jurisprudência.pt

Tribunal da Relação de Lisboa
Processo nº 351/20.8PZLSB-C.L1-5

Relator: MANUEL ADVÍNCULO SEQUEIRA
Sessão: 09 Novembro 2021
Número: RL
Votação: UNANIMIDADE
Meio Processual: RECURSO PENAL
Decisão: PROVIDO

APREENSÃO DE DADOS INFORMÁTICOS **CORREIO ELECTRÓNICO**

Sumário

- A apreensão de dados informáticos a que a Lei do Cibercrime se refere não equivale à apreensão prevista no Código de Processo Penal, pela própria natureza das coisas.
- Esta última passa por desapossar alguém da coisa corpórea, enquanto a apreensão do conteúdo digital, bastas vezes virtual e armazenado num servidor em qualquer lugar do mundo, facilmente possibilita, especialmente quanto ao correio electrónico, a continuação do acesso pelo utilizador original ao seu conteúdo, o qual, em bruto, é apenas linguagem binária.
- Apreensão de dados informáticos tem muito mais a ver com a respectiva percepção e assim apenas ocorre quando o conteúdo de mensagens de correio electrónico é desvendado e junto ao processo em linguagem comum.
- Não por acaso, é apenas nesse momento que ocorre a efectiva compressão do direito à inviolabilidade da correspondência que a lei visa salvaguardar com as garantias e formalidades processuais que impõe, designadamente a da reserva judicial no que respeita àquela correspondência electrónica.
(Sumariado pelo relator)

Texto Integral

Acordam, em conferência, na 5ª Secção Criminal do Tribunal da Relação de Lisboa.

No âmbito deste processo foi declarado nulo despacho do Ministério Público, bem como a obtenção de prova electrónica em consequência daquele.
*

Interpôs o Ministério Público o presente recurso concluindo:
"1ª) No dia 06.11.2020, foram apreendidos aos arguidos AA, BB, CC e DD, entre outros objectos, diversos telemóveis e outros equipamentos informáticos;
2ª) Por despachos proferidos nos dias 12.11.2020 (cfr. fls. 2130 a 2133) e 26.11.2020 (cfr. fls. 2289 a 2298) foi determinada a realização de perícias e pesquisas informáticas aos referidos sistemas informáticos, tendo sido solicitado ao Mm.° Juiz … do Juízo Central de Instrução Criminal por despacho proferido no dia 06.04.2021 (cfr. fls. 3426), que tomasse conhecimento e autorizasse a junção aos autos das mensagens de correio electrónico e outros registos de natureza semelhante, os quais se encontram armazenados em suporte digital (seis DVD's) e que foram encontrados na sequência da pesquisa informática ordenada no âmbito dos presentes autos;
3ª) O Mm.° Juiz … do Juízo Central de Instrução Criminal determinou a nulidade do despacho proferido pelo Ministério Público a fls. 1684, 2130 e 2289, bem como a nulidade da prova obtida a partir do correio electrónico e registos de natureza semelhante apreendido aos arguidos AA, BB, CC e DD, ordenando a eliminação dos suportes informáticos em causa após o trânsito em julgado daquela decisão;
4ª) A remissão efectuada pelo legislador no artigo 17° da Lei do Cibercrime (Lei n.°109/2009, de 15 de Setembro) para o regime da apreensão da correspondência previsto no Código de Processo Penal deve ser entendida e realizada, naturalmente, com as necessárias adaptações, porque o âmbito das mesmas é, necessariamente, diferente;
5ª) Como refere Rui Cardoso (in Apreensão de correio electrónico e registo de comunicações de natureza semelhante — artigo 17º da Lei n.°109/2009 de 15.IX, Revista do Ministério Público, nº 153, Janeiro - Março de 2018, página 191), «O artigo 17° determina a correspondente aplicação do regime de apreensão de correspondência do CPP, não a aplicação integral», e, mais à frente página 195): «Se fosse intenção do legislador aplicar integralmente o regime de apreensão de correspondência do CPP, bastar-lhe ia ter dito que "à apreensão de mensagens de correio electrónico ou registos de natureza semelhante é aplicável o regime de apreensão de previsto no CPP»;
6ª) O regime legal da apreensão do correio electrónico foi definido pelo legislador, apenas se aplicando subsidiariamente o regime legal da apreensão de correspondência quando não tiverem sido legalmente previstas quaisquer soluções no regime especial de prova electrónica previsto na Lei do Cibercrime;
7ª) No âmbito dos presentes autos, foram emitidos pelo Ministério Público mandados de pesquisa informática para todos os sistemas informáticos

elencados nos autos, pelo que foram as respeitadas todas as formalidades legais aplicáveis no caso concreto;
8ª) A autoridade judiciária competente, no decurso do inquérito, é o Ministério Público;
9ª) Mais uma vez, como refere Rui Cardoso (in Apreensão de correio electrónico e registo de natureza semelhante — artigo 17° da Lei n.º 109/2009 de 15.IX, Revista do n.°153, Janeiro - Março de 2018, página 171), «Como regime-regra, a apreensão deve ser feita por ordem ou autorização da autoridade judiciária competente, que, no inquérito, será o Ministério Público», em conformidade com a estrutura acusatória do processo, consagrada no artigo 32º, n.º 5, da Constituição da República Portuguesa respeitando a função do Ministério Público como titular do inquérito e respeitando a função do juiz de instrução como juiz das garantias;
10ª) A decisão judicial proferida pelo Mm.° Juiz ... do Juízo Central de Instrução Criminal, tendo sido violado o disposto no artigo 32% n.°5, da Constituição da República Portuguesa e o disposto no artº 17º da Lei do Cibercrime (Lei n.°109/2009, de 15 de Setembro)."
*

Os arguidos não responderam.
*

Neste Tribunal da Relação, o Digno Procurador-Geral Adjunto emitiu douto parecer no sentido da procedência do recurso.
*

Dispensados os vistos, foram os autos à conferência.
*

Fundamentação.
*

A decisão recorrida tem o seguinte teor:
"Por promoção de fls. 3426, veio o MP solicitar, invocando o disposto no artigo 17° da lei 109/2009, de 15 de Setembro, que o JIC proceda à tomada de conhecimento e autorize a junção aos autos das mensagens de correio electrónico e outros registos de natureza semelhante, os quais se encontram armazenados em suporte digital (seis DVD's) e que foram encontrados na sequência da pesquisa informática ordenado no âmbito dos presentes autos (fls. 3421 e 3422).
Por despacho judicial de fls. 3456 foi solicitada a indicação do local onde foi apreendido o correio electrónico, o despacho judicial que autorizou a apreensão e o titular do correio electrónico.
A fls. 3556 consta a promoção do MP a informar que o correio electrónico foi encontrado na sequência da pesquisa informática ordenada no âmbito dos

