de abrir caminho à ponderação que subjaz à chamada doutrina dos «frutos proibidos». O que, cotejado com a amplitude das garantias de defesa contidas no artigo 32º da CRP, permitiu ao Tribunal Constitucional (acórdão citado) considerar que certas situações de «efeito-à-distância» não deixam de constituir uma das dimensões garantísticas do processo criminal, permitindo verificar se o nexo naturalístico que, caso a caso, se considere existir entre a prova inválida e a prova posterior é, também ele, um nexo de antijuridicidade que fundamente o «efeito-à-distância», ou se, pelo contrário, existe na prova subsequente um tal grau de autonomia relativamente à primeira que a destaque substancialmente daquela.
Concluindo o Tribunal Constitucional que outro sentido não tem a doutrina

dos «frutos da árvore venenosa», desde a sua formulação no direito norte-americano, que não seja aquele que exige a ponderação do caso concreto determinando a existência, ou não, desse nexo de antijuridicidade entre a prova proibida e a prova subsequente que exige para esta última o mesmo tratamento jurídico conferido àquela.
Trata-se, assim, com a doutrina do «fruto da árvore venenosa», de estendera «regra de exclusão» às provas reflexas. Porém, esta projeção de invalidade aparece, desde os primórdios da formulação da doutrina [na jurisprudência norte americana], matizada por uma série de circunstâncias em que a prova derivada (derivada porque de alguma forma relacionada com a prova inválida) pode, não obstante, ser aceite como prova válida.
Com efeito, aceita-se que o efeito à distância não seja definido em termos de *conditio sine qua non*, ou seja, que qualquer conexão entre a prova inicial e a prova derivada contaminaria esta última, equacionando-se que nos casos em que essa conexão possa ser aparente ou formal, existindo na prova derivada um grau de autonomia que a destaque da primeira e que não determine desde logo a sua antijuridicidade.
Através de uma longa elaboração jurisprudencial o Supremo Tribunal norte-americano particularizou as circunstâncias em que uma prova reflexa deve ser excluída do efeito próprio da doutrina do «fruto da árvore venenosa». São fundamentalmente três esses grupos de circunstâncias: a chamada limitação da «fonte independente» (independente *source limitation*); a limitação da «descoberta inevitável» (*inevitable discovery limitation*); e a limitação da «mácula (nódoa) dissipada» (*purged taint limitation*).
A fonte independente reporta-se à existência de um meio probatório paralelo, autónomo em relação à prova proibida e que permite revelar os mesmos factos, ou seja, esta fonte independente cria uma nova relação causal (a prova proibida não é a única que permite revelar os factos).
A descoberta inevitável reporta-se a percursos probatórios hipotéticos, ou seja, percursos pelos quais a prova derivada poderia ter sido (não foi) obtida. De outro modo, mesmo sem a prova inicial proibida, através da investigação era inevitável obter a prova derivada. Neste caso, a prova derivada teria uma fonte autónoma, ainda que virtual, obtida por outros meios e, por isso, com uma conexão distante da prova inicial.
Por fim, a limitação da mácula respeita aos casos em que circunstâncias supervenientes interrompem a ligação, ou a atenuam, entre a prova derivada e a prova inicial.). Nesta, admite-se que uma prova, não obstante derivada de outra prova ilegal, seja aceite, sempre que os meios de alcançar aquela apresentem uma forte autonomia relativamente a esta, em termos tais que produzam uma decisiva atenuação da ilegalidade precedente. Indica-se como

exemplo o caso da admissão livre e esclarecida dos factos pelo visado, ou seja, quando o visado, de forma autónoma e com vontade livre e esclarecida decide superar o vício.
Estão em causa soluções próprias de uma ordem jurídica que é substancialmente diferente da nossa, e que muitas não têm nem poderiam ter correspondência no nosso direito. Porém, são soluções que nos podem influenciar no percurso decisivo e, sobretudo, que permitem perceber que a doutrina dos «frutos da árvore venenosa» não tem necessariamente um «efeito dominó» que arrasta todas as provas que, em quaisquer circunstâncias, apareçam em momento posterior à prova proibida e com ela possam, de alguma forma, ser relacionadas. Diversamente, trata-se com esta doutrina da procura de modelos de decisão assentes em critérios coerentes com a ponderação de interesses que justifica que, em determinadas circunstâncias, se projete a invalidade de uma prova proibida, para além de nela própria, noutras provas e, em circunstâncias distintas, se recuse tal projeção [Acórdão TC 198/2004].
Vejamos então o caso concreto.
No caso concreto a denúncia inicial teve origem numa ação de monotorização na internet das redes de partilha P2P (*peer-to-peer*) levada a cabo pela Polícia Judiciária (fls. 2 a 4) na qual foi detetado o IP (.....), através do qual, por sua vez, foram descarregados e partilhados ficheiros com designações internacionalmente conhecidas como sendo de pornografia de menores.
Usando o IP identificado na denúncia e por referência aos grupos data/hora indicados a fls. 6, foi solicitado à NOS que fornecesse todos os elementos de identificação do utilizador do IP em causa. As informações colhidas junto da NOS, a partir de dados conservados, indicam que o IP indicado na denúncia, associado àquelas comunicações denunciadas, está associado ao arguido, com morada na (.....) (fls. 12).
Nessa sequência foram realizadas buscas à habitação sita na morada apurada, designadamente ao quarto do arguido, onde foram apreendidos vários equipamentos eletrónicos (fls. 47 e 48) todos pertencentes e utilizados pelo arguido e que posteriormente foram sujeitos a exame e perícia [fls. 53 a 73-A e Anexo I].
Sujeito a primeiro interrogatório judicial de arguido detido, o arguido não prestou declarações sobre os factos.
É manifesto, no caso, que são os dados obtidos relativos às comunicações efetuadas (fls. 12), que permitem obter a morada onde vêm a ser apreendidos os equipamentos informáticos relevantes. Ora, os dados referentes ao número de acesso de cliente, ao *user* e ao endereço associados ao local das comunicações denunciadas, são dados conservados com violação de direitos

