

**Tribunal da Relação de Lisboa**  
**Processo nº 184/12.5TELSB-B.L1-3**

**Relator:** CONCEIÇÃO GONÇALVES

**Sessão:** 07 Março 2018

**Número:** RL

**Votação:** UNANIMIDADE

**Meio Processual:** RECURSO PENAL

**Decisão:** PROCEDENTE

**CORREIO ELECTRÓNICO**

**CORRESPONDÊNCIA**

**PROVAS NULAS**

**JUIZ DE INSTRUÇÃO CRIMINAL**

## Sumário

I. Com a aprovação da Lei do Cibercrime (Lei 109/2009 de 25 de Setembro) foi introduzida, pela primeira vez no nosso ordenamento, um regime jurídico de prova digital.

II. O regime de apreensão de correio electrónico e registos de comunicações de natureza semelhante mostra-se regulado directamente pelo artigo 17º da Lei do Cibercrime e, subsidiariamente (por remissão do mesmo) pelos pressupostos e requisitos legais relativos à apreensão de correspondência, previstos no artº 179º do CPP (deixando de se aplicar a extensão legal prevista no artº 189º, nº 1 do CPP).

III. Quer o artº 179º, nº 1 do CPP quer o artº 17º da Lei do Cibercrime sancionam com nulidade a violação das regras relativas à competência para a autorização de apreensão de correio electrónico.

IV. A intromissão nas comunicações e na correspondência está sujeita a autorização judicial, o que se justifica pelo princípio da proporcionalidade face à especial danosidade social que implica tal intromissão.

V. Da redacção do artº 17º 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, conseqüentemente, 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.

VI. 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 artº 179º do CPP.

## **Texto Integral**

Acordam, em conferência, na 3ª Secção Criminal do Tribunal da Relação de Lisboa

I-Relatório.

1. No processo de Inquérito a correr termos no Departamento Central de Investigação e Acção Penal - Secção Única (DCIAP), com o número supra identificado, em que é arguido R..., foi proferido pelo Srº Juiz de Instrução Criminal - Secção Única, em 3.7.2017, o despacho exarado a fls. 2034 a 2047, no âmbito do qual se decidiu: "...declaro a nulidade do despacho do MºPº na parte em que autorizou a apreensão de correio electrónico de R..... (...). Esta ilegalidade reconduz a busca, na parte relativa à apreensão do correio electrónico, a um meio proibido de prova, por violação à privacidade e sigilo de correspondência e, conseqüentemente, à nulidade da prova obtida com a mesma".

2. Inconformado com o assim decidido, recorreu o Ministério Público, formulando as seguintes conclusões (transcrição):

"O objeto do presente recurso.

1.O presente recurso é interposto do despacho proferido pelo M.mo juiz de instrução junto do Tribunal Central de Instrução Criminal, de fls. 2034 a 2048, através do qual julgou verificada a nulidade a que alude o art. 179º, n.º 1, do Código de Processo Penal (aplicável por força do art. 17º, da Lei do Cibercrime), do despacho proferido pelo Ministério Público "na parte em que autorizou a apreensão de correio eletrônico de R... (...)", e através do qual, em consequência, determinou que, "[após] trânsito, [se procedesse] à eliminação do suporte informático constante do Saco Prova B 068531 (REN) e do suporte informático identificado a fls. 1834".

O âmbito de aplicação do regime de apreensão de correio eletrónico.

2.A matriz legal respeitante à apreensão, em processo penal, de correio eletrónico, encontra-se no art. 17º, da Lei do Cibercrime, e no art. 179º, do Código de Processo Penal, que, tutelando os termos em que pode ser efetuada a apreensão ou o controlo de correspondência em processo penal, faz rodear a possibilidade de se lançar mão deste meio de obtenção de prova de cautelas muito específicas - das quais se salienta a circunstância de o recurso à mesma depender da intervenção do juiz de instrução, que deve decidir em função de um estrito critério de necessidade (cf. art. 179º, n.º 1), e o facto de o conteúdo de correspondência que venha a ser seu objeto dever ser primeiramente conhecida pelo juiz de instrução (cf. art. 179º, n.º 3) - em função da intrusão de natureza violenta em direitos e garantias constitucionais dos visados (cf. art. 34º, n.ºs 1 e 4, da Constituição da República Portuguesa) que tal medida representa.

3.A operacionalidade deste regime legal depende de um fator que é absolutamente desvalorizado na decisão em recurso e que a coloca numa posição de inaceitabilidade face à constelação valorativa que o informa: é pressuposto material e essencial para que este conjunto normativo possa ser chamado à colação que se esteja perante correspondência.

4.Correspondência é a mensagem transmitida de um remetente para um destinatário, desde o momento em que aquele a emite até ao momento em que este a recebe, o momento em que dela toma conhecimento.

5.Requisito indispensável ao conceito processual penal relevante de correspondência que se esteja perante um processo comunicacional não concluído, pois se a dinâmica comunicacional se mostrar concluída, isto é, se a mensagem se encontrar já na esfera de conhecimento do destinatário, a mensagem perdeu as características que a faziam pertinente à tutela da correspondência, já que se mostra esgotado o procedimento dinâmico, objetivo e intersubjetivo do ato comunicacional merecedor da especial tutela da privacidade formal, à distância.

6.No entendimento de Manuel da Costa ANDRADE, "depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer à área de tutela das telecomunicações, passando a valer como um normal escrito", estabelecendo-se como meio idóneo da busca em sentido tradicional, e sujeitando-se ao regime correspondente àquele a que ficam sujeitos os documentos que o visado cria e arquiva no seu computador (Bruscamente no Verão Passado — A reforma do Código de Processo Penal, Coimbra Editora, Coimbra, 2009, p. 157).

7.*Quae sunt Caesaris, Caesari*: a tutela da correspondência apenas é aplicável a correspondência, seja ela física, seja ela digital.

8. Diverso entendimento, designadamente aquele preconizado na decisão sob recurso, que não distingue normativamente o que é naturalmente distinto, significaria que a inclusão do regime restritivo previsto no art. 17º, da Lei do Cibercrime no ordenamento jurídico português, não teria, afinal, aportado nada de novo ao regime, porquanto qualquer registo digital, ainda que com origem em correio eletrónico, mas que não fosse já correio, estaria sempre abrangido pela reserva jurisdicional que aquela norma prescreve, deixando de existir espaço normativo para a aplicabilidade do prescrito pelo art. 16º, da Lei do Cibercrime.

9. Ao nível jurisprudencial este tratamento diferenciado tem vindo a ser destacado, entendendo-se que “a mensagem mantida em suporte digital, depois de recebida e lida, tem a mesma proteção da carta em papel que, tendo sido recebida pelo correio e aberta, foi guardada em arquivo pessoal”, mas se afirmando que, “[sendo] um mero documento escrito, aquela mensagem não goza da aplicação do regime de proteção específico da reserva da correspondência e das comunicações” [cf. acórdão do Tribunal da Relação de Guimarães de 12-10-2009, proc. n.º 1396/08.1PBGMR-A.G1 (Tomé Branco), acórdão do Tribunal da Relação do Porto de 20-01-2016, proc. n.º 1145/08.4PBMTS.P1 (Artur Oliveira), e acórdão do Tribunal da Relação de Lisboa de 02-03-2011, proc. n.º 463/07.3TAALM-A.L1-3, (Jorge Raposo), todos disponíveis em WW w .dgsi.pt] .

10. Nos termos do art. 16º, da Lei do Cibercrime, a apreensão de documentos não correspondentes a mensagens de correio eletrónico basta-se com a intervenção legitimadora do Ministério Público, enquanto autoridade judiciária competente, nos termos conjugados dos art.s 1º, al. b), 53º, n.º 2, al. b), 263º, n.º 1, e 262º, n.º 1, do Código de Processo Penal.