presentes autos (fls. 3421-3422) aos telemóveis de AA, BB, CC e DD e que os telemóveis foram apreendidos aos arguidos na sequência de mandados de busca domiciliária emitidos pelo JIC, tendo sido ordenada uma pesquisa informática nos termos do artigo 15° n° 1 da lei 109/2009, de 15-09, por despacho datado de 12-11-2020 e a realização da perícia informática por despacho datado de 26-11-2020.
Vejamos os elementos constantes dos autos:
A fls. 1457 a 1460, de 22-10-2020 e 1594-1596 de 3010-2020, consta o despacho judicial a autorizar a realização de buscas domiciliárias às residências, entre outras, dos arguidos acima referidos.
Dos despachos judiciais em causa não consta qualquer autorização para apreensão de correio electrónico dos suspeitos em causa.
Por despacho do MP, fls. 1614 a 1619, de 4-11-2020, foi determinada a realização de buscas não domiciliárias, bem como a realização de uma pesquisa informática nos sistemas informáticos encontrados na residência de EE.
A fls. 1684 consta o mandado de pesquisa informática emitido pelo MP em relação à suspeita EE.
A fls. 1965 a 1975 consta o cumprimento do mandado de pesquisa informática em relação ao telemóvel da arguida EE.
A fls. 1976 a 1998, consta o relatório das buscas onde estão indicados os telemóveis e demais equipamentos informáticos apreendidos.
A fls. 2000 a 2022 as apreensões foram validadas pelo MP.
A fls. 2130 a 2132, de 12-11-2020 consta o despacho do MP a determinar, nos termos do artigo 15° n° 1 da Lei 109/2009, de 15-09, a realização de uma pesquisa nos sistemas informáticos (telemóveis e Tablet) apreendidos, para apreensão dos seguintes dados informáticos relevantes para a prova, nos termos do disposto no artigo 16° n° 1 e no artigo 17°: dados referentes a comunicações — registos de contactos (comunicações SMS e correio electrónico); agenda; SMS, aplicativos multiplataforma de mensagens instantâneas e chamadas de voz para smartphones; correio electrónico.
A fls. 2289-2291, de 26-11-2020 consta novo despacho do MP a ordenar a realização de perícia informática nos mesmos termos que o despacho de 2130.
A fls. 3421 consta a informação do OPC a dará da gravação de seis DVD relativo ao conteúdo extraído das pesquisas informáticas relativas aos esquipamentos apreendidos.
Cumpre apreciar
As provas têm por função a demonstração da realidade dos factos (art° 341° do Código Civil).
Os meios de prova são os elementos de que o julgador se pode servir para

formar a sua convicção acerca de um facto (Antunes Varela, J. Miguel Bezerra e Sampaio e Nora — Manual de Processo Civil, pág.452).
Os meios de obtenção de prova são os instrumentos de que se servem as autoridades judiciárias para investigar e recolher meios de prova Cfr. Germano Marques da Silva — Curso de Processo Penal II, pág. 209.
Os meios de obtenção de prova, previstos nos artigos 171° e seguintes do CPP, visam descobrir as provas reais, localizar e contactar as provas pessoais com o intuito de se promover a realização da justiça com a descoberta da verdade dos factos. Na tarefa obtenção de prova impõe-se ao titular da acção penal e aos órgãos de polícia criminal, com respeito pelos princípios da legalidade, objectividade, da isenção e da imparcialidade, que carreiem para o processo as provas reais que indiciem a existência de um crime e quem são os seus autores.
Um dos princípios basilares do processo penal é o princípio da legalidade ou legitimidade da prova previsto no artigo 125.° do CPP, do qual se extrai que só poderão ser admitidas as provas que não forem proibidas por lei, não podendo ser admitidas quaisquer provas obtidas ilicitamente, ou que ponham em causa os direitos fundamentais constitucionalmente consagrados, a não ser nos casos em a própria constituição expressamente o permite.
Deste princípio resulta o exposto no artigo 126° n.°1 e n.°3 do CPP, que só vem densificar o que determina a própria Constituição nos seus artigos 32.° n° 8 e 34° n.°4, ou seja, "são nulas, não podendo ser utilizadas as provas obtidas mediante tortura, coacção ou com ofensa da integridade física das pessoas", e "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 e nas telecomunicações sem o consentimento do respectivo titular".
Em anotação ao artigo 32° n° 8 da CRP, escrevem J. Gomes Canotilho e Vital Moreira Constituição da República Portuguesa Anotada — 3" Ed., pág.206., "Os interesses do processo criminal encontram limites na dignidade humana (art°1°) e nos princípios fundamentais do Estado de direito democrático (art° 2°), não podendo, portanto, valer-se de actos que ofendam direitos fundamentais básicos. Daí a nulidade das provas obtidas com ofensa da integridade pessoal, da reserva da intimidade da vida privada, da inviolabilidade do domicílio e da correspondência (..). A interdição é absoluta no caso do direito à integridade pessoal, e relativa nos restantes casos, devendo ter-se por *abusiva* a intromissão quando efectuada fora dos casos previstos na lei e sem intervenção judicial (art.32°-2 e 4), quando desnecessária ou desproporcionada, ou quando aniquiladora dos próprios direitos (cfr. art.18°-2 e 3).

A este respeito, o Acórdão do Tribunal Constitucional (AC TC n° • $46^{4}/_{2}019$ de 21-10-2019): «Desde logo, a realização da justiça, não sendo um fim único do processo criminal, apenas pode ser conseguida de modo processualmente válido e admissível e, portanto, com o respeito pelos direitos fundamentais das pessoas que no processo se vêem envolvidas. O respeito desses direitos conduz, por exemplo, a considerar inadmissíveis certos métodos de provas e a cominar a nulidade de «todas as provas obtidas mediante tortura, coacção, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações» (cf. artigo 32.°, n.° 8, da CRP). A nulidade das provas, com a consequente impossibilidade da sua valoração no processo, quando sejam obtidas por ingerência abusiva nas comunicações, corresponde assim a uma garantia do processo criminal e resulta de ter havido acesso à informação fora dos casos em que a própria Constituição consente a restrição ao princípio da inviolabilidade dos meios de comunicação privada».
Passemos agora ao regime legal da apreensão do correio e em particular do correio electrónico.
Esta matéria está actualmente regulada pelo art° 179°, n° 1 a 3, do C.P.P e pelo art° 17°, da Lei n° 109/2009, de 15 de Setembro.
O do direito fundamental à inviolabilidade do domicílio e da correspondência, concretizado, nos termos do n.° 4 do artigo 34.° da CRP, consagra urna proibição de "ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal".
O artigo 34.° da Constituição visa proteger o direito fundamental à inviolabilidade do domicílio e da correspondência, ou seja, e *prima facie,* a liberdade de manter uma esfera de privacidade e sigilo, livre de interferência e ingerência estadual, quer no que respeita ao domicílio, quer quanto à correspondência incluindo nesta toda espécie de correspondência entre pessoas, em suporte fisico, ou. electrónico.
Ao nível europeu a protecção e garantia dos direitos fundamentais à reserva da intimidade da vida privada, ao sigilo das comunicações e à inviolabilidade da correspondência, encontra consagração no artigo 8.° da CEDH. Dispõem as normas deste artigo que: 1) qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência e 2) não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral,