fundamentais (com intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular, sem norma que legitime essa compressão), e que, por conseguinte, são prova proibida.
E é na morada obtida através desses dados que vem a ser efetuada a busca e apreensão de diverso equipamento informático (computadores e discos externos), ao qual é efetuada perícia na qual se descobre a matéria criminal.
Dúvidas não restam que, independentemente da sua correção formal, a apreensão e perícia são consequência da prova proibida original, são causa desta, é esta prova proibida original que permite a subsequente recolha de dados com relevância criminal.
Por conseguinte, por via da doutrina do efeito à distância, porque alcançados através da prova proibida original também a busca e apreensão, o exame e perícia, os dados colhidos nos equipamentos informáticos do arguido estão contaminados. E, salvo melhor entendimento, não existe qualquer limitação para restringir este efeito à distância.
Não existe qualquer fonte independente que permitisse revelar a identificação do utilizador registado do IP, uma vez que nenhum outro meio probatório poderia conduzir à identificação do arguido como suspeito.
Não existe qualquer percurso probatório hipotético, pois só através dos dados obtidos referentes à identificação do utilizador registado do IP e respetiva morada foi possível proceder à busca e apreensão na morada que através de diligências subsequentes se veio a apurar e identificar o arguido como proprietários dos equipamentos ligados ao serviço de *internet* e como autor dos *uploads* denunciados. Não havia no processo qualquer outro meio de prova que pudesse ser obtido por outra via e que permitisse a identificação do arguido, pelo que inexiste um percurso hipotético alternativo. Nem se diga a este propósito que se poderia ter recorrido ao mecanismo previsto na Lei 42/2004, pois como supra referido, este diploma não se aplica à investigação criminal. Para além de que, a ideia de uma atividade investigatória que não foi levada a cabo, mas que iria conduzir inevitavelmente ao mesmo resultado, é uma solução importada da experiência norte americana e que não tem enquadramento no nosso ordenamento jurídico penal e processual penal.
Por fim, no que respeita à limitação da mácula dissipada, há que considerar se é possível o aproveitamento da confissão do arguido em audiência de julgamento.
Com efeito, em sede de audiência de julgamento, o arguido de forma parcial assumiu a factualidade em causa. Parcial, na medida em que não admitiu a partilha automática dos ficheiros, alegando desconhecer que os programas informáticos instalados no computador o fizessem, pois quando os instalou as

instruções eram em inglês e não percebe inglês, e na medida em que referiu que este tipo de pornografia lhe aparecia quando pesquisava outros conteúdos para adultos, admitindo, todavia, que visualizava os ficheiros e guardava alguns para ver noutro momento. Ou seja, não obstante a admissão de alguns dos factos – os factos óbvios dada a localização dos ficheiros nos suportes informáticos o arguido não confessou integralmente e sem reservas os factos. Como se refere no Acórdão 198/2004 do TC, a confissão – funciona, de forma quase intuitiva, como verdadeiro paradigma de uma prova subsequente autónoma, concretamente por decorrer de um ato de vontade – de uma decisão de agir de determinada forma – de quem é advertido (trata-se de prova produzida na audiência de julgamento) do sentido das declarações que eventualmente venha a prestar (v. artigo 343º, nº 1 do CPP) e que se encontra assistido por advogado.
No caso, cremos que a admissão parcial dos factos pelo arguido, não deve ser considerada como forma autónoma e independente de acesso aos factos, sem conexão estreita com a prova proibida, na medida em que é motivada pela apreensão e exame aos equipamentos informáticos onde é descoberta matéria com relevância criminal (que é prova proibida contaminada pela prova proibida original). As declarações do arguido só surgem perante a evidência da apreensão, só surgem por causa daquela, para a justificar e, por isso são um efeito sequencial. Tanto assim, que na parte que não decorre da evidência digital o arguido não assume. As declarações do arguido surgem na sequência da prova inicialmente recolhida, no pressuposto da validade dos elementos de prova – apreensão e perícia – equacionando-se que caso soubesse da sua invalidade as suas declarações poderiam ter sido outras. Note-se que em momento algum o arguido invocou a sua invalidade. O facto de já serem posteriores ao Acórdão do Tribunal Constitucional não afasta o que se acabou de dizer, pois mesmo com a garantia de assistência de um advogado, naquele momento a prova fora apresentada ao Tribunal e o arguido desconhecia que validade lhe poderia ser atribuída. Não é seguro dizer que, mesmo consciente do vício original, o arguido prestaria as mesmas declarações.
Com efeito, e ao contrário da situação analisada no Acórdão do Tribunal da Relação de Coimbra de 22 de fevereiro de 2023, publicado em texto integral no site *www.dgsi.pt*, neste processo em momento algum do mesmo foi suscitada a questão da invalidade da prova [o que reforça a ideia de que as declarações do arguido surgem no pressuposto da validade dos elementos de prova] e não há uma confissão integral e sem reservas, que permita, só por si, dar por provados os factos constantes da acusação.
Também ao contrário da situação analisada no Acórdão 198/2004 do T.C., neste caso, a confissão não tem tal autonomia que possibilite um acesso aos