11. A argumentação a que se recorreu no despacho em recurso encontra-se viciada pela desconsideração do comando legal que determina que, na fixação do sentido e alcance da lei, o intérprete presumirá que o legislador soube exprimir o seu pensamento em termos adequados, inscrito no art. 9º, n.º 3, do Código Civil.

12. No contexto do direito da informática, “armazenar” não significa necessariamente “arquivar após tomada de conhecimento”, como parece dar-se a entender na decisão sob recurso.

13. Existem fases no processo comunicacional em que a mensagem de correio eletrónico, embora jacente, não foi ainda conhecida pelo seu destinatário, estando-se, portanto, ainda perante correio eletrónico.

14. A situação a que respeita a decisão em recurso é diversa: tratar-se-ão de ficheiros, outrora correio, mas que, já que conhecidos do seu destinatário e armazenados em arquivo após tomada desse conhecimento, deixaram de ter

essa natureza.

15. Este tipo de documentos não merece a tutela legal conferida à correspondência eletrônica, revelando-se um contrassenso invocar o ritualismo da apreensão de correspondência quando já não há correspondência.

16. A decisão tomada pelo M.mo juiz de instrução revelou-se precipitada e ilegal (além de desajustada), ao julgar verificada a nulidade do despacho proferido pelo Ministério Público nos termos em que o fez.

A atividade jurisdicional em sede de inquérito no âmbito de uma apreensão de correio eletrônico.

17. O despacho ora colocado em crise parte do pressuposto de que o Ministério Público deveria ter solicitado autorização judicial para proceder a pesquisa, em suportes informáticos, de ficheiros contendo dados relativos a correio eletrônico.

18. Entende o Ministério Público que, na verdade, tal autorização não era carecida para a atividade investigatória a desenvolver nas diligências de busca determinadas, considerando que no despacho proferido, através do qual o Ministério Público determinou a realização de buscas aos locais em causa e a apreensão de documentos que se revelassem relevantes para o objeto probatório dos autos, especificou-se que "as deverão incidir sobre toda a documentação encontrada nos respetivos postos de trabalho e arquivos utilizados pelos visados, ou pela respetiva instituição, incluindo toda a que se encontre em formato digital, ainda que se trate de documentos originados ou recebidos via correio eletrônico no período em causa nos autos".

19. As pesquisas a realizar visariam, exclusivamente, documentos originados em correio eletrônico recebido ou remetido durante o período compreendido entre os anos de 2004 a 2014, tendo sido convicção do Ministério Público que inexistiriam, em relação a tal período e face à sua anterioridade no tempo, ficheiros de correio eletrônico propriamente ditos armazenados que suscitassem intervenção judicial para o efeito de acesso aos mesmos e sua apreensão.

20. Na execução da busca, "face à impossibilidade de, em tempo útil, efetuar pesquisa informática com base nas referidas palavras-chave nos ficheiros resultantes de correio eletrônico de R(...), foi efetuada cópia em bruto dos mesmos, relativa ao período compreendido entre 2004 e Janeiro de 2017, para disco rígido (...), sendo possível (mas não certo) que tenham sido apreendidos ficheiros correspondentes a mensagens de correio eletrônico que, pela sua data recente, não terão qualquer interesse para o desenvolvimento das diligências de inquérito nos presentes autos.

21. Dispõe o art. 16º, n.º 3, da Lei do Cibercrime que caso, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, sejam apreendidos dados ou documentos informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto.

22. Em conformidade com tal norma, o Ministério Público decidiu apresentar o produto apreendido ao M.mo juiz de instrução, para que este, em primeira mão, verificasse da existência, naquela plêiade de documentação digital, de correio eletrónico e, sendo caso disso, agisse em conformidade em relação a tais específicos ficheiros.

23. A fim de que a sua legítima atividade jurisdicional fosse desenvolvida de forma lícita e sem vícios, deveria o M.mo juiz de instrução, ao invés de tomar a decisão de que ora se recorre, certificar-se da existência, de entre os documentos digitais apreendidos, ficheiros que correspondessem a mensagens de correio eletrónico.

24. A intervenção jurisdicional na fase de inquérito é contida, prendendo-se com aqueles atos que, nos termos do art. 269º, do Código de Processo Penal, estejam na disponibilidade decisória do juiz de instrução, ou com aqueles outros que devam ser pessoalmente praticados por aquele (cf. art. 268º, do mesmo diploma legal).

25. A decisão ora colocada em crise, ao apreciar, em bloco e sem o cuidado de destringir entre o que é documento digital (nos termos e para os efeitos do que dispõe o art. 16º, da Lei do Cibercrime) e o que possa eventualmente corresponder a mensagens de correio eletrónico (cuja junção aos autos depende de apreciação judicial em função de critérios de necessidade face aos interesses do caso concreto), extravasou as competências que legalmente são atribuídas ao juiz de instrução em fase de inquérito.

26. Com efeito, quanto àqueles documentos, e nos termos do art. 16º, da Lei do Cibercrime, é ao Ministério Público que compete o juízo de necessidade quanto à sua apreensão, na esteira, aliás, do que sucede com os demais documentos, instrumentos, produtos ou vantagens relacionados com a prática de um facto ilícito típico suscetíveis de servir a prova (cf. art. 178º, n.º 1, do Código de Processo Penal, em conjugação com os art.s 262º, n.º 1 e 263º, n.º 1, do mesmo diploma legal).

27. A decisão proferida é, assim, e ao contrário do que nela se afirma, violadora do princípio do acusatório que rege o processo penal, desrespeitando a autonomia do Ministério Público enquanto autoridade judiciária que dirige, com poderes decisórios, a fase de inquérito.

28. Não cabe, na presente fase processual, na competência jurisdicional do juiz de instrução a decisão sobre a relevância ou não de determinados elementos para as finalidades do inquérito, ou seja, a investigação da existência de crime, a determinação dos seus agentes e a sua responsabilidade. Tal competência cabe, em exclusivo, ao Ministério Público, enquanto autoridade judiciária titular do processo penal na fase de inquérito.

29. A decisão ora em recurso trata-se de um ato materialmente de inquérito (cf. art. 262º, n.º 1, do Código de Processo Penal) que se revela absolutamente desenquadrado da atividade legalmente atribuída ao juiz de instrução criminal nesta fase processual (cf. art. 17º, do mesmo diploma legal).

30. A decisão proferida pelo tribunal a quo é, nestes termos ilegal, por não se conformar com os limites legalmente estabelecidos à atividade do juiz de instrução em fase de inquérito, revelando-se ferida de nulidade, uma vez que viola as regras de competência do tribunal [cf. art. 119º, al. e), do Código de Processo Penal].

31. A estrutura acusatória do processo penal implica a cisão entre as funções daquele que investiga daquele que julga, significando, sendo inadmissível qualquer intervenção do juiz à revelia do Ministério Público, para se pronunciar sobre a justiça do caso antes do exercício da ação penal.

32. O art. 219º, n.º 1, da Constituição da República Portuguesa, definindo as funções e estatuto do Ministério Público, densifica, do ponto de vista orgânico, uma das dimensões da estrutura acusatória do processo penal, ao consagrar esta magistratura como aquela a quem compete, entre o demais, o exercício da ação penal orientada pelo princípio da legalidade, proclamando, concomitantemente, a autonomia do Ministério Público, seja em relação aos demais órgãos de poder do Estado, seja em relação à magistratura judicial.