ou a protecção dos direitos e das liberdades de terceiros.
Este direito encontra, ainda, protecção ao nível do direito da União, mais concretamente na Carta dos Direitos Fundamentais da EU.
A CDFUE reafirma no seu preâmbulo «os direitos que decorrem, nomeadamente, das tradições constitucionais e das obrigações internacionais comuns aos Estados-Membros, do Tratado da União Europeia e dos Tratados comunitários, da Convenção europeia para a protecção dos direitos humanos e das liberdades fundamentais, das Cartas Sociais aprovadas pela Comunidade e pelo Conselho da Europa, bem corno da jurisprudência do Tribunal de Justiça das Comunidades Europeias e do Tribunal Europeu dos Direitos Humanos».
A norma do artigo 7.° consagra o direito ao respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, sendo a norma tributária de todo o percurso de densificação destes direitos percorrido no plano europeu até à sua aprovação.
A Lei do Cibercrime, Lei n° 109/2009, de 15 de Setembro, transpõe para a ordem jurídica interna a Decisão Quadro n° 2005/222/JAI, do Conselhã da Europa; de 24 de Fevereiro, relativa a ataques contra sistemas de informação e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, materializando a matéria da recolha de prova em ambiente digital, designadamente nos seus ares. 11° a 19°.
Dispõe o art° 17°, da Lei n° 109/2009, sob a epigrafe da "apreensão de correio electrónico e registo de comunicações de natureza semelhante", que, quando no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados armazenados nesse sistema informático ou noutro que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem de grande interesse para a descoberta da verdade ou para a prova, aplicando-se, correspondentemente, o regime de apreensão de correspondência previsto no Código de Processo Penal.
Por sua vez, o artigo 179.° do Código de Processo Penal, que dispõe quanto à apreensão de correspondência, diz no seu n° 1 que, "(...) sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho, a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência, quando tiver fundadas razões para crer que:
a) a correspondência foi expedida pelo suspeito ou lhe é dirigida, mesmo que sob nome diverso ou através de pessoa diversa;
b) está em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos; e

c) a diligência se revelará de grande interesse para a descoberta da verdade ou para a prova (...)"
Diz, o seu n° 3., que o juiz que tiver ordenado ou autorizado a apreensão deverá ser o primeiro a tomar conhecimento do conteúdo da correspondência apreendida.
Tendo em conta o estatuído .no artigo 17°, da Lei do cibercrime, o disposto no art° 179°, do C.P.P e os direitos fundamentais em causa, isto é, o direito à reserva da intimidade da vida privada e familiar, a que se refere o artigo 26°, n° 1, da C.R.P. e a inviolabilidade da correspondência, a que se refere o art° 34°, n° 1, da C.R.P., acompanhamos o entendimento de que o legislador não quis, através da Lei do Cibercrime, consagrar uma menor protecção à correspondência electrónica do que aquele que consagra em relação à correspondência física.
E porque estão em causa direitos, liberdades e garantias constitucionalmente protegidos, como o direito à privacidade e reserva da vida privada e familiar e à inviolabilidade da correspondência e comunicações - cfr. arts. 26.°, n.° 1, 34. °, n.° 1 e 18.°, n.°s 2 e 3, todos da CRP -, as respectivas restrições têm de obedecer aos pressupostos materiais da necessidade, adequação e proporcionalidade em sentido restrito (cfr. Gomes Canotilho e Vital Moreira, Constituição da República Portuguesa Anotada, vol. I, 4.º ed., Coimbra Editora, 2007, págs. 388 e 392).
Por outro lado, conforme tem sido afirmado pela Jurisprudência dos Tribunais superiores, é pacífico o entendimento de que, quando se trata de interpretar e aplicar normas restritivas de direitos fundamentais, o critério interpretativo não pode deixar de ser aquele que assegure a menor compressão possível dos direitos afectados, a restrição do direito fundamental em causa há-de limitar-se ao estritamente necessário à salvaguarda do interesse (também constitucionalmente tutelado) na descoberta de um concreto crime e na punição do (s) seu (s) agente (s).
Resulta, então, que aplicando-se à apreensão do correio electrónico o regime de apreensão de correspondência previsto no Código de Processo Penal, o mesmo terá que seguir a disciplina do art.° 179°, o qual estabelece, no seu n° 1, corno já dissemos, que tais apreensões sejam determinadas por despacho judicial, "... sob pena de nulidade ...", e que " ...o juiz que tiver autorizado 'ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida ...", o que se aplica ao correio electrónico já convertido em ficheiro legível.
Assim, a remissão para o regime da apreensão de correspondência está, pois, condicionada aos seguintes aspectos:
(i) a referência à nulidade, em caso de inobservância dos requisitos legais

(artigo 179.°, número 1,2 e 3, do C.P.P.);
(ii) a apreensão ocorrerá, apenas, quando se tratar de correspondência/ correspondência electrónica que foi "expedida pelo suspeito ou lhe é dirigida, mesmo que sob nome diverso ou através de pessoa diversa" (artigos 1° al. e) e 179.°, número 1, alínea a), do C.P.P);
(iii) a apreensão de correspondência electrónica entre arguido e o seu defensor é proibida, "salvo se o juiz tiver fundadas razões para crer que aquela constitui objecto ou elemento de um crime." (artigo 179.°, n° 2, do C.P.P.)
(iv) o juiz (que ordenou ou autorizou a diligência), deverá ser o primeiro a tornar conhecimento do conteúdo da correspondência electrónica apreendida (art° 179.°, n° 3, do C.P.P).
De acordo com o artigo 1° al. e) do CPP, "suspeito" é toda a pessoa relativamente à qual exista indício de que cometeu ou se prepara para cometer um crime, ou que nele participou ou se prepara para participar.
No sentido da exigência de despacho judicial prévio veja-se o que diz Sónia Fidalgo, in Revista Portuguesa de Ciência Criminal, ano 29/2019, pág. 67: «A lei exige claramente um despacho judicial prévio a qualquer apreensão. Poderá questionar-se as dificuldades que tal exigência levanta na prática, mas não poderá dizer-se que a lei não faz esta exigência. Esta tem sido, também, a posição da nossa jurisprudência».
Quanto à exigência de ser o juiz, em primeira mão, a tomar conhecimento do conteúdo da correspondência electrónica, diz a mesma autora na pág. 68: «A nossa jurisprudência não tem sido, porém, sensível a estes argumentos. Entendendo que está em causa o direito à privacidade e ao sigilo da correspondência electrónica (artigos 26.°, n.° 1, e 34.°, n.° 4, da Constituição da República Portuguesa), considera que a remissão que no artigo 17.° da Lei do Cibercrime se faz para o regime da apreensão de correspondência previsto no Código de Processo Penal abrange o disposto no n.° 3 do artigo 179.° Os nossos tribunais têm entendido que o juiz que autoriza ou ordena a diligência deve ser a primeira pessoa a tornar conhecimento do conteúdo das mensagens de correio electrónico apreendidas».
Refere a mesma autora, in A Escolha de prova em suporte electrónico - Em particular, a apreensão de correio electrónico, Julgar, n° 38 — 2019, págs. 157-160 o seguinte: "Não nos parece, porém que a lei não seja expressa a este propósito. Para além da remissão para o regime da apreensão de correspondência previsto no Código de Processo Penal (artigo 179° n° 1), o próprio artigo 17° da Lei do Cibercrime estabelece que quando forem encontrados mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a