factos totalmente destacável de qualquer outra forma de acesso anteriormente surgida e afetada por um valor negativo. Com efeito, a admissão genérica pelo arguido de que acedia através da *internet* a *sites* de pornografia de menores, fazendo *downloads* de conteúdos que guardava mas não partilhava, não permite, no caso, só por si, imputar-lhe os factos tal como descritos na acusação. Donde, cremos não se poder igualmente valorar as declarações prestadas pelo arguido por estarem igualmente contaminadas pelo vício da prova inicial.
E, por conseguinte, toda a factualidade é não provada, sendo certo que, não se demonstrando a factualidade objetiva, naturalmente fica prejudicado o conhecimento e vontade do arguido.
*
4. **Enquadramento Jurídico-Penal**
Ao arguido é imputada a prática, em autoria material e em concurso efetivo de:
- 3866 crimes de pornografia de menores, na forma agravada, previsto e punido pelos artigos 176.º, n.º 1, al. c) e d), n.º 5 e 177.º, n.º 7 do Código Penal;
- 850 crimes de pornografia de menores, na forma agravada, previsto e punido pelos artigos 176.º, n.º 1, al. c) e d) e n.º 5 e 177.º, n.º 6 do Código Penal,
- 2976 crimes de pornografia de menores, na forma agravada, previsto e punido pelos artigos 176.º, n.º 1, al. c) e d), n.º 5 e 177.º, n.º 7 do Código Penal;
- 180 crimes de pornografia de menores, na forma agravada, previsto e punido pelos artigos 176.º, n.º 1, al. c) e d), n.º 5 e 177.º, n.º 6 do Código Penal.
Dispõe o artigo 176.º do Código Penal, sob a epígrafe “Pornografia de Menores” que:
1 - *Quem*:
a) *Utilizar menor em espetáculo pornográfico ou o aliciar para esse fim*;
b) *Utilizar menor em fotografia, filme ou gravação pornográficos, independentemente do seu suporte, ou o aliciar para esse fim*;
c) *Produzir, distribuir, importar, exportar, divulgar, exibir, ceder ou disponibilizar a qualquer título ou por qualquer meio, os materiais previstos na alínea anterior*;
d) *Adquirir, detiver ou alojar materiais previstos na alínea b) com o propósito de os distribuir, importar, exportar, divulgar, exibir ou ceder; é punido com pena de prisão de um a cinco anos*.
2 - *Quem praticar os atos descritos no número anterior profissionalmente ou com intenção lucrativa é punido com pena de prisão de um a oito anos*.
3 - *Quem praticar os atos descritos nas alíneas a) e b) do n.º 1 recorrendo a*

violência ou ameaça grave é punido com pena de prisão de 1 a 8 anos.
4 - *Quem praticar os atos descritos nas alíneas c) e d) do n.º 1 utilizando material pornográfico com representação realista de menor é punido com pena de prisão até dois anos.*
5 - *Quem, intencionalmente, adquirir, detiver, aceder, obtiver ou facilitar o acesso, através de sistema informático ou qualquer outro meio aos materiais referidos na alínea b) do n.º 1 é punido com pena de prisão até 2 anos.*
6 - *Quem, presencialmente ou através de sistema informático ou por qualquer outro meio, sendo maior, assistir, facilitar ou disponibilizar acesso a espetáculo pornográfico envolvendo a participação de menores é punido com pena de prisão até 3 anos.*
7 - *Quem praticar os atos descritos nos n.ºs 5 e 6 com intenção lucrativa é punido com pena de prisão até 5 anos.*
8 - *Para efeitos do presente artigo, considera-se pornográfico 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.*
9 - *A tentativa é punível*".
Nos termos do artigo 177.º do mesmo código, dispõe-se que:
"1 - *As penas previstas nos artigos 163.º a 165.º e 167.º a 176.º são agravadas de um terço, nos seus limites mínimo e máximo, se a vítima*:
a) *For ascendente, descendente, adotante, adotado, parente ou afim até ao segundo grau do agente; ou*
b) *Se encontrar numa relação familiar, de coabitação, de tutela ou curatela, ou de dependência hierárquica, económica ou de trabalho do agente e o crime for praticado com aproveitamento desta relação.*
c) *For pessoa particularmente vulnerável, em razão de idade, deficiência, doença ou gravidez.*
2 - *As agravações previstas no número anterior não são aplicáveis nos casos da alínea c) do n.º 2 do artigo 169.º e da alínea c) do n.º 2 do artigo 175.º*
3 - *As penas previstas nos artigos 163.º a 167.º e 171.º a 174.º são agravadas de um terço, nos seus limites mínimo e máximo, se o agente for portador de doença sexualmente transmissível.*
4 - *As penas previstas nos artigos 163.º a 168.º e 171.º a 175.º, nos n.ºs 1 e 2 do artigo 176.º e no artigo 176.º-A são agravadas de um terço, nos seus limites mínimo e máximo, se o crime for cometido conjuntamente por duas ou mais pessoas.*
5 - *As penas previstas nos artigos 163.º a 168.º e 171.º a 174.º são agravadas de metade, nos seus limites mínimo e máximo, se dos comportamentos aí descritos resultar gravidez, ofensa à integridade física grave, transmissão de*

agente patogénico que crie perigo para a vida, suicídio ou morte da vítima.
6 - *As penas previstas nos artigos 163.º a 165.º, 168.º, 174.º, 175.º e no n.º 1 do artigo 176.º são agravadas de um terço, nos seus limites mínimo e máximo, quando os crimes forem praticados na presença ou contra vítima menor de 16 anos;*
7 - *As penas previstas nos artigos 163.º a 165.º, 168.º e 175.º e no n.º 1 do artigo 176.º são agravadas de metade, nos seus limites mínimo e máximo, se a vítima for menor de 14 anos*.
8 - *Se no mesmo comportamento concorrerem mais do que uma das circunstâncias referidas nos números anteriores só é considerada para efeito de determinação da pena aplicável a que tiver efeito agravante mais forte, sendo a outra ou outras valoradas na medida da pena*".
No caso concreto, considerando que não foram provados quaisquer dos factos constantes da acusação, não se mostra necessário analisar os elementos objetivos e subjetivos do tipo de crime, ou sequer menos do número de crimes cometidos, impondo-se, sem maiores considerações, a absolvição do arguido. (…).»