33. Tais referentes constitucionais foram densificados legalmente no Estatuto do Ministério Público [cf. arts. 1º, 2º, 3º, n.º 1, al. c), e 75º, n.º 1], assim como no Código de Processo Penal, onde se estabeleceu que compete ao Ministério Público dirigir o inquérito [cf. arts. 53º, n.º 2, al. b), e 263º, n.º 1], enquanto atividade dirigida à investigação da existência de um crime, à determinação dos seus agentes e da responsabilidade destes (cf. art. 262º, n.º 1, do Código de Processo Penal).

34. O Ministério Público surge assim, na estrutura processual penal portuguesa, como o dominus da fase de inquérito, cabendo-lhe a sua direção e a tomada de decisões com vista à prossecução da sua finalidade: a decisão sobre a acusação ou o seu arquivamento.

35. Neste contexto, qualquer interpretação das normas processuais penais, designadamente dos arts. 17º, 53º, n.º 2, al. b), 262º, n.º 1, 263º, n.º 1, 268º ou 269º, do Código de Processo Penal, que admita uma intervenção judicial

conformadora do destino do processo tem subjacente uma matriz essencialmente inquisitória que colide com a malha constitucional positivada. 36.A decisão recorrida, não se baseando numa análise prévia do que estará e do que não estará na alçada jurisdicional, consubstancia a prática de um ato de recolha de prova para o qual se não mostra habilitado o juiz de instrução, já que se assume como um ato materialmente de inquérito (cf. art. 262º, n.º 1, do Código de Processo Penal), considerando que lhe subjaz, ainda que tal não tenha sido expressamente invocado, um juízo de necessidade assente na circunstância de, no entender do M.mo juiz de instrução, se estar perante ficheiros correspondentes a mensagens de correio eletrónico.

37.Tal atividade é constitucionalmente vedada ao juiz de instrução, sendo violadora dos arts. 32º, n.º 5, e 219º, n.ºs 1 e 2, da Constituição da República Portuguesa, uma interpretação dos arts. 17º, 53º, n.º 2, al. b), 262º, n.º 1, 263º, n.º 1, 268º ou 269º, do Código de Processo Penal, que admita uma conformação do processo em fase de inquérito pelo juiz de instrução à revelia do poder decisório do Ministério Público.

38.O Mmo. juiz a quo excedeu os seus poderes, substituiu-se ao Ministério Público, violando as normas ínsitas aos arts. 4º, 17º, 53º, n.º 2, al. b), 263º, n.º 1, 262º, n.º 1, e 267º do Código de Processo Penal, e 1º, 2º, 3º, n.º 1, al. c), e 75º, n.º 1, do Estatuto do Ministério Público.

39.A interferência que o M.mo juiz a quo provocou na atividade do Ministério Público comprometeu irremediavelmente a acusatoriedade do processo, violando o princípio do acusatório e a autonomia do Ministério Público, consagrados, respetivamente, no art. 32º, n.º 5, e 219º, da Constituição da República Portuguesa, ao interpretar os arts 17º, 53º, n.º 2, al. b), 262º, n.º 1, 263º, n.º 1, 268º ou 269º, do Código de Processo Penal, por forma a admitirem uma conformação do processo em fase de inquérito pelo juiz de instrução à revelia do poder decisório do Ministério Público.

Pelo exposto o presente recurso merece provimento, devendo ser o despacho recorrido revogado, porquanto exorbitante das competências do juiz de instrução, em violação da Constituição da República Portuguesa e da lei, devendo ser determinado ao M.mo juiz *a quo* que o substitua por outro que determine a seleção, de entre os elementos digitais apreendidos, entre o que se trata de ficheiros correspondentes a mensagens de correio eletrónico e o que se trata de meros documentos de natureza digital para, então, sobre os primeiros, poder ser exercida validamente a competência jurisdicional em fase de inquérito”.

3. O recurso foi admitido com subida imediata, nos próprios autos e efeito devolutivo (cfr. despacho de fls. 2198).

4. O arguido veio responder ao recurso apresentado, terminando as contra-alegações com a formulação das seguintes conclusões (transcrição):
  - “1. No dia 02 de Julho de 2017 foi apreendido nas instalações da R... correio electrónico do Recorrido, através de uma cópia em bruto, relativamente ao período compreendido entre 2004 a Janeiro de 2017.
  2. O Mm<sup>o</sup> Juiz de Instrução considerou que a apreensão do correio electrónico do recorrido assume a natureza de um meio proibido de prova -violação do direito à vida privada e sigilo de correspondência -uma vez que violou o preceituado no art<sup>o</sup> 17<sup>o</sup> da LeiCIBER;
  3. O MP recorreu fundamentando a sua posição no facto de a apreensão em causa ser reconduzível ao regime previsto no artigo 16<sup>o</sup> LCIBER, carecendo assim a apreensão de prévio despacho do juiz de Instrução.
  4. Adicionalmente, o Recorrente alega, por entender que a diligência em causa não carece de despacho que a ordene ou autorize, que foram violados os artigos 17<sup>o</sup>, 53<sup>o</sup>, n<sup>o</sup> 2, al. b), 262<sup>o</sup>, n<sup>o</sup> 1, 268<sup>o</sup> e 269<sup>o</sup>, todos do CPP.
  5. A apreensão de correio electrónico está em confronto com um conjunto de direitos liberdades e garantias, com a consagração constitucional: direitos ao sigilo da correspondência e à intimidade da vida privada, cuja violação, coloca em causa a dignidade da pessoa, o desenvolvimento da personalidade, e, essencialmente, o direito à reserva da intimidade da vida privada e familiar.
  6. A LCIBER consagrou um novo regime processual -através dos artigos 11<sup>o</sup> a 19<sup>o</sup>.
  7. O regime previsto no art<sup>o</sup> 16<sup>o</sup> aplica-se sempre que esteja em causa a apreensão de dados informáticos e o do artigo 17<sup>o</sup> sempre que esteja em causa a apreensão de correio electrónico e registo de comunicações de natureza semelhante.
  8. De acordo com o artigo 17<sup>o</sup> da LCIBER a apreensão de correio electrónico ou registos de comunicações de natureza semelhante, carecem sempre de ordem ou autorização prévia do Juiz de Instrução.
  9. Com a publicação deste novo regime processual deixou de existir tratamento diferenciado relativamente ao correio electrónico lido e não lido, perdendo assim qualquer razão de ser a discussão que existiu no passado sobre a recondução da mensagem de correio electrónico já lido ao conceito normativo de correspondência.
  10. Sobre esta temática já se pronunciou a nossa jurisprudência, a saber: Ac. TRP de 9.12.12; Ac. TRL de 01.11.2011; Ac. TRE de 20.01.2015; Ac. TRL de 22.01.2013; e Ac. TRG de 29.03.2011.
  11. Bem como o MP -através do Gabinete de Cibercrime -Nota Prática n<sup>o</sup> 10/2016, de 21 de Setembro, onde refere que se as mensagens estão

armazenadas em aparelho de quem não autoriza a obtenção das mensagens: neste caso exige-se intervenção judicial, nos termos do artigo 17º da lei do Cibercrime.

12. A remissão efectuada pelo artigo 17º para o regime da correspondência, abrange quatro pressupostos específicos daquele regime. i. a referência à nulidade; ii. ao facto de ser aplicável a correio electrónico e registos de comunicação de natureza semelhante enviado ou recebido pelo suspeito, mesmo que de um endereço electrónico de outra pessoa; iii. a proibição de apreensão de correio electrónico e registos de comunicação de natureza semelhante trocado entre arguido e o seu defensor; e iv. O facto de ter que ser o juiz que autorizou ou ordenou a diligência o primeiro a tomar conhecimento do respectivo teor.

13. Restantes pressupostos do artº 179º do CPP estão consagrados no próprio artigo 17º -a título de exemplo, a necessidade de diligência revelar grande interesse ou necessidade de despacho judicial.