apreensão daquelas que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova. A lei exige claramente um d6spachã judicial prévio a qualquer apreensão".
Ainda neste sentido Tiago Aguiar, in O Correio Electrónico, A Apreensão e a intercepção no Processo Penal Português, Coimbra 2017, págs. 115-118 quando refere: "(...) afirmar que a lei não exige um prévio despacho judicial para a apreensão de mensagens de correio electrónico, é, assim o julgamos, fazer uma interpretação *contra legem* do preceito em questão, colocando-se em causa o princípio da legalidade, expondo-se a prova às vicissitudes decorrentes da teoria dos frutos da árvore envenenada".
De resto, conforme Santos Cabral in Código de Processo Penal comentado, Almedina Editora 2° Edição, 2016. P. 708, a não observância de tal exigência, sobe pena de nulidade expressa absoluta, prevista no artigo 179° n° 1 do CPP, reconduzirá a diligência ao regime de proibição de prova, devendo considerar-se que, nos termos do artigo 268° n° 1 al d), do CPP, constitui acto da exclusiva competência do JIC ser o primeiro a tomar conhecimento do correio electrónico já convertido em ficheiro digital.
Ao nível da Jurisprudência, Cfr. Acórdão do TRL de 11/01/2011, P° n° 5412/08.9TDLSB-A.L1-5, in www.dgsi.pt -, "...a lei do Cibercrime, lei n° 109/2009, de 15 de Setembro (...), determina no seu art° 17° (...) que, quando no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados nesse sistema informático ou noutro que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime de apreensão de correspondência previsto no Código de Processo Penal.
Aplicando-se assim o regime de apreensão de correspondência previsto no Código de Processo Penal, este encontra-se disciplinado no art° 179°, o qual estabelece desde logo no n° 1 que tais apreensões sejam determinadas por despacho judicial «sob pena de nulidade» expressa (n° 1), e que «o juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida», o que se aplica ao correio electrónico já convertido em ficheiro legível, o que constitui acto da competência exclusiva do Juiz de Instrução Criminal. Com efeito, o princípio constitucional do devido processo legal, consagrado. no artigo 20° n° 4_ da CRP e artigo 6° da CEDH, impõe que determinados actos e diligências processuais, sobretudo quando está em cãu¯sa a restrição de direitos

fundamentais pessoais, sejam precedidas de autorização judicial, ou seja, exige uma tutela reforçada através do princípio da jurisdicionalidade. (artigos 26% n° 1, 2 e 3, 32° n° 4, 34° n° 3 e 4 e 35° da CRP).
Cumpre realçar que esta tutela jurisdicional não esgota na prévia autorização judicial, pois impõe que nessa intervenção do juiz seja, através de decisão fundamentada, devidamente ponderado a necessidade, a imprescindibilidade e a indispensabilidade de recurso àquele meio intrusivo da vida privada e familiar por parte da investigação criminal.
Como refere Manuel Guedes Valente, in Cadeira de Custódia de Prova, Almedina, p. 76: "A tutela jurisdicional não se esgota na mera forma de determinar ou ordenar, mas cabe-lhe o dever constitucional e legal de controlar toda a actividade dos demais operadores judiciários que colide com direitos, liberdades e garantias fundamentais pessoais sobe pena de termos uma tutela de mera forma ou de mero papel timbrado".
E quanto à consequência da violação das referidas disposições legais — quanto à ausência de despacho judicial a determinar a apreensão do correio electrónico, o referido n° 1, do art° 179°, do C.P.P; e quanto à violação do conhecimento do correio electrónico em 1a mão pelo J.I.C., o referido n° 3, do art° 179°, do C.P.P. -, diz o Tribunal da Relação de Lisboa que tal violação constitui nulidade expressa absoluta que se reconduz, "...a final, ao regime de proibição de prova...".
Refere ainda este acórdão que "...em caso de urgência, isto é de perda de informações úteis à investigação de um crime em caso de demora, o juiz pode sempre autorizar a abertura imediata da correspondência (assim como de correio electrónico) pelo órgão de polícia criminal e o órgão de polícia criminal pode mesmo ordenar a suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações, nos termos dos n°s. 2 e 3 do art° 252° do Código de Processo Penal, devendo a ordem policial ser convalidada no prazo de 48 horas, sob pena de devolução ao destinatário caso não seja atempadamente convalidada, ou caso seja rejeitada a convalidação...".
Prosseguindo e aprofundando o que antecede, no mesmo sentido da competência exclusiva do J.I.C, para autorizar ou determinar a apreensão do correio electrónico, pronunciou-se o Acórdão do Tribunal da Relação de Lisboa, por acórdão de 20/12/2017, proferido no âmbito do processo n° 184/12.5TELSB-A.L1.
Começando pela análise que o acórdão faz quanto ao disposto no art° 189°, do C.P.P. - após a reforma introduzida pela Lei n° 48/2007, de 29 de Agosto -, ao disposto no art° 17°, da Lei n° 109/2009, de 15/09 e à sua conjugação com o disposto no art° 179°, do C.P.P, diz o Tribunal que "... o art° 189°, do CPP

passou então a estender o regime das escutas telefónicas às «conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardados em suporte digital».
Ora, se bem vemos, esta alteração legislativa do referido art° 189°, do CPP que se mantém, desde 2007 até à presente data numa redacção intocada, constitui sinal claro do órgão legiferante no sentido de afastar, no que tange ao correio electrónico, a distinção arbitrária entre mensagens abertas/ fechadas ou lidas/não lidas.
Da leitura que fazemos da lei, parece-nos que este aditamento teve por escopo quebrar - de uma vez por todas - a alegada analogia entre a correspondência física e a digital, submetendo esta última, em todas as suas formas, a uma protecção reforçada de inviolabilidade da correspondência.
Na verdade, com este .escopo, a lei estendeu a protecção conferida. às comunicações, que requerem, sob pena de nulidade, a intervenção do juiz de instrução, ao correio electrónico armazenado em suporte digital, independentemente de se o destinatário tomou ou não dele conhecimento ....".
E convocando a Doutrina, prossegue o Tribunal citando o Senhor Professor Costa Andrade, o qual entende que "... *na parte em que se estende o regime das escutas telefónicas ao email guardado no computado do destinatário, assegurando a este documentos urna tutela mais consistente do que a oferecida pelo regime das buscas. (...) É certo que, em boa hermenêutica — que fizesse prevalecer a força dos momentos sistemático e teleológico sobre o argumento literal — sempre poderia empreender-se uma interpretação restritiva, circunscrevendo o inciso aos emails guardados nos sistemas informáticos do provider. Isto é, àqueles emails que, já o vimos, numa interpretação que nos parece pertinente, é legítimo continuar a manter à sombra da categoria e da tutela jurídica das telecomunicações. Só que as coisas não são tão lineares: não pode, na verdade, esquecer-se que uma interpretação restritiva com este sentido e alcance configura urna verdadeira redução teleológica in mala partem. Sendo, como tal, constitucionalmente insustentável (..)*" (cfr. ANDRADE, Manuel de Costa, "bruscamente no Verão passado", a reforma do Código de Processo penal — Observações críticas sobre uma lei que podia e devia ter sido diferente, Coimbra, Coimbra editora, 2009, pág. 186).
Diz, assim, o Tribunal da Relação - referindo-se à posição do mesmo autor -, que "...pese embora divergente da solução positivada na reforma de 2007 no art° 189 do CPP, o certo é que o mesmo não deixa de reconhecer as consequências que dela efectivamente resultam (...)", quanto à impossibilidade de destrinça entre o correio electrónico lido/não lido, para efeitos de tutela