2.3. **Apreciação do mérito do recurso**
A questão central suscitada no recurso em apreço, interposto pelo Ministério Público, do acórdão absolutório proferido pelo Tribunal *a quo*, é a da validade/legalidade da prova obtida, através dos dados facultados pela operadora de telecomunicações NOS, atinentes à identificação e à morada do utilizador do IP (…..), detetado no decurso de uma ação de monitorização na *internet* desenvolvida pela Polícia Judiciária em redes de partilha "*Peer-to-peer*", relacionados com pornografia infantil.
O Tribunal *a quo*, no acórdão recorrido, entendeu que a informação solicitada pelo MP e prestada pela operadora NOS, identificando o arguido, nome e morada, como sendo o utilizador do referenciado IP, com a indicação das datas e horas do início e termo da ligação, nos termos em que ocorreu, respeita a dados conservados, "metadados", obtidos/fornecidos pela operadora, ao abrigo de disposições legais, designadamente, do artigo 4º da Lei n.º 32/2008, de 17 de julho, abrangidas pela declaração de inconstitucionalidade, com força obrigatória e geral, decidida pelo Tribunal Constitucional, no Acórdão n.º 268/2022.
O recorrente Ministério Público divergindo desse entendimento, sustenta que os dados solicitados e facultados pela operadora de telecomunicações NOS, atinentes à identificação e à morada do utilizador de um determinado IP, num concreto lapso temporal, foram legitima e validamente obtidos, ao abrigo do

disposto no artigo 14º, n.ºs 1 a 4, da Lei n.º 32/2008, de 17 de julho, que se mantém em vigor, constituindo prova legal, não estando abrangidos pela enunciada declaração de inconstitucionalidade. Em apoio da posição defendida, indica o recorrente diversos acórdãos proferidos pelos Tribunais Superiores, dos quais dois desta Relação de Évora, um deles em que a ora relatora também o foi, tratando-se do acórdão de 09/05/2023, proc. n.º 150/19.0TELSB.E1.
Vejamos:
Salvo o devido respeito pelo entendimento contrário, defendido pelo recorrente Ministério Público, consideramos, tal como se decidiu no acórdão recorrido, que, no caso concreto, os dados obtidos/fornecidos pela operadora NOS, respeitantes à identificação e morada do arguido, como utilizador do IP detetado em redes de partilha "*peer-to-peer*", relacionadas com pornografia de menores, com referência/indicação das datas e horas de início e termo da ligação a partir desse IP, se tratam de dados de tráfego conservados, nos termos do artigo 4º, n.º 1, al. a), n.º 2 al. b), da Lei 32/2008 e, como tal, abrangidos pela declaração de inconstitucionalidade a que se vem fazendo referência.
Explicitando:
Conforme vem sendo frisado pela jurisprudência, em matéria de telecomunicações, há que distinguir os dados de base (elementos de suporte técnico e de conexão estranhos à própria comunicação em si mesma, designadamente os relacionados com a identificação, nome e endereço, do assinante ou do utilizador registado, a quem o endereço do protocolo IP está atribuído), os dados de tráfego (elementos que se referem já à comunicação, mas não envolvem o seu conteúdo, por exemplo, referentes à localização do utilizador do equipamento móvel ou da rede, bem assim como do destinatário, data e hora da comunicação, duração da mesma, frequência, etc.) e os dados de conteúdo (elementos que se referem ao próprio conteúdo da comunicação) [1].
No referente aos dados de localização, inseridos no âmbito dos dados de tráfego, como se refere no Acórdão da RC de 12/10/2022[2], «são os dados tratados numa rede de comunicações electrónicas que indicam a posição geográfica do equipamento terminal de um assistente ou de qualquer utilizador de um serviço de comunicações electrónicas acessíveis ao público. Só cabem dentro dos dados de localização os autênticos dados de comunicação ou de tráfego, i.e., aqueles que se reportam a comunicações efectivamente realizadas ou tentadas/falhadas entre pessoas.»
Apenas os dados de tráfego e localização conservados/armazenados pelos fornecedores de serviços de comunicações eletrónicas ou das redes públicas