14. A LCIBER não distingue, propositadamente, no âmbito do escopo do artº 17º, entre mensagens de correio electrónico lidas e não lidas, abrangendo ambas, pelo que a apreensão de mensagens de correio electrónico, ainda que armazenadas, carecem sempre de ordem ou autorização do Juiz de Instrução.

15. O legislador criou um regime específico para apreensão de correio electrónico e registos de comunicação de natureza semelhante, o que faz com que a respectiva apreensão não seja abrangida na previsão normativa do artº 16º da LCIBER.

16. Neste sentido já se pronunciou a nossa doutrina, nomeadamente Paulo Pinto de Albuquerque, Rita Castanheira Neves e David Silva Ramalho, entre outros.

17. Assim, e como bem referido no despacho recorrido, a apreensão de mensagens de correio electrónico, ainda que armazenado, cai no âmbito de aplicação do regime processual penal previsto o artº 17º da LCiber, pelo que carece, sob pena de nulidade, de ordem ou autorização do juiz de Instrução.

18. Logo, bem andou o Tribunal a quo, ao considerar que a busca e apreensão efectuada ao correio electrónico e aos registos de comunicação de natureza semelhante do arguido careciam de despacho do Juiz de Instrução, violação que, nos termos do artº 179º do CPP, por remissão do artº 17º do LCiber, determina a nulidade da busca e da apreensão.

19. Quanto às demais questões suscitadas no recurso do MP, e uma vez que a decisão do Mmº Juiz a quo foi proferida de acordo com o regime do artigo 17º da LCiber, não está em causa qualquer violação da lei, da constituição ou do estatuto do MP, e muito menos a violação da estrutura acusatória do nosso sistema processual penal.

20. A decisão proferida pelo Tribunal a quo, por estar de acordo com as normas legais aplicáveis, deverá ser mantida por V. Exas., julgando-se o recurso apresentado pelo MP improcedente por não provado”.

5. Neste Tribunal o Exm<sup>o</sup> Procurador Geral Adjunto emitiu parecer no sentido da confirmação do recurso.

6. Foram colhidos os Vistos legais.

7. Procedeu-se então à Conferência com observância do legal formalismo.

Cumprido decidir.

\*

## II-FUNDAMENTAÇÃO.

1. Verificam-se, com relevância, as seguintes ocorrências processuais para a decisão do recurso:

1.1. No âmbito do presente Inquérito, por despacho proferido a 24.05.2017 (fls. 1379 a 383), o Ministério Público ordenou, na sequência do relatório intercalar da Polícia Judiciária, fls. 1360 a 1363 e 1375-1376 e despachos do Ministério Público de fls. 1356-1357, e 1370 a 1372, a realização de buscas não domiciliárias, entre as quais às empresas T... Group e à R... S.A (onde um dos visados era o ora recorrente R...).

1.2. Nessa decisão do Ministério Público consta que as buscas deverão incidir sobre toda a documentação encontrada nos respectivos postos de trabalho e arquivos utilizados pelos visados, ou pela respectiva instituição, incluindo toda a que se encontre em formato digital, ainda que se trate de documentos originados ou recebidos via correio electrónico no período em causa nos autos, fazendo constar “...entendemos existirem fundadas suspeitas de que nas instalações das empresas indicadas pode encontrar-se prova documental, mormente registos, apontamentos, ou documentos bancários, contratuais, negociais, relacionados com a actividade ilícita em investigação neste inquérito, nomeadamente em formato digital.

1.3. Do despacho em causa consta, ainda, a indicação das palavras-chave que deverão ser objecto de pesquisa a realizar nos computadores.

1.4. No mandado de busca de fls. 1407 e 1457 consta que os factos em

investigação são referentes a acontecimentos ocorridos entre 2004-2014 e têm subjacente a matéria normalmente referida como CAE e CMEC, sendo os factos susceptíveis de configurar a prática de crimes de corrupção passiva (artº 373º do CP), corrupção activa com agravação (artº 374º e 374º A do CP) e participação económica em negócio (artº 377º do CP).

1.5. No despacho de fls. 1370-1371, datado de 13.03.2017 proferido pelo Ministério Público na sequência de reunião de coordenação com a Polícia Judiciária, precisamente para preparação das buscas, refere-se:

“Realizou-se em 9.03.2017 uma reunião entre o MP (...) e a PJ (...) com vista a preparação inicial das buscas a realizar tendo sido mencionada a necessidade de se especificar bem quem são os alvos e aquilo que se busca...

Assim, necessita-se de:

“A) os documentos relacionados com o objecto dos autos (que referimos em despacho anterior);

“B) cópia dos emails pessoais/profissionais que se conseguirem através de computadores portáteis e servidores das entidades.

“Para tal é necessário o apoio de engenheiros da PJ que apõem nessas tarefas.

“As palavras que deverão ser objecto de pesquisa no conteúdo dos emails - para além daqueles que a PJ-UNCC entender como pertinentes -são:

“CMC

“custos para manutenção do equilíbrio contratual.

(...)

“Por ser mais célere, o procedimento quanto aos portáteis deverá ser o de apreender, e, depois de serem analisados pela PJ (e retirados eventuais emails), devolvem-se aos seus possuidores. No resto deve realizar-se a pesquisa informática local.

“Quanto às buscas da R... os visados serão o engenheiro JC... (Gabinete e emails) e o Dr. R... que já não trabalha lá.

a) Contudo, existe Srª A... que era sua ex-secretária. Podemos, pelo menos, abordá-la e perguntar-lhe onde estão os emails e docs ou, talvez apreender-lhe os emails e fazer uma pesquisa on site...

b) Com o Engº JC trabalhava o Engº PF.. que também teve intervenção na matéria dos CMEC e deverá ser alvo ao nível dos emails e documentação existentes no seu gabinete”.

1.7. No despacho do Ministério Público em que ordenou as buscas, não foi requerida autorização judicial para pesquisa, em suportes informáticos, de ficheiros contendo dados relativos a correio electrónico (expedido, recebido, lido) guardado em sistema informático.

1.8. A fls. 1384-1387 e 1406-1409 constam os mandados de busca.

1.9. No dia 2 de Junho de 2017 foram realizadas as buscas ordenadas.

1.10. Do auto de busca e apreensão de fls. 1450-1454, (instalações da R...), consta o seguinte:

“Face à impossibilidade de, em tempo útil, efectuar pesquisa informática com base nas referidas palavras-chave nos ficheiros resultantes de correio electrónico de R..., JC... e de PP..., foi efectuada cópia em bruto dos mesmos, relativa ao período compreendido entre 2004 e Janeiro de 2017, para o disco rígido (...) e acondicionado em saco de prova série B068531”.

1.11. O ora recorrente, conforme resulta do auto de busca e apreensão, não estava presente no momento da busca e nem se fez representar.

1.12. Por promoção de fls. 1559, com data de 9-6-2017, veio o M<sup>o</sup> P<sup>o</sup> remeter ao TCIC todos os dados que foram apreendidos em suporte digital para que o JIC proceda ao seu exame e decisão sobre a sua junção aos autos nos termos do artigo 17<sup>o</sup> da Lei n<sup>o</sup> 109/2009 e art<sup>o</sup> 179<sup>o</sup> n<sup>o</sup> 3 e 188<sup>o</sup> n<sup>o</sup> 1 e 4 do CPP.

1.13. Por requerimento de fls. 1864 ss, de 27-6-2017, veio o arguido invocar a nulidade da apreensão do correio electrónico por a mesma não ter sido precedida de autorização judicial, requerendo a declaração de nulidade da apreensão de correspondência electrónica por violação do disposto no artigo 17<sup>o</sup> da Lei do Cibercrime e artigo 179<sup>o</sup> do CPP.