penal e constitucional.
E prossegue, dizendo que materializando a Lei n° 109/2009, de 15/09, diploma essencial em matéria de recolha de prova em ambiente digital, nos seus artigos 11° a 19°, releva entanto, para o caso concreto — para a apreensão do correio electrónico -, o art° 17° da citada lei, pelo qual o legislador veio consagrar aplicável à apreensão do correio electrónico e registos de comunicações de natureza semelhante, o regime de apreensão de correspondência previsto no art° 179°, do Código de Processo Penal.
Não fazendo o art° 17°, da Lei n° 109/2009 — lei esta que foi posterior à Lei n ° 48/2007, de 29 de Agosto, que introduziu as referidas alterações ao art° 189°, do C.P.P. - qualquer distinção entre "correio aberto"/"correio fechado", mensagens lidas/não lidas, há que concluir, da interpretação objectiva do referido art° 17°, que as mensagens de correio electrónico que se encontrem armazenadas num sistema informático, só podem ser apreendidas mediante despacho prévio do Juiz de instrução criminal, seja correio já lido ou não lido.
Beneficiando, assim, o correio electrónico e o registo de mensagens de natureza semelhante, por via do art° 17°, da lei do Cibercrime, de uma aparente tutela acrescida em relação ao demais correio a que se refere o art° 179°, do C.P.P. afigura-se-nos que, por via do art° 34°, n° 1, da C.R.P., todo ou qualquer desequilíbrio de tutela que possa ocorrer em relação ao demais correio - e às apreensões em arquivos resultantes de comunicações postais ou de idêntica natureza -, será salvaguardado em cada caso concreto pelo Juiz de Instrução, por via do art° 32° e 34°, da C.R.Portuguesa, no seu papel de "Juiz das liberdades".
Mas, sem prejuízo do que antecede, há que considerar que tal tutela, aparentemente acrescida, tem razão de ser nos tempos actuais, atenta a crescente preocupação de protecção da inviolabilidade da privacidade das pessoas individuais ou entes colectivos, face à facilidade da ingerência por terceiros - nos - sistemas electrónicos, _ com a consequente violação da privacidade.
No mesmo sentido o Acórdão da Relação de Lisboa de 06/02/2018, no processo n.° 1950/17.0T9LSB-A.L1-5: «A Lei do Cibercrime, lei n° 109/2009, de 15 de Setembro, a qual transpõe para a ordem jurídica interna a Decisão Quadro n° 2005/222/JAI, do Conselho da Europa, de 24 de Fevereiro, relativa a ataques contra sistemas de informação e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, determina no seu art.° 17°, sob a epígrafe da "apreensão de correio electrónico e registo de comunicações de natureza semelhante", dispõe que, quando no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados armazenados nesse sistema informático ou noutro que seja

permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime de apreensão de correspondência previsto no Código de Processo Penal.
Aplicando-se assim o regime de apreensão de correspondência previsto no Código de Processo Penal, este encontra-se disciplinado no art.° 179°, o qual estabelece desde logo no n.° 1 que tais apreensões sejam determinadas por despacho judicial, "sob pena de nulidade" expressa (n.° 1), ¯e que "o juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida", o que se aplica ao correio electrónico já convertido em ficheiro legível, o que constitui acto da competência exclusiva do Juiz de Instrução Criminal, nos termos do art.° 268° n.° 1 alínea d) do CPP, o qual estabelece que "compete exclusivamente ao juiz de instrução, tomar conhecimento, em primeiro lugar, do conteúdo da correspondência apreendida", o que se estendeu ao conteúdo do correio electrónico, por força da subsequente Lei n° 109/2009, de 15 de Setembro, constituindo a sua violação nulidade expressa absoluta e que se reconduz, a final, ao regime de proibição de prova».
No Acórdão de 07/03/2018, no processo n.° 184/12.5TELSB-B.L1-3, consta que: «Da redacção do art° 17° da Lei do Cibercrime resulta de forma clara que não esteve no espírito do legislador transpor para o correio electrónico e registos de comunicações de natureza semelhante a distinção, por referência ao correio tradicional, de correio aberto ou fechado, o que desde logo se colhe do elemento literal previsto neste preceito legal com a expressão "armazenados" o que pressupõe que a comunicação já foi recebida/lida e, consequentemente, armazenada, além de não existirem razões para considerar diminuídas as exigências garantísticas do correio electrónico quando aberto/lido relativamente ao correio electrónico fechado. atenta a natureza própria destas comunicações.
As mensagens de correio electrónico que se encontrem armazenadas num sistema informático só podem ser apreendidas mediante despacho prévio do Juiz de Instrução Criminal, devendo ser o juiz a primeira pessoa a tomar conhecimento do conteúdo da correspondência, conforme remissão para o art° 179° do CPP.
Ainda no mesmo sentido, o Acórdão da Relação de Lisboa de 4-2-2020, proferido no processo 1286/14.9IDLSB-AL1-5: «Sem prejuízo das descontinuidades de regulamentação encontradas e do entendimento que a expressão *correspondentemente* possa concitar, temos por inelutável que