de comunicações estão abrangidos pela declaração de inconstitucionalidade das normas dos artigos 4º, 6º e 9º da Lei n.º 32/2008, de 17 de julho, do aludido Acórdão do TC n.º 268/2022.
Como assinalou o TC no referenciado Acórdão, com referência às normas do artigo 4º em conjugação com o artigo 6º da Lei n.º 32/2008 e, concretamente, no respeitante à «obrigação de conservação dos *dados de tráfego,* gerados a propósito de uma específica comunicação, com especial relevância para os *dados de localização.*
A conservação dos dados de localização, ainda que não sejam gerados em virtude de uma comunicação pessoal, materializam uma agressão mais intensa à intimidade da vida privada dos sujeitos privados do que a preservação dos dados de base, ao permitirem identificar, a todo o tempo, a posição e os movimentos dos utilizadores. O mesmo se diga quanto aos dados de tráfego, mesmo quando não pressupõem uma comunicação (ou sua tentativa) interpessoal, como os sítios da *internet* consultados, por quanto tempo, em que momento e a quantidade de tráfego gerado. Estes dados permitem traçar um perfil do utilizador, identificar os seus interesses e mesmo reconhecer, em certos casos, o tipo de conteúdos consultados.»
Já no referente aos dados de base, relacionados com a identificação do titular de um número de telefone ou de um IMEI, no caso de ser um assinante registado, bem como o utilizador de determinado IP, tratando-se de elementos recolhidos aquando da contratação do serviço de telecomunicações e que se mantêm independentemente de qualquer comunicação efetuada e a que a autoridade judiciária pode ter acesso, designadamente, por via do disposto no artigo 14º da Lei n.º 109/2009, de 15 de setembro, não respeitando à privacidade da vida da pessoa ou à sua esfera íntima, em termos de encontrarem proteção, no contexto dos bens jurídicos protegidos pela Constituição[3], não se encontram abrangidos pela declaração de inconstitucionalidade emanada do Acórdão do TC n.º 268/2022.
A distinção entre dados de base e dados de tráfego e de localização, o respetivo regime de conservação, bem assim como o regime de transmissão dos dados de tráfego e de localização, estão atualmente definidos na Lei n.º 18/2024, de 5 de fevereiro – que regula o acesso a metadados referentes às comunicações eletrónicas para fins de investigação criminal, procedendo à alteração da Lei n.º 32/2008, de 17 de julho, conformando-a com os acórdãos do Tribunal Constitucional n.º 268/2022 e 800/2023 –.
Para melhor compreender os contornos da questão em apreciação, atentemos, ainda que sucintamente, a algumas das principais alterações introduzidas pela Lei n.º 18/2024:
De harmonia com o estabelecido neste diploma legal (cf. artigo 6º, n.º 1), os

dados que deverão ser conservados, pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações e para efeitos da finalidade exclusiva, da investigação, deteção e repressão de crimes graves, por parte das autoridades competentes, pelo período de um ano, a contar da data da conclusão da comunicação, são os seguintes:
a) Os dados relativos à identificação civil dos assinantes ou utilizadores de serviços de comunicações publicamente disponíveis ou de uma rede pública de comunicações;
b) Os demais dados de base;
c) Os endereços de protocolo IP atribuídos à fonte de uma ligação (cf. artigo 6º, n.º 1, da Lei n.º 32/2008, de 17 de julho, na redação dada pela Lei n.º 18/2024, de 5 de fevereiro).
No respeitante aos dados de tráfego e de localização apenas podem ser objeto de conservação mediante autorização judicial (cabendo a competência para o efeito ao Supremo Tribunal de Justiça – cf. n.º 7 do artigo 6º da Lei n.º Lei n.º 32/2008, de 17 de julho e n.º 4 dos artigos 47º e 54º da Lei da Organização do Sistema Judiciário, todos na redação dada pela Lei n.º 18/2024, de 5 de fevereiro), fundada na sua necessidade para a finalidade «*da investigação, deteção e repressão de crimes graves por parte das autoridades competentes*» (prevista no n.º 1 do artigo 3º da Lei n.º 32/2008), devendo limitar-se ao estritamente necessário para a prossecução dessa finalidade e cessando logo que se confirme a desnecessidade da sua conservação (cf. artigo 6º, n.ºs 2 e 5, da Lei n.º 32/2008, de 17 de julho, na redação dada pela Lei n.º 18/2024, de 5 de fevereiro).
Em ordem a conformar a Lei n.º 32/2008, com os Acórdãos do TC n.º 268/2022 e n.º 800/2023[4], passou a prever-se que, na fase de inquérito, o despacho que autoriza a transmissão dos dados deverá ser notificado ao seu titular no prazo máximo de 10 dias, salvo se o Ministério Público considerar que a referida notificação «*comporta risco de pôr em causa a investigação, dificultar a descoberta da verdade ou criar perigo para a vida, para a integridade física ou psíquica ou para a liberdade dos participantes processuais, das vítimas do crime ou de outras pessoas devidamente identificadas*», podendo, nessa situação, «*solicitar ao juiz de instrução criminal que protele a notificação, sendo esta realizada logo que a razão do protelamento deixara de existir ou, o mais tardar, no prazo máximo de 10 dias após ser proferido despacho de encerramento*» do inquérito (cf. n.ºs 7 e 8 do artigo 9.º da Lei n.º 32/2008, de 17 de julho, na redação dada pela Lei n.º 18/2024, de 5 de fevereiro).
Revertendo ao caso dos autos, importa atentar no seguinte:
Na sequência da comunicação efetuada PJ, lavrada em auto de notícia, da