1.14. Subsequentemente veio a ser proferido o despacho judicial ora sob recurso, que declarou a nulidade do despacho do M<sup>o</sup> P<sup>o</sup> na parte em que autorizou a apreensão de correio electrónico de R... (R...).

Do qual consta o seguinte:

“Os presentes autos tiveram início em 3-10-2012, com base na denúncia anónima de fls. 2.

Por despacho proferido a 24-05-2007 (fls. 1379-1383), o Ministério Público ordenou, na sequência do relatório intercalar da PJ, fls. 1360 a 1363 e 1375-1376 e despachos do M<sup>o</sup> P<sup>o</sup> de fls. 1356-1357, e 1371-1372, a realização de buscas não domiciliárias, entre as quais à requerente T... Consulting ..., assim como à R... S.A (onde um dos visados era o agora requerente).

Nessa decisão, consta que as buscas deverão incidir sobre toda a documentação encontrada nos respectivos postos de trabalho e arquivos utilizados pelos visados, ou pela respectiva instituição, incluindo toda a que se encontre em formato digital, ainda que se trate de documentos originados ou recebidos via correio electrónico no período em causa nos autos.

Mais é dito que, considerando o teor das informações acima referidas, em face de toda a prova indiciária presente nos autos, entendemos existirem fundadas suspeitas de que nas instalações das empresas indicadas pode encontrar-se prova documental, mormente registos, apontamentos, ou documentos bancários, contratuais, negociais, relacionados com a actividade ilícita em investigação neste inquérito, nomeadamente em formato digital.

Do despacho em causa consta, ainda, a indicação das palavras-chave que deverão ser objecto de pesquisa a realizar nos computadores.

No mandado de busca de fls. 1407 e 1457 consta que os factos em investigação são referentes a acontecimentos ocorridos entre 2004-2014 e têm subjacente a matéria normalmente referida como CAE e CMEC. São susceptíveis de configurar a prática de crimes de corrupção passiva (artº 373º do CP), corrupção activa com agravação (artº 374º e 374º A do CP) e participação económica em negócio (artº 377º do CP).

Nesse despacho, não foi requerida autorização judicial para pesquisa, em suportes informáticos, de ficheiros contendo dados relativos a correio electrónico (expedido, recebido, lido) guardado em sistema informático, e, com vista à apreensão dos relevantes para o objecto dos autos, de acordo com o disposto no art.º 17º da Lei n.º 109/09, de 15 de Setembro.

A fls. 1384-1387 e 1406-1409 constam os mandados de busca.

No dia 2 de Junho de 2017 foram realizadas as buscas ordenadas.

Do auto de busca e apreensão de fls. 1450-1454, (instalações da REN), consta que, face à impossibilidade de, em tempo útil, efectuar pesquisa informática com base nas referidas palavras-chave nos ficheiros resultantes de correio electrónico de R, Re P, foi efectuada cópia em bruto dos mesmos, relativa ao período compreendido entre 2004 e Janeiro de 2017, para o disco regido, acondicionado em saco de prova série B068531.

O requerente, conforme resulta do auto de busca e apreensão, não estava presente no momento da busca e nem se fez representar.

Por promoção de fls. 1559, com data de 9-6-2017, veio o Mº Pº remeter a este TCIC todos os dados que foram apreendidos em suporte digital para que o JIC proceda ao seu exame e decisão sobre a sua junção aos autos nos termos do artigo 17º da Lei nº 109/2009 e artº 179º nº 3 e 188º nº 1 e 4 do CPP.

Por requerimento de fls. 1864ss, entrado no DCIAP no dia 27-6-2017, veio o requerente invocar a nulidade da apreensão do correio electrónico por a mesma não ter sido precedida de autorização judicial.

Requerer, assim, que seja declarada a nulidade da apreensão de correspondência electrónica por violação do disposto no artigo 17º da Lei do cibercrime e artigo 179º do CPP.

A fls. 2001 veio o Mº Pº responder pugnando pela improcedência da ilegalidade invocada dizendo, em síntese, que a busca não visou o correio electrónico mas sim uma pesquisa informática.

Cumprido conhecer:

Antes de mais, há que dizer que o que está em causa com a pretensão do

arguido acima referido não é a autonomia do M<sup>o</sup> P<sup>o</sup> e nem, muito menos, a titularidade do inquérito, mas sim a defesa de direitos, liberdades e garantias dos cidadãos.

Ora, tratando-se de direitos fundamentais a questão (artigo 34<sup>o</sup> da CRP) não poderá estar fora da sindicância jurisdicional a exercer pelo juiz de instrução criminal, enquanto juiz de garantias e de liberdades, por força do artigo 202<sup>o</sup> n<sup>o</sup> 2 da CRP quando afirma que, na administração da justiça incumbe aos tribunais assegurar a defesa dos direitos e interesses legalmente protegidos dos cidadãos e do artigo 17<sup>o</sup> do CPP quando estatui que o juiz de instrução tem competência, além do mais, (...) exercer todas as funções jurisdicionais até a remessa do processo a julgamento».

Para além disso, este entendimento não colide com a estrutura acusatória do processo penal, consagrada no artigo 32<sup>o</sup> n<sup>o</sup> 5 da CRP, nem com a separação orgânica e funcional entre as duas magistraturas que se verifica mesmo na fase de inquérito e nem, muito menos, poderá ser tida como uma posição de sindicante por parte do JIC da actividade do Ministério Público. Esta posição é, em nosso entender, a que melhor se coaduna com as funções do juiz de instrução enquanto garante de direitos fundamentais dos cidadãos.

No mesmo sentido se pronunciou J, para quem a declaração de nulidade tem carácter materialmente judicial, e porque na fase do inquérito compete ao juiz de instrução criminal praticar ou sindicat todos os actos que contendem com direitos, liberdades e garantias individuais, onde se inclui o conhecimento das nulidades (In Contributo para a Análise da Inexistência e das Nulidades Processuais Penais, pág. 189 e ss, nota 439).

Para além disso, o n.º 4 do artigo 32<sup>o</sup> da CRP prossegue a tutela de defesa dos direitos do cidadão no processo criminal e, nessa exacta medida, determina o monopólio pelo juiz da instrução, juiz-garante dos direitos fundamentais dos cidadãos (“reserva do juiz”).

Neste sentido, veja-se o AC do Tribunal Constitucional n<sup>o</sup> 228/2007 quando diz que: «Decisivamente, entende o Tribunal que, tratando-se de uma intervenção significativa nos direitos fundamentais do arguido, se impõe um controlo prévio pelo juiz como expressão da separação de poderes e competências decorrente da estrutura acusatória do Processo Penal consagrada nos artigos 32<sup>o</sup>, n<sup>os</sup> 4 e 5 do Código de Processo Penal».

«..., o n.º 4 do artigo 32<sup>o</sup> da CRP prossegue a tutela de defesa dos direitos do cidadão no processo criminal e, nessa exacta medida, determina o monopólio pelo juiz da instrução, juiz-garante dos direitos fundamentais dos cidadãos (“reserva do juiz”)».

Sob a epígrafe “Outros direitos pessoais” a Constituição da República consagra no seu artigo 26<sup>o</sup> um conjunto de direitos fundamentais que

protegem “um círculo nuclear da pessoa, correspondendo, genericamente, a direitos de personalidade”. Entre esses direitos, está o direito fundamental à reserva da vida privada, cuja tutela se projecta em sede processual penal, o direito ao bom nome e reputação. Por sua vez, o artigo 32º nº 2 consagra o princípio da presunção de inocência.

Cumprir referir, também, que estando em causa direitos fundamentais a sua restrição, no âmbito dos presentes autos, apenas se justifica para prossecução das finalidades específicas do processo penal, ou seja, com vista à investigação da existência de um crime, determinar os seus agentes e a responsabilidade deles e descobrir e recolher provas, em ordem à decisão (artigo 262º nº1 do CPP).