constituindo a regra de que o "*juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida*" precisamente uma das normas mais emblemáticas do regime de apreensão para que se remete (tanto mais que, como vimos, constitui até fonte expressa de uma nulidade correspondente a proibição de prova), não vemos como através do elemento literal a mesma possa ser afastada.
Como a este propósito o refere o Exmo. Sr. Conselheiro Santos Cabral, que nesta parte assegura o Comentário do art. 179.° no Código de Processo Penal de António Henriques Gaspar e Outros (Almedina, 2014, págs. 762/3), citando para o efeito Gomes Canotilho e Vital Moreira (Constituição da República Portuguesa Anotada, pág.º 545), "o direito ao sigilo da correspondência e restantes comunicações privadas, implica, não apenas o direito que ninguém as viole ou as devasse, mas também o direito de terceiros que a elas tenham acesso não as divulguem".
Ou seja, "a Constituição não garante somente o sigilo da correspondência e outros meios de comunicação privados (n.^{0} 1), mas também proíbe toda a ingerência (n.° 4), envolvendo a liberdade de envio e de recepção de correspondência, a proibição de retenção ou de apreensão, bem como de interferência (telefónica etc.) (...)."
Donde, não se ter em vista assegurar apenas o conteúdo da correspondência apreendida, mas também a protecção conferida pelo referido regime ao direito à reserva da intimidade da vida privada e familiar».
Ainda no mesmo sentido, o recente acórdão do Tribunal da Relação de Lisboa proferido a 23-12-2020 no processo 126/12.8TELSB ao referir que: "Como se pode constar, o art° 17° da LC e o art° 179° n° 1, do CPP, contêm um requisito de admissibilidade comum: apenas ao juiz é conferida competência para poder autorizar ou ordenar, se entender revestir grande interesse para a descoberta da verdade ou para prova, a apreensão de *e-mails*. Ora, se por si só, a convergência entre disposições já seria dissuasora para perfilharmos o entendimento dos doutrinadores que pugnam pela aparente competência do MP para legitimar a admissibilidade da diligência de apreensão, doutro passo, cremos somente com a exigência do prévio despacho judicial do juiz, se acautelam os potenciais abusos cometidos pelos agentes de investigação criminal, na medida em que o resultado das diligências de apreensão revelam, muitas vezes, que a investigação com recurso a aplicações que permitem a realização de pesquisas gerais nos servidores (normalmente com obtenção de passwords ou sem dela estar munida), estendeu-se a dados partilhados no sistema informático comum, não abrangidos e delimitados pelo despacho judicial que autorizou a diligência, acabando por se ter acesso a ficheiros

pertencentes a pessoas não visadas, que nenhuma conexão têm com a matéria que se investiga nos autos, apreendendo-se *e-mails* com conteúdo da esfera reservada e íntima da vida das pessoas, trazendo-se para dentro dos processos judiciais uma quantidade indeglutível de informação referente às suas compras, vendas, planificações de negócios, património, movimentos bancários, fotografias de cariz sexual, informação sobre o estado de saúde, religião, expondo-se gratuitamente e ao livre arbítrio, a vida privada das pessoas".
Manuel Guedes Valente, in Cadeia de Custódia de Prova, Almedina. P 74 refere, a propósito da apreensão do correio electrónico, o seguinte "Só após este deferimento judicial, se determina a perícia. Há um controlo judicial do acto de pesquisa, de apreensão e visionamento original. Não está nas atribuições e competências das polícias criminais — não deve estar *ex lege* — o acesso a esse conteúdo privado (domínio privado de acesso restrito), sob pena de nulidade da diligência e das provas meio obtidas e da respectiva prova resultado. Esta nulidade é de natureza insanável, tornando inexistente o acto e a prova recolhida e, por isso, inadmissível como prova do processo por via directa ou por via da inadmissibilidade de valoração probatória"
Por fim, cumpre dizer que não faz qualquer sentido fazer distinção entre correio electrónico lido e não lido e comparar essa realidade com a correspondência aberta ou fechada. Com efeito, tratam-se de duas realidades completamente distintas, na medida em que o correio electrónico encontra-se armazenado numa caixa de correio (conta de correio electrónico) a qual só pode ser acedível através de uma *password,* não tendo, por isso, qualquer semelhança com urna busca e apreensão de papéis que se encontram numa gaveta ou numa secretária.
Para além disso, há que ter em conta a volatilidade de se alterar o estatuto da comunicação através da opção "read" "unread" o que permite a possibilidade de contaminação da prova por parte da investigação.
Deste modo, como refere Rita Castanheira Neves, in A ingerência nas comunicações...p. 194: "Assim para nós, são também as particulares características da prova digital, concretamente, a sua volatilidade, que justificam a prévia exigência de despacho do juiz que autorize ou ordene a apreensão de mensagens de correio electrónico".
Face ao que acabamos de expor e de acordo com a Jurisprudência, que mostra praticamente pacifica, e a Doutrina que seguimos, a autorização para a apreensão de correspondência e conhecimento em primeira mão, constitui acto da competência exclusiva do Juiz de Instrução Criminal, nos termos do art.° 269°, n° 1, al. d), do C.P.P, que diz que "...durante o inquérito compete exclusivamente ao juiz de instrução ordenar ou autorizar (...) apreensões de

correspondência, nos termos do n° 1, do art° 179° (...)" e art° 268°, n° 1, alínea d), do C.P.P, o qual estabelece que "... compete exclusivamente ao juiz de instrução, tomar conhecimento, em primeiro lugar, do conteúdo da correspondência apreendida...".
Estamos, assim, perante um acto de Reserva de Juiz conforme resulta do artigo 17° do CPP.
Tendo em conta o caso concreto, como resulta dos elementos do processo acima mencionados, não existe qualquer despacho emitido pelo juiz de instrução criminal a autorizar a apreensão do correio electrónico. Essa decisão foi tomada pelo MP.
Quanto à consequência da violação da competência do JIC, prevista no art° 17°, da Lei n° 109/2009, de 15 de Setembro, como já vimos acima, mostra-se assente que a mesma constitui nulidade expressa absoluta e que se reconduz, a final ao regime de proibição de prova.
A preterição de reserva do juiz e a inobservância de formalismos legais previstos nos artigos 179.°, 189.° e 190.° do CPP e 17.° da LCC é cominada com a nulidade e redunda em proibição de prova - Art.° 126.º/3 CPP e Arts.° 32.°/8 e 34.°/1 e 4 CRP.
Uma vez delimitado o âmbito de protecção das normas constitucionais e processuais penais que consagram o direito à inviolabilidade da correspondência, bem como as regras processuais relativas à obtenção de prova baseada na apreensão de correspondência, em particular correio electrónico e tendo em conta a factualidade acima referida, é agora chegado o momento de apreciar a validade da prova proveniente da apreensão do correio electrónico apreendido pelo MP às arguidas AA, BB, CC e DD.
Conforme já vimos, para além de autorização judicial prévia, a lei exige, para que possa ser proferido um despacho judicial de autorização de apreensão de correio electrónico, a presença dos pressupostos materiais previstos no artigo 179° n° 1 do CPP por remissão feita pelo artigo 17° da Lei 109/2009.
Da análise dos autos não consta que os titulares do correio electrónico em causa, de forma voluntária, esclarecida e expressa, tenham dado o seu consentimento para o acesso ao conteúdo do correio electrónico e utilização do mesmo no âmbito destes autos.
Assim sendo, não ocorre a excepção do consentimento do visado, a que se refere o art° 174°, n° 5, al. b), do C.P.P., bem como o art° 126°, n° 3, do C.P.P
Pelo que, face ao exposto e atento o disposto nos art°s 18°, 34^{0}, n° 1 e 4, 32°, n° 8, da C.R.P., art°s. 269°, n° I, al. d), do C.P.P., 179°, n° 1, do C.P.P., conjugado com o art°A 7°, da Lei n° 109/2009 e art° 126°, if 3, do C.P.P., o despacho do Ministério Público de fls. 1684, 2130 e 2289, no qual determinou a cópia autónoma de todos as mensagens de correio electrónico constantes