deteção, no decurso de ação de monotorização na *internet*, em redes de partilha P2P (*Peer-to-peer*), com foco na descarga de ficheiros relacionados com pornografia de menores, do endereço IP (.....), através do qual se encontravam disponíveis para serem descarregados e partilhados ficheiros, nos grupos, datas e horas indicados a fls. 6, o Ministério Público, através de formulário próprio, junto a fls. 9, solicitou à operadora NOS, indicando as disposições do artigo 14º da Lei n.º 109/2009 e dos artigos 267º, 262º e 164º, todos do CPP e assinalando a quadrícula C "*Sobre endereços de IP*": «*Todos os elementos disponíveis de identificação do IP descriminado a fls. 6 (cuja cópia se anexa para melhor esclarecimento), nos grupos data/hora e fuso horário ali indicados*.»
O ofício remetido pela operadora NOS, em resposta à solicitação do Ministério Público, datado de 13/05/2022 e inserto a fls. 10 dos autos é do seguinte teor:
«(...)
NOS COMUNICAÇÕES, S.A. vem (...) remeter em suporte digital os dados de tráfego solicitados, ressalvando que a(s) data(s) e hora(s) indicadas são referentes à hora e local de Portugal Continental.
Mais informa que os dados de identificação dos números ativos na NOS e/ou os carregamentos associados aos mesmos podem ser consultados no TMENU / NOS Comunicações S.A.
Para os efeitos tidos por convenientes, informa-se que a cópia do ficheiro ora enviado será eliminada pela NOS após o decurso de um período de 3 meses sobre a presente data.
(...).»
Os dados em apreço, fornecidos em suporte digital (cf. CD junto a fls. 11), de onde foi extraído o "Report 1" constante a fls. 12 dos autos, tratam-se de dados de tráfego conservados pela NOS.
Não estamos, pois, *in casu*, perante dados, respeitantes à identificação do assinante e ao endereço de protocolo IP atribuídos à fonte de uma ligação, sem qualquer conexão com as comunicações efetuadas, que hajam sido fornecidos pela NOS com base no contrato firmado com o cliente.
Esta diferença é crucial para que a solução preconizada seja contrária àquela que propugnamos no mencionado acórdão de 09/05/2023, proferido no âmbito do proc. n.º 150/19.0TELSB.E1.
No caso tratado nesse acórdão, conquanto tivessem sido também obtidos/fornecidos pela operadora de telecomunicações dados de tráfego conservados/armazenados, os mesmos não foram utilizados/valorados, pelo tribunal recorrido, para sedimentar a convicção formada, dando como provados os factos impugnados pelo ali recorrente, tendo a identificação do utilizador e o endereço de IP associado ao perfil do *Facebook Messenger* sido apurado

através de outros meios de prova.
Acontece que a situação em causa nos presentes autos, é totalmente diversa.
Como se refere no Acórdão recorrido:
«Os presentes autos, tal como decorre do teor do auto de notícia de fls. 2 a 4, iniciam-se com uma ação de monotorização na *internet* por parte da PJ, em redes de partilha P2P (*peer-to-peer*), com foco na descarga de ficheiros com assinatura digital específica relacionados com pornografia de menores e onde foi detetado um determinado IP que disponíveis para partilha, naquele momento, alguns desses ficheiros.
A partir desse IP, e como decorre de fls. 9 (frente e verso) foi solicitado pelo Ministério Público à operadora de comunicações NOS o envio de todos os elementos de identificação do utilizador do IP identificado a fls. 6 nos grupos data/hora e fuso horário indicados.
O que veio acontecer como decorre da informação da NOS de fls. 12.
Todavia, da conjugação do teor de fls. 9 e 12 decorre igualmente que a informação foi prestada por referência às comunicações estabelecidas nos grupos data/hora indicados a fls. 6 e não por referência a informações conservadas para fins comerciais ou inerentes a elementos contratuais.
Donde, salvo melhor entendimento, e pese embora o formulário utilizado pelo Ministério Público para solicitar as informações às operadoras não o invoque expressamente, impõe-se no caso, invocar o regime da Lei 32/2008, de 17.07, e, por consequência, o Acórdão do Tribunal Constitucional n.º 268/2022, que declarou "a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4.º da Lei n.º 32/2008, de 17 de julho, conjugada com o artigo 6.º da mesma Lei" e "a inconstitucionalidade, com força obrigatória geral, da norma do artigo 9.º da Lei n.º 32/2008, de 17 de julho, relativa à transmissão de dados armazenados às autoridades competentes para a investigação, deteção e repressão de crimes graves, na parte em que não 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 a integridade física de terceiros".
Com efeito, pese embora o formulário utilizado pelo Ministério invoque como fundamento legal para o pedido o artigo 14.º da Lei 109/2009 e os artigos 267.º, 262.º e 164.º do Código de Processo Penal, os dados solicitados são obtidos a partir de um concreto IP em conexão com uma certa comunicação realizada (as indicadas a fls. 6) e não a partir de uma relação contratual. Por conseguinte, dúvidas não restam que se tratam de dados conservados pela operadora nos termos do artigo 4.º, n.º 1, al. a), n.º 2 al. b) da Lei 32/2008. Ou seja, dados que integram as categorias dos dados que devem ser conservados

nos termos do artigo 4.º da Lei 32/2008 e que foi declarada inconstitucional com fundamento na violação do disposto nos números 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o artigo 18.º, n.º 2 da Constituição da República Portuguesa, por se considerar que a conservação de tais dados relativos às comunicações realizadas interfere com o direito de acesso aos seus dados pessoais informatizados e à proibição de acesso por terceiros e com o direito à reserva da intimidade da vida privada e ao livre desenvolvimento da personalidade.
(…)»
Merece-nos inteira concordância o assim decidido pelo Tribunal *a quo*.
Na verdade, tal como se considerou, no acórdão recorrido, os dados fornecidos pela operadora NOS, que permitiram identificar o utilizador do IP (…..) – detetado no decurso de uma ação de monitorização na *internet* desenvolvida pela Polícia Judiciária em redes de partilha "*Peer-to-peer*", relacionados com pornografia infantil –, respetivo endereço, horas de início e termo da ligação, efetuada a partir desse IP, consubstanciam dados conservados, tratando-se de dados de tráfego, reportados às comunicações efetuadas, nas datas indicadas e nos horários assinalados, com a identificação do utilizador do IP em questão e o respetivo endereço.
Não se tratam, pois, de dados de base, obtidos a partir da relação contratual estabelecida entre a operadora NOS e o cliente, mas de dados gerados pela utilização da rede.
Salvo o devido respeito pelo entendimento propugnado pelo recorrente Ministério Público, em face da declaração de inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4º, conjugada com a do artigo 6º, da Lei n.º 32/2008, de 17 de julho, com fundamento de que elas permitiam uma lesão desproporcionada da reserva da intimidade e da vida privada dos cidadãos, não podem, por via do disposto no artigo 14º da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), ser obtidos dados de tráfego conservados, o que se traduziria em seguir um «caminho espúrio»[5], face à enunciada declaração de inconstitucionalidade e aos fundamentos que a determinaram, contornando-a.
Os dados que podem ser obtidos pela autoridade judiciária, no caso pelo Ministério Público, por via do disposto no artigo 14º da Lei n.º 109/2009, de 15 de setembro, estando em investigação de crimes enunciados no artigo 11º, n.º 1, do mesmo diploma legal, designadamente, crimes cometidos por meio de sistema informático – alínea b) –, respeitam a dados permanentes, sem qualquer conexão a comunicações realizadas, como é o caso da identificação, com a indicação do nome e morada, do cliente utilizador de um determinado IP, resultante da relação contratual estabelecida entre a operadora e o cliente.