Face ao exposto, conclui-se que, contendo a situação em causa, com direitos, liberdades e garantias fundamentais do visado, a sua admissibilidade no decurso da fase de inquérito depende, pelas mesmas razões que justificam essa dependência no caso dos actos que constam da lista constante do artigo 269º do Código de Processo Penal, isto é, por consubstanciar intervenção significativa nos direitos fundamentais do arguido/suspeito, de apreciação por parte do juiz de instrução.

Assim sendo, a apreciação da questão é da competência do Juiz de Instrução Criminal.

Da nulidade da apreensão de correio electrónico.

O artigo 189.º número 1 do Código de Processo Penal que determina a aplicação das regras e formalidades relativas ao regime da interceptação e gravação de comunicações telefónicas, quando esteja em causa a intromissão nas comunicações ou conversações já armazenadas em suporte digital.

Daqui resulta que a intromissão nas comunicações já armazenadas em suporte digital deverá seguir o regime processual aplicável à interceptação e gravação de comunicações telefónicas (artigo 189.º número 1, segunda parte).

Assim, só é permitido o recurso a este tipo de diligência em processos relativos aos crimes elencados no artigo 187.º número 1 (deixando de fora um conjunto significativo de crimes informáticos); o recurso a este tipo de diligência só é permitido durante a fase do inquérito e “se houver razões para crer que a diligência é indispensável para a descoberta da verdade, ou que a prova seria, de outra forma, impossível ou muito difícil de obter e apenas quanto às pessoas identificadas no nº 4 do artigo 187º do CPP.

A matéria relativa ao correio electrónico mostra-se actualmente regulada pelo Art.º 17º da Lei nº 109/2009, de 15/09.

A Lei do Cibercrime, Lei nº 109/2009, de 15 de Setembro, a qual transpõe para a ordem jurídica interna a Decisão Quadro nº 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.º 17º, 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.

Daqui resulta que, aplicando-se o regime de apreensão de correspondência previsto no Código de Processo Penal, o mesmo terá que seguir a disciplina do art.º 189º, o qual estabelece, desde logo, no nº 1 que tais apreensões sejam determinadas por despacho judicial, “sob pena de nulidade” expressa (nº 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.º 268º nº 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 nº 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.

Por sua vez, diz o artigo 17º da Lei nº 109/2009, de 15 de Setembro: «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».

Da leitura desta norma, verifica-se que, no que diz respeito ao correio electrónico, o legislador foi mais exigente, na medida em que criou um regime específico para apreensão de «correio electrónico e registos de comunicação de natureza semelhante» o que faz com que esta matéria esteja fora do âmbito

do regime para a apreensão de dados informáticos previsto no artigo 16º da Lei do Cibercrime.

Deste modo, verifica-se que os regimes processuais previstos na Lei do Cibercrime e no Código de Processo Penal, a respeito da ingerência nas comunicações electrónicas armazenadas em suporte digital, são distintos. Em face do exposto, a primeira questão que se coloca é de saber qual o regime processual que deve ser aplicado quando esteja em causa a intromissão em comunicações electrónicas já armazenadas em suporte digital: o regime consagrado na da Lei do Cibercrime? Ou, por sua vez, o regime previsto no artigo 189.º número 1 do Código de Processo Penal, que remete para a aplicação do regime das “escutas telefónicas”?

Por sua vez, se concluirmos que é o regime estatuído no artigo 17.º - que remete para a aplicação das regras e formalidades consagradas nos artigos 179.º e 252.º do Código de Processo Penal - se as referidas regras e formalidades aplicam-se na íntegra.

Quanto a esta questão, concordamos com Paulo Dá Mesquita quando considera que o artigo 17.º da Lei do Cibercrime foi “o primeiro passo da directa revogação de algumas implicações do regime do Código de Processo Penal sobre intromissão em comunicações.” Assim, para este Autor, a extensão legal prevista no artigo 189.º número 1 do Código de Processo Penal deixa de se aplicar quando esteja em causa a apreensão de mensagens de correio electrónico e registos de comunicações de natureza semelhante o que faz com que o regime da apreensão de correio electrónico e registos de comunicações de natureza semelhante esteja regulado directamente pelo artigo 17.º da Lei do Cibercrime e, subsidiariamente (por remissão expressa do mesmo), pelos pressupostos e requisitos legais relativos à apreensão de correspondência, previstos nos artigos 179.º e 252.º (nº 2 e 3) do Código de Processo Penal.

No mesmo sentido, Pedro Verdelho defende que ao regime da apreensão de correspondência electrónica deve ser aplicado, por remissão expressa, o regime processual previsto nos artigos 179.º do CPP.

Tal como foi referido no acórdão do Tribunal da Relação de Guimarães, de 29 de Março de 2011, a redacção introduzida pelo legislador em 2007 ao artigo 189.º número 1 do CPP foi “infeliz” uma vez que incluíram no regime das “escutas telefónicas” o produto do acto comunicacional, que nada tem a ver com o fundo do regime, nomeadamente, a intromissão nas telecomunicações, tratando-se antes de meros arquivos digitais.

No mesmo sentido, acórdão do Tribunal da Relação de Lisboa, de 11-1-2011: «Quanto à apreensão de mensagens de correio electrónico ou registos de comunicações de natureza semelhante, a Lei do Cibercrime, ao remeter para o

regime geral previsto no Código de Processo Penal, determina a aplicação deste regime na sua totalidade, sem redução do seu âmbito - tais apreensões têm de ser autorizadas ou determinadas por despacho judicial, devendo ser o juiz a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida, sob pena de nulidade».

Uma vez aqui chegados, cumpre saber se, ao caso concreto, é aplicável o regime de apreensão de correspondência previsto no Código de Processo Penal na sua totalidade.

Nos termos do artigo 179.º do Código de Processo Penal:

1. A apreensão de correspondência só poderá ser ordenada ou autorizada quando existirem “fundadas razões para crer que:

- a) a correspondência foi expedida pelo suspeito ou lhes 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”

2. A referida diligência terá de ser previamente autorizada ou ordenada pela autoridade judicial, só sendo permitida, em casos excepcionais, que os órgãos de polícia criminal procedam à sua apreensão sem prévia autorização;

3. 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 17º da Lei do cibercrime e os direitos fundamentais em causa - direito à reserva da intimidade da vida privada e familiar - artigo 26º n 1 e inviolabilidade da correspondência - artigo 34º 1, ambos da CRP - entendemos 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. Na verdade, não faria sentido, deixar de considerar os restantes requisitos, fazendo a apreensão de correio electrónico depender apenas de a diligência “se afigurar ser de grande interesse para a descoberta da verdade ou para a prova”, e ignorar os demais previstos no citado artigo 179º do CPP.

Para além disso, 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 (cf. arts. 26.º, n.º 1, 34.º, n.º 1 e 18.º, n.ºs 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.ª ed., Coimbra Editora, 2007, págs. 388 e 392).

Por outro lado, 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, ou seja, 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). Assim sendo, a remissão para o regime da apreensão de correspondência está, pois, condicionada aos seguintes aspectos:

A referência à nulidade, em caso de inobservância dos requisitos legais (artigo 179.º número 1 e 2);

Quando se tratar de correspondência electrónica que foi “expedida pelo suspeito ou lhe é dirigida, mesmo que sob nome diverso ou através de pessoa diversa” (artigo 179.º, número 1, alínea a));

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.º número 2).

4. O juiz (que ordenou ou autorizou a diligência) deverá ser o primeiro a tomar conhecimento do conteúdo da correspondência electrónica apreendida (artigo 179.º número 3).