dos equipamentos, comunicações ou registos de comunicações de natureza semelhante é nulo por violação do principio da reserva de juiz exigido pelo disposto no art° 179°, n° 1, do C.P.P., em conjugações com o disposto no art° 17°, da Lei n° 109/2009, por falta de prévio despacho judicial a autorizar a busca informática para apreensão de correio electrónico e registos de comunicações de natureza semelhante.
Cumpre dizer, ainda, que no caso concreto, também não ocorreu situação de urgência, que implicasse possível perda de informação útil à investigação de um crime, nem ocorreu qualquer uma das situações a que se refere o art° 174°, n° 3, do C.P.P. — para o qual remete o art° 15°, n° 6, da Lei n° 109/2009, quanto ao regime da pesquisa em sistemas informáticos, para efeitos de produção de prova -, pelo que também por esta via não ocorreu qualquer situação que pudesse justificar a apreensão efectuada sem prévia autorização judicial.
Estamos, por conseguinte, no caso concreto, no âmbito do art° 126°, n° 3, do C.P.P. - e, seguindo a posição que, pensamos, actualmente maioritariamente adoptada pelos Tribunais Superiores -, perante prova proibida, porque obtida através de uma apreensão de correspondência electrónica não consentida pelos visados, que não foi autorizada pelo juiz de instrução (nas situações supra identificadas), fora dos pressupostos materiais previstos na lei, nos termos das disposições conjugadas dos art°s 17°, da Lei n° 109/2009 e 179°, do C.P.P.
Quanto aos seus efeitos e de acordo com o entendimento que seguimos, a nulidade do n.° 1, do artigo 126.° tem os mesmos efeitos da nulidade do seu n.° 3, pois em ambos os casos estamos perante proibições de prova (cfr., para além dos citados autores, também José Mouraz Lopes, Escutas Telefónicas seis teses e uma conclusão, na Revista do MP n.° 104, 2005, págs. 150, nota 24; ao que parece, também, José Manuel Darnião da Cunha, A Jurisprudência do Tribunal Constitucional em Matéria de Escutas Telefónicas. Anotação aos Acórdão do Tribunal Constitucional n.° 407/97, 374/01, 411/02 e 528/03, Jurisprudência Constitucional, n.° 1, Jan./Março 2004, págs. 55-56), que segue na esteira da posição defendida por Teresa Pizarro Beleza, Apontamentos de Direito Processual Penal, II vol., AAFDL, 1993, pág. 150-151 e por Germano Marques da Silva, Curso de Processo Penal, II vol., cit., pág. 205-206).
Por último, cumpre referir que: *«A nulidade da prova proibida pode ser conhecida quer a prova já tenha sido utilizada pelo tribunal, quer ainda não tenha sido. Neste caso, a nulidade da prova há-de ser declarada, com a consequência da sua rejeição»* Paulo Pinto de Albuquerque, Comentário ao Código Processo Penal, pág. 320, nota 7.
Reconduzindo-se a uma proibição absoluta de prova, não pode ser valorada

pelo Tribunal.
Em face do exposto, está em causa uma proibição de prova, nos termos do art° 126°, n° 3, do C.P.P., de conhecimento oficioso e que tem como consequência a nulidade da prova obtida.
Nesta conformidade, declaro a nulidade do despacho do MP proferido a fls. 1684, 2130 e 2289, bem como a nulidade da prova obtida a partir do correio electrónico e registos de comunicações de natureza semelhante apreendido às arguidas AA, BB, CC e DD.
Após trânsito em julgado deste despacho, proceda-se à eliminação dos suportes informáticos em causa, ficando o mesmo, até essa data, no cofre deste TCIC.”
*
Cumpre apreciar.
De acordo com a jurisprudência fixada pelo Acórdão do Plenário das Secções do STJ de 19.10.1995 (D.R., série I-A, de 28.12.1995), o âmbito do recurso define-se pelas conclusões que o recorrente extrai da respectiva motivação, sem prejuízo, contudo, das questões de conhecimento oficioso.
*
Atendendo às conclusões apresentadas é questão a apreciar se foi cometida nulidade probatória e consequentemente o destino do dados electrónicos obtidos.
*
Tanto a decisão recorrida como depois o recurso da mesma interposto, partem do princípio de que a correspondência electrónica em causa foi apreendida por ordem do Ministério Público.
Ora, não foi esse o caminho processual trilhado, salvo o devido respeito e perante os dados processuais constantes.
O que sucedeu, em rigor, foi, sem visualização prévia, a extracção encriptada (inacessível e protegida por programa e chave próprios) de dados informáticos (sequências digitais) em bruto, que encerram possibilidade de acesso aos correspondentes conteúdos, designadamente mensagens de correio electrónico ou similares, para apresentação ao juiz de instrução criminal, na sequência de pesquisa informática, essa sim, ordenada pelo Ministério Público de seguida à apreensão aos arguidos de computadores e telemóveis (que também são computadores), sendo de esperar que tais conteúdos fossem acessíveis a partir daquelas máquinas.
Destarte, a quem cabia (e cabe) a primeira abertura, leitura e eventual determinação de apreensão das mensagens é ao juiz de instrução criminal, apenas podendo ser, legalmente, lavrada promoção nesse sentido.
Na verdade, dispõe o artº 17º da Lei do Cibercrime, sob a epígrafe apreensão

de correio electrónico e registos de comunicações de natureza semelhante, que “quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.”
Dali resulta desde logo que a apreensão em causa faz parte, indubitavelmente, da reserva do juiz.
Neste mesmo sentido se pode verificar o recente acórdão do Tribunal Constitucional (nº 687/2021, D.R. de 22.9.2021), com o seguinte sumário: “decide, com referência ao Decreto n.º 167/XIV, da Assembleia da República, publicado no Diário da Assembleia da República, série II-A, n.º 177, de 29 de julho de 2021, e enviado ao Presidente da República para promulgação como lei, pronunciar-se pela inconstitucionalidade das normas constantes do seu artigo 5.º, na parte em que altera o artigo 17.º da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime).”
Aquele Decreto, em apertada síntese, previa justamente atribuir ao Ministério Público a competência para ordenar a referida apreensão, subtraindo-a àquela reserva judicial e foi, por tal motivo, julgada inconstitucional, em processo de apreciação preventiva.
Ou seja, é constitucionalmente inviável a posição do Ministério Público veiculada neste recurso.
Não obstante, vejamos então o que processualmente sucedeu, reparando-se nas concretas decisões do Ministério Público (idênticas, a fls. 2132 e 2290), quando determinou as pesquisas:
“(…) *Assim, nos termos do disposto no n.° 1 do artigo 15°, n.°1, da Lei n.° 109/2009, de 15 de Setembro (Lei do Cibercrime), ordena-se a pesquisa nos sistemas informáticos (telemóveis e tablas) apreendidos no âmbito dos presentes autos, no prazo de 30 dias (n.° 2 do referido preceito legal), para apreensão dos seguintes dados informáticos relevantes para a prova, nos termos do disposto no artigo 16°, n.°1, e no artigo 17° da Lei do Cibercrime:*
a) Dados referentes a comunicações — registos de contactos (comunicações, SMS e correio electrónico);
b) Agenda;
c) SMS;
d) Aplicativos multiplataforma de mensagens instantâneas e chamadas de voz