Isso mesmo resulta do n.º 4 do artigo 14º da Lei n.º 109/2009, ao estatuir que:

«O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar:
a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;
b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou
c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.»
Esta linha de entendimento vem sendo sufragada pelo Supremo Tribunal de Justiça, entre outros, no Acórdão de 13/04/2023[7], cujo sumário se transcreve:
«I - O STJ tem decidido que os dados identificativos do titular de IP assumem um caráter permanente, que resultam dos elementos contratuais celebrados pelo cliente com a fornecedora de serviço de telecomunicações, pelo que nada têm que ver com dados relativos às comunicações eletrónicas em si mesmo consideradas.
Não respeitando estes dados a comunicações efetuadas, tratadas e armazenadas ao abrigo da Lei n.º 32/2008, de 17-07, mas a elementos contratuais com carácter permanente que podem ser obtidos independentemente de qualquer comunicação, a sua obtenção pelas autoridades judiciárias cai fora do âmbito deste diploma e da declaração de inconstitucionalidade do acórdão do Tribunal Constitucional.
II - Com a declaração de inconstitucionalidade com força obrigatória geral do art. 4.º da Lei n.º 32/2008, de 17-07, a conservação e armazenamento de dados de base, designadamente, de dados de subscritor do IP pelos fornecedores de serviço, não passou a ser proibida.
III - A Lei n.º 41/2004, que permite, além do mais, a conservação de dados de identificação dos clientes das operadoras de telecomunicações, não foi abrangida pela declaração de inconstitucionalidade do acórdão do TC n.º 268/2022.
IV - Também a Lei n.º 109/2009, de 15-09, que embora não regule a conservação de dados, regula a sua obtenção, não foi objeto de declaração de

inconstitucionalidade pelo acórdão do TC n.º 268/2022.
V - O art. 14.º da Lei do Cibercrime, permite a obtenção, pelas autoridades judiciárias, dos dados de subscritor e de acesso, elencados nas diferentes alíneas do n.º 4, incluindo o IP, para prova de todos os crimes incluídos na previsão do art. 11.º, n.º 1, ou seja, dos crimes previstos na Lei do Cibercrime, dos cometidos por meio de um sistema informático ou, em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.
VI - Estando em causa a investigação de um crime de pornografia de menores, cometido por meio de um sistema informático e em relação ao qual se mostrava necessário proceder à recolha de prova em suporte eletrónico, podia a autoridade judiciária, ao abrigo do art.14.º daquele diploma, requerer, como requereu, à fornecedora de serviço, a identificação do subscritor do IP, para prova do crime pela pessoa visada.»
Sucede que, no caso dos autos, tal como referimos, os dados fornecidos pela operadora NOS, estão conexionados com comunicações realizadas, indicando-se as datas e horas em que tiveram lugar, a localização do endereço IP e o respetivo utilizador como sendo o arguido.
Neste quadro, entendemos ter o Tribunal *a quo* decidido corretamente, ao considerar estarem em causa dados de tráfego, que foram transmitidos pela operadora NOS, ao abrigo do disposto no artigo 4º da Lei n.º 32/2008, de 17 de julho, norma esta que foi declarada inconstitucional, com força obrigatória geral, no Acórdão do TC n.º 268/2022.
Nessa decorrência, acompanha-se o entendimento do Tribunal *a quo* de se estar perante uma proibição de prova, nos termos do disposto no artigo 126º, n.º 3, do CPP, posto essa prova ter sido obtida, «fora dos casos admitidos pela lei e sem o consentimento do respetivo titular, mediante intromissão na vida privada, no domicílio e nas telecomunicações» e, como tal, não podendo ser utilizada, nem valorada.
Tendo sido com base nessa prova que foi possível localizar o endereço IP indicado e, nessa sequência, sido determinada a realização da busca domiciliária, à residência do arguido, em resultado da qual foi apreendido o equipamento/material informático, que veio a ser objeto de exame pericial (conforme relatório junto a fls. 53 a 73-A do Anexo I), por força do "efeito à distância" daquela proibição de prova (prova primária), a apreensão do equipamento/material informático que teve lugar no âmbito da busca domiciliária realizada, mostra-se "contaminada", não podendo ser utilizada a prova obtida por esse meio (prova sequencial ou secundária).
Merece-nos também concordância a conclusão a que chegou o Tribunal *a quo*, no sentido da não verificação, no caso concreto, de qualquer exceção ou limitação do "efeito à distância", decorrente da assinalada proibição de prova,