Tendo em atenção o caso em apreço, verifica-se que os crimes em investigação - corrupção e participação económica em negócio - admitem o recurso a este meio de obtenção de prova.

Porém, quanto ao segundo requisito, verifica-se, desde logo, que a apreensão do correio electrónico do arguido R... (R..) teve lugar na sequência de uma decisão não judicial, ou seja, mediante despacho do Ministério Público.

A questão que se coloca agora é a de saber se, tratando-se de correio electrónico, como é o caso concreto, já recebido e armazenado, o mesmo deverá ser objecto de tratamento semelhante relativamente à apreensão de arquivo físico já recebido/lido e armazenado, podendo, neste caso, a autoridade judiciária (incluindo o Ministério Público al. b) artº 1º do CPP), ordenar a sua apreensão nos termos do artigo 16º da Lei do Cibercrime ou se, pelo contrário, deverá continuar a merecer o mesmo tratamento relativo às intercepções de correio electrónico em tempo real.

Em primeiro lugar, se tivermos em atenção o texto do artigo 17º da Lei do Cibercrime verifica-se que o legislador fala em «...forem encontrados, armazenados nesse sistema informático...», o que pressupõe que a comunicação já foi recebida/lida e, conseqüentemente, armazenada. Assim, recorrendo ao argumento literal somos levados a concluir que o legislador não quis fazer distinção entre correio armazenado e correio não armazenado.

Para além disso, da leitura do citado artigo 17º, verifica-se, como já dissemos acima, que, no que diz respeito ao correio electrónico, o legislador foi mais exigente, na medida em que criou um regime específico para apreensão de «correio electrónico e registos de comunicação de natureza semelhante» o que faz com esta matéria esteja fora do âmbito do regime para a apreensão de dados informáticos previsto no artigo 16º da Lei do Cibercrime.

Por fim, se tivermos presente os direitos fundamentais em conflito, nomeadamente, os constantes nos artigos 26º nº 1 e 34º da CRP - reserva da intimidade da vida privada e inviolabilidade da correspondência - teremos de concluir que se justifica uma tutela acrescida nos casos de ingerência nas comunicações armazenadas em suporte digital em relação à ingerência nos arquivos físicos que não contenham comunicações.

Assim sendo, a situação em causa não recai no âmbito do artigo 16º (que regula a apreensão de dados informáticos), o que faz com que o Mº Pº não tenha competência para ordenar a sua pesquisa e apreensão, mas sim no âmbito do artigo 17º da Lei do Cibercrime e artigo 179º nº 1 do CPP e incluída entre os actos a ordenar ou autorizar pelo juiz de instrução, nos termos do artigo 269º nº 1 c) do CPP.

Nesta conformidade e sancionando a lei - artigo 179º nº 1 do CPP e artigo 17º da Lei do Cibercrime - com nulidade a violação das regras relativas à competência para a autorização de apreensão de correio electrónico, faz com que o despacho do Mº Pº esteja ferido de nulidade, nulidade esta que, por força do artigo 120º nº 1 do CPP deve ser invocada pelos interessados.

Uma vez que o interessado não estava presente no momento da busca e apenas tomou conhecimento da mesma, assim como do despacho do Mº Pº, no dia 27-6-2017 (cfr fls. 1856) e invocou a nulidade no próprio dia 27-06, essa invocação é tempestiva - artigo 120º nº 1 e 3 do CPP.

As nulidades tornam inválido o acto em que se verificarem, bem como os que dele dependerem e aqueles que puderem afectar, o que faz com que o acto não produza efeitos, não tenha valor (cf. art.º 122.º).

Em face do exposto, declaro a nulidade do despacho do Mº Pº na parte em que autorizou a apreensão de correio electrónico de R. (R...).

Esta ilegalidade reconduz a busca, na parte relativa à apreensão do correio electrónico, a um meio proibido de prova, por violação do direito à privacidade e sigilo de correspondência e, conseqüentemente, à nulidade da prova obtida com a mesma,

Após trânsito, proceda-se à eliminação do suporte informático constante do Saco Prova B 068531 (REN) e do suporte informático identificado a fls. 1834, ficando os mesmos, até lá, acondicionados no cofre deste TCIC.

Notifique”.

\*

## 2. O Direito.

2.1. Conforme entendimento pacífico da doutrina e jurisprudência, o âmbito do recurso é delimitado pelas conclusões do recorrente[1], vindo o presente recurso a colocar as seguintes questões:

a. Do regime jurídico de *apreensão* de mensagens de *correio electrónico*.

-O âmbito de aplicação do artº 17º da Lei do Cibercrime e a remissão para o artigo 179º do Código de Processo Penal;

b. Da ocorrência ou não de nulidade da apreensão de correio electrónico no caso dos autos.

c. Da competência do juiz de Instrução para apreciar e declarar eventual nulidade da apreensão de correio electrónico levada a efeito pelo Ministério Público durante o Inquérito?

O recurso coloca a seguinte sub-questão:

d. O âmbito do conceito de *correspondência*: correio fechado/aberto, lido/não lido.

-Quando o correio electrónico já se encontre aberto, na esfera de conhecimento do destinatário e armazenado no sistema informático, deixa de ter natureza de *correspondência*, seguindo a sua apreensão o regime previsto no artº 16º da Lei do Cibercrime, não carecendo por isso a sua apreensão de autorização judicial?

2.2. O Ministério Público insurge-se contra o despacho proferido pelo Srº Juiz de Instrução Criminal de 15.06.2017, por neste despacho ter declarado a nulidade do despacho do Ministério Público, na parte em que o Ministério Público autorizou a apreensão de correio electrónico de R... (R...), e ter considerado que tal ilegalidade reconduz a busca, na parte relativa à apreensão do correio electrónico, a um meio proibido de prova, por violação do direito à privacidade e sigilo de correspondência.

Entende também o Digno recorrente que o despacho do Sr. Juiz de Instrução deverá ser revogado, por ter exorbitado as competências que legalmente lhe são atribuídas em fase de Inquérito, não tendo o Juiz de Instrução competência para declarar a nulidade da apreensão levada a efeito pelo Ministério Público.

2.3. Para melhor compreensão cumpre fazer um breve enquadramento processual tendo em vista a cronologia dos factos:

2.3.1. No caso dos autos está em causa a realização de buscas não domiciliárias ordenadas pelo Ministério Público, considerando que os factos indiciados são susceptíveis de configurar a prática de crimes de corrupção passiva (artº 373º do CP), corrupção activa com agravação (artº 374º e 374º-A do CP) e participação económica em negócio (artº 377º do CP).

2.3.2. Na decisão do Ministério Público que ordenou as buscas consta que as mesmas tinham por objecto toda a documentação encontrada nos respectivos postos de trabalho e arquivos utilizados pelos visados, ou pela respectiva instituição, incluindo toda a que se encontre em *formato digital*, ainda que se trate de documentos originados ou recebidos via *correio electrónico* no período em causa nos autos, fazendo constar “..existirem fundadas suspeitas de que nas instalações das empresas indicadas pode encontrar-se prova documental, mormente registos, apontamentos, ou documentos bancários, contratuais, negociais, relacionados com a actividade ilícita em investigação neste inquérito, nomeadamente em *formato digital*”.

2.3.3. No despacho datado de 13.03.2017 proferido pelo Ministério Público na sequência de reunião de coordenação com a Polícia Judiciária, precisamente para preparação das buscas, refere-se:

“Realizou-se em 9.03.2017 uma reunião entre o MP (...) e a PJ (...) com vista a preparação inicial das buscas a realizar tendo sido mencionada a necessidade de se especificar bem quem são os alvos e aquilo que se busca...