para smartphones (sistema Whatsapp Alessenger e semelhantes);
e) Correio electrónico.
Caso, no decurso da pesquisa informática, venham a ser recolhidos dados cujo conteúdo, para além daquele que se revele fundamental para a prova nos autos, inclua dados referentes a registos de comunicações e mensagens de correio electrónico, nos termos do disposto no artigo 17° da Lei do Cibercrime, deverão ser tais dados extraídos, nos termos do disposto no artigo 16°, na alínea b) do n.° 7, alínea b), e n.° 8, da referida Lei do Cibercrime, efectuando cópias em duplicado, digitalmente encriptadas, as quais serão seladas, uma para entrega ao secretário judicial e outra entregue para posterior promoção da apreensão dos dados informáticos, sem visualização prévia, ao Mm.° Juiz de Instrução Criminal (...)
E bem assim na promoção sequente à pesquisa e que veio a ser objecto da decisão recorrida:
" Nos termos conjugados dos artigos 17º, da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime) e artigo 179º, nºs 1 e 3, do Código de Processo Penal, remeta os autos ao Mm.º Juiz do Tribunal Central de Instrução Criminal, para que o mesmo tome conhecimento e autorize a junção aos autos das mensagens de correio electrónico e outros registos de natureza semelhante, que se revelam ser de grande interesse para a descoberta da verdade e para a recolha de prova, os quais se encontram armazenados/ guardados em suporte digital (seis DVD's), e que foram encontrados na sequência da pesquisa informática ordenada no âmbito dos presente autos (cfr. fls. 3421 e 3422)" (...)
*
O que antecede significa que aquelas mensagens foram efectivamente apreendidas por determinação do Ministério Público, como defendem, quer a decisão recorrida, quer o recurso desta interposto?
Não o cremos, de novo, salvo o elevado respeito pela referida conclusão.
Nas promoções que antecederam a pesquisa, foi efectiva e legalmente ordenada a apreensão de dados informáticos relevantes para a prova, logo ali se salvaguardando, contudo, que os dados referentes a registos de comunicações e mensagens de correio electrónico deveriam ser extraídos, sem visualização prévia, efectuando-se cópias digitalmente encriptadas e seladas para posterior promoção da apreensão dos dados informáticos, ao Mm.° Juiz de Instrução Criminal (sublinhados nossos).
E é a tal promoção que equivale a posterior, quando o Ministério Público solicita ao tribunal recorrido que tome conhecimento e autorize a junção aos autos das mensagens de correio electrónico e outros registos de natureza semelhante.

Do todo da atitude processual do Ministério Público até então (excluído portanto o teor das alegações de recurso) se verifica que apreensão alguma, neste particular, foi determinada.
Assim, esta só ocorreria após a abertura daquelas mensagens e eventual junção (esta já posterior).
De que tipo de apreensão se trata aqui é questão a investigar de seguida.
Não corresponde, desde logo, ao conceito processual geral, o qual se surpreende e resulta do que dispõem os art^{os} 178º, n^{os} 1 e 2, 179º, nº 1, 181º, n^{os} 1 e 2, 182º, nº 1, 183º, 184º, 185º, 186º, n^{os} 1 e 2, 249º, nº 2, alínea c), 252º, 499º, nº 3 e 500º, nº3, todos do Código de Processo Penal.
Tal conceito, sem qualquer excepção, equivale à retirada do poder de disponibilidade sobre realidades físicas para a esfera da investigação.
Ora, os dados digitais não correspondem a realidade física.
Apenas quando o seu conteúdo, depois de devidamente processado, é desvendado e materializado, ou consultado, obteremos algo apreensível pelos sentidos humanos.
Até então, não passam de sequências em linguagem virtual e binária de zeros e uns.
Acresce que fácil e correntemente, uma mensagem de correio electrónico e com aquela configuração, não se encontra armazenada no computador (aqui incluindo todos aparelhos com semelhante poder de processamento), outrossim, num servidor em qualquer lugar do mundo (sistemas de “webmail” e “dropbox”, por exemplo, ao que ainda acrescem as caixas compartilhadas), sendo apenas o acesso àquele o que se encontra no computador.
Logo, a apreensão de dados informáticos a que a lei do cibercrime se refere, não corresponde, de todo, à apreensão clássica, digamos assim, pela própria natureza das coisas.
Basta pensar que esta última passa por desapossar alguém da coisa corpórea e que, por outro lado, não obstante o acesso ao conteúdo digital, em boa parte das situações (especialmente no que ao correio electrónico respeita) o respectivo utilizador pode continuar a aceder ao seu conteúdo, copiando-o, transferindo-o, ou mesmo apagando-o. E para tanto basta aceder à mesma conta de correio por intermédio de outro computador.
Apreensão de dados informáticos, por conseguinte, tem muito mais a ver com o sinónimo de percepção, ou compreensão, apenas possível depois daquela operação de processamento, absolutamente necessário para que o seu conteúdo seja disponibilizado em termos inteligíveis.
Se assim é, como aqui se defende, então aquela apreensão apenas ocorre, em rigor, quando o conteúdo é desvendado e depois junto ao processo em linguagem comum.

E, não por acaso, é apenas nesse momento que ocorre a efectiva compressão do direito à reserva da vida privada, direito constitucional convocado aqui na vertente da inviolabilidade da correspondência, que a lei processual visa salvaguardar com as garantias e formalidades que impõe, designadamente a da reserva judicial no que respeita àquela forma de correspondência electrónica.
Tal como para o correio tradicional, forçoso é que o respectivo conteúdo seja acedido, em primeira mão, pelo juiz de instrução criminal, que apenas ordenará a junção ao processo do que for estritamente necessário à investigação do crime noticiado, de resto, a única razão justificativa daquela compressão de direito fundamental.
*
Retornando ao caso, conclui-se que quanto aos dados em bruto e encriptados que se encontram à disposição dos autos, não foi, ainda, determinada qualquer apreensão, cabendo ordenar o processo em conformidade.
*
Consequentemente, procede o recurso, ainda que por motivo diverso.
*
Pelo exposto, acordam em conceder provimento ao recurso, ordenando que o tribunal recorrido proceda à abertura das mensagens e similares, determinando a apreensão e junção das que tenham grande interesse para a descoberta da verdade e recolha de prova.
Sem custas.
*
Lisboa, 9 de Novembro de 2021
Manuel Advínculo Sequeira
Alda Tomé Casimiro