designadamente, a existência de prova sequencial obtida através de uma fonte independente e autónoma da prova inquinada ou a ocorrência da situação de "mácula dissipada", com o sentido e alcance explicitados no acórdão recorrido e que aqui damos por reproduzidos.
As declarações prestadas pelo arguido, na audiência de julgamento, tendo admitido alguns dos factos que lhe são imputados na acusação, cingiu-se, segundo se refere no acórdão recorrido (e não foi posto em causa no recurso), aos factos óbvios, dada a localização dos ficheiros nos suportes informáticos apreendidos, não deve ser considerada como meio de prova autónomo, sem conexão estreita com a prova proibida.
Importará referir que, neste domínio, certo setor da doutrina[8] defende que ocorrendo uma proibição de prova, mesmo quando haja confissão do arguido, este tem de ser previamente informado de que aquela prova não poderá ser contra ele valorada, para poder haver "limpeza de mácula".
Acolhemos as considerações expendidas pelo Tribunal *a quo* que o levaram a afastar a valoração das declarações do arguido como prova autónoma, não inquinada pela prova (primária) proibida. Reproduzem-se, por isso, essas considerações:
«(…) a admissão parcial dos factos pelo arguido, não deve ser considerada como forma autónoma e independente de acesso aos factos, sem conexão estreita com a prova proibida, na medida em que é motivada pela apreensão e exame aos equipamentos informáticos onde é descoberta matéria com relevância criminal (que é prova proibida contaminada pela prova proibida original). As declarações do arguido só surgem perante a evidência da apreensão, só surgem por causa daquela, para a justificar e, por isso são um efeito sequencial. Tanto assim, que na parte que não decorre da evidência digital o arguido não assume.
As declarações do arguido surgem na sequência da prova inicialmente recolhida, no pressuposto da validade dos elementos de prova – apreensão e perícia – equacionando-se que caso soubesse da sua invalidade as suas declarações poderiam ter sido outras.
Note-se que em momento algum o arguido invocou a sua invalidade.
O facto de já serem posteriores ao Acórdão do Tribunal Constitucional não afasta o que se acabou de dizer, pois mesmo com a garantia de assistência de um advogado, naquele momento a prova fora apresentada ao Tribunal e o arguido desconhecia que validade lhe poderia ser atribuída. Não é seguro dizer que, mesmo consciente do vício original, o arguido prestaria as mesmas declarações.
Com efeito, e ao contrário da situação analisada no Acórdão do Tribunal da Relação de Coimbra de 22 de fevereiro de 2023, publicado em texto integral

no *site www.dgsi.pt*, neste processo em momento algum do mesmo foi suscitada a questão da invalidade da prova [o que reforça a ideia de que as declarações do arguido surgem no pressuposto da validade dos elementos de prova] e não há uma confissão integral e sem reservas, que permita, só por si, dar por provados os factos constantes da acusação.
Também ao contrário da situação analisada no Acórdão 198/2004 do T.C., neste caso, a confissão não tem tal autonomia que possibilite um acesso aos factos totalmente destacável de qualquer outra forma de acesso anteriormente surgida e afetada por um valor negativo. Com efeito, a admissão genérica pelo arguido de que acedia através da *internet* a *sites* de pornografia de menores, fazendo *downloads* de conteúdos que guardava mas não partilhava, não permite, no caso, só por si, imputar-lhe os factos tal como descritos na acusação.
Donde, cremos não se poder igualmente valorar as declarações prestadas pelo arguido por estarem igualmente contaminadas pelo vício da prova inicial.»
Por todo o exposto, havendo que concluir não existir suporte probatório passível de poder determinar a modificação da decisão de facto proferida pelo Tribunal *a quo*, resultando não provada toda a factualidade constante do libelo acusatório, deve manter-se a absolvição do arguido/recorrente, nos termos decididos no acórdão recorrido.
Improcede, por conseguinte, o recurso.

3. DECISÃO
Pelo exposto e em conformidade, **acordam** os Juízes da Secção Criminal do Tribunal da Relação de Évora, em **negar provimento ao recurso** interposto pelo arguido/recorrente *(A)* e, em consequência, confirmar o acórdão absolutório recorrido.
Sem tributação.
Notifique.

Évora, 05 de março de 2024
Fátima Bernardes
Fernando Pina
Filipa Costa Lourenço

---

[1] Cf., entre outros, Ac. da RL de 03/03/2022, proc. n.º 106459/20.6YIPRT.L1-6 e Ac. do STJ de 06/09/2022, proc. 243/17.0T9PRT-K.S1, in www.dgsi.pt

[2] Proferido no proc. n.º 538/22.9JALRA.C1, in www.dgsi.pt.
[3] Cf. citado Acórdão da RL de 03/03/2022.
[4] Este último proferido, em sede de fiscalização preventiva de constitucionalidade, pronunciando-se «pela inconstitucionalidade da norma constante do artigo 2.º do Decreto n.º 91/XV, da Assembleia da República, publicado no Diário da Assembleia da República n.º 26, II Série A, de 26 de outubro de 2023, e enviado ao Presidente da República para promulgação como lei, na parte em que altera o artigo 4.º da Lei n.º 32/2008, de 17 de julho, conjugado com o artigo 6.º da mesma lei, quanto aos dados previstos no n.º 2 do mencionado artigo 6.º, por violação do disposto nos números 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo 18.º, todos da Constituição»
[5] Neste sentido, a propósito dos de dados respeitantes à localização celular conservada, vide, Ac. da RC de 10/12/2022, proc. n.º 538/22.9JALRA.C1, in www.dgsi.pt.
[6] Nosso sublinhado.
[7] Proferido no proc. n.º 390/16.3TELSB-A.S1, in www.dgsi.pt.
[8] Cf., entre outros, Helena Morão, “Efeito-â-distância das proibições de prova e declarações confessórias – o acórdão n.º 198/2004 do Tribunal Constitucional e o argumento “the cat is out of the bag”, in Revista Portuguesa de Ciência Criminal, Ano 22, outubro-dezembro 2012, pág. 723.