Assim, necessita-se de:

“A) os documentos relacionados com o objecto dos autos (que referimos em despacho anterior);

“B) cópia dos emails pessoais/profissionais que se conseguirem através de computadores portáteis e servidores das entidades.

“Para tal é necessário o apoio de engenheiros da PJ que apõem nessas tarefas. (...)”

“Por ser mais célere, o procedimento quanto aos portáteis deverá ser o de apreender, e, depois de serem analisados pela PJ (e retirados eventuais emails), devolvem-se aos seus possuidores. No resto deve realizar-se a pesquisa informática local.

“Quanto às buscas da R.. os visados serão (...) e o Dr. R... que já não trabalha lá.

a) Contudo, existe Srª A... que era sua ex-secretária. Podemos, pelo menos, abordá-la e perguntar-lhe onde estão os emails e doc´s ou, talvez apreender-lhe os emails e fazer uma pesquisa on site...

(...)”

2.3.4. Do *auto de busca e apreensão* consta que, face à impossibilidade de, em tempo útil, efectuar pesquisa informática nos ficheiros resultantes de correio electrónico dos visados, foi efectuada cópia em bruto dos mesmos, relativa ao período compreendido entre 2004 e Janeiro de 2017, para o disco rígido, acondicionado em saco de prova série B068531.

2.3.5. Por promoção de fls. 1559, com data de 9-6-2017, veio o M<sup>o</sup> P<sup>o</sup> remeter ao TCIC todos os dados que foram apreendidos em suporte digital para que o JIC proceda ao seu exame e decisão sobre a sua junção aos autos nos termos do artigo 17<sup>o</sup> da Lei n<sup>o</sup> 109/2009 e art<sup>o</sup> 179<sup>o</sup> n<sup>o</sup> 3 e 188<sup>o</sup> n<sup>o</sup> 1 e 4 do CPP.

2.3.6. Por requerimento de 27-6-2017, veio o arguido invocar a nulidade da apreensão do correio electrónico por a mesma não ter sido precedida de *autorização judicial*, requerendo a declaração de nulidade da apreensão de correspondência electrónica por violação do disposto no artigo 17<sup>o</sup> da Lei do Cibercrime e artigo 179<sup>o</sup> do CPP.

2.3.7. Subsequentemente veio a ser proferido o despacho judicial ora sob recurso, que declarou a nulidade do despacho do M<sup>o</sup> P<sup>o</sup> na parte em que autorizou a apreensão de correio electrónico de R... (R...).

2.4. O Digno Recorrente assenta a sua posição, em que pugna pela revogação do despacho do Sr<sup>o</sup> Juiz de Instrução, aduzindo a seguinte argumentação:

- A operacionalidade do regime previsto no art<sup>o</sup> 17<sup>o</sup> da Lei do Cibercrime e art<sup>o</sup> 179<sup>o</sup> do CPP depende de um facto que foi absolutamente desvalorizado na decisão em recurso: é que só se aplica este regime se estiver em causa a *apreensão de correspondência*, que é um pressuposto material e essencial para cair no âmbito do art<sup>o</sup> 17<sup>o</sup> da Lei do Cibercrime.

-Constitui requisito relevante do conceito de *correspondência* que se esteja perante um processo comunicacional não concluído, isto é, que a mensagem tenha sido expedida pelo remetente e não tenha ainda entrado no domínio cognitivo do destinatário.

-Deixa de ser *correspondência* desde que o correio electrónico seja aberto pelo destinatário, ficando assim concluída a dinâmica comunicacional e perdendo a mensagem as características que a faziam pertinente à tutela da correspondência.

-Só o correio electrónico a cujo conteúdo o seu destinatário não tenha acedido pode ser candidato à protecção legal prescrita nos termos do art<sup>o</sup> 17<sup>o</sup>, da Lei do Cibercrime e do art<sup>o</sup> 179<sup>o</sup> do Código de Processo Penal (reserva jurisdicional).

-No caso dos autos, de acordo com os referidos critérios, entende o recorrente

que o que foi apreendido na busca levada a efeito não se trata de *correspondência*, porquanto não estão em causa mensagens em trânsito, expedidas por um remetente e ainda não entradas no domínio cognitivo do destinatário.

-Muito pelo contrário, tratam-se de mensagens já abertas e cujo conteúdo já foi plenamente apreendido pelo destinatário e armazenadas em arquivo após tomada desse conhecimento. O que está em causa são *ficheiros electrónicos* outrora correio electrónico, tendo a mesma natureza que escritos guardados pelo seu detentor.

-Entende que este correio electrónico fica apenas sujeito ao regime a que alude o artº 16º da Lei do Cibercrime, bastando-se as suas necessidades de tutela com um controlo judicial posterior, ao abrigo do disposto no nº 3 do artº 16º da Lei do Cibercrime.

-As pesquisas a realizar visariam, exclusivamente, documentos originados em correio electrónico recebido ou remetido durante o período compreendido entre os anos de 2004 a 2014, tendo sido convicção do MP que inexistiriam, em relação a tal período e face à sua anterioridade no tempo, ficheiros de correio electrónico propriamente ditos armazenados que suscitasse a intervenção judicial para o feito de acesso aos mesmos e sua apreensão.

-Subsequentemente, após a apreensão, e depois de o arguido ter suscitado a nulidade da apreensão de correio electrónico, o Ministério Público remeteu para ao TCIC todos os dados que foram apreendidos em suporte digital, solicitando ao Juiz de Instrução o seguinte:

- a. Que determine a selecção, de entre os elementos digitais apreendidos, entre o que se trata de ficheiros correspondentes a mensagens de correio electrónico e o que se trata de meros documentos de natureza digital (correio electrónico já lido) para, então, sobre os primeiros, poder ser exercida validamente a competência jurisdicional;
- b. e nessa destrição entre o que é documento digital nos termos do artº 16º, da Lei do Cibercrime, aferir, nos termos do nº 3 deste preceito, da susceptibilidade do seu conteúdo poder revelar dados pessoais ou íntimos e ponderar da sua junção ou não aos autos.

Feito este caminho, lamenta o Ministério Público que o Srº Juiz de Instrução Criminal não tenha dado cumprimento ao solicitado (a destrição entre correio electrónico lido ou não lido), ficando assim sem se saber se existia correio electrónico já lido, que na perspectiva do Ministério Público podia legalmente ter sido apreendido sem autorização judicial.

### 3. Conhecendo.

3.1. Em face das relatadas vicissitudes, e pelas razões que abaixo iremos explicar, desde já adiantamos que, com o devido respeito por opinião diversa, não nos parece assistir razão ao Digno recorrente, desde logo, porque a cópia das mensagens de *correio electrónico*, realizada na sequência da referida *pesquisa informática*, integra materialmente o procedimento de *apreensão* do artº 17º da Lei do Cibercrime, que remete para o disposto o artº 179º do CPP, pelo que não podia ser autorizada pelo Ministério Público sem que este obtivesse *previamente* o competente mandado judicial para o efeito.

Vejamos o porquê deste entendimento.

Antes de tudo o mais, importa salientar que a questão a decidir incide fundamentalmente na protecção de direitos fundamentais: o direito à reserva da intimidade da vida privada e familiar e o direito ao sigilo de correspondência (cfr. arts. 26º e 34º da CRP).

O nº 1 do artº 34º da nossa Constituição estabelece que “...o *sigilo da correspondência e dos outros meios de comunicação* privada são *invioláveis*, e no nº 4 estabelece que excepções à proibição de ingerência das autoridades públicas na correspondência, nas telecomunicações e nos outros meios de comunicação só podem ocorrer nos “*casos previstos na lei em matéria criminal*”, estando assim as excepções sujeitas a *reserva de lei*.

O Tribunal Constitucional tem entendido que não exigindo o nº 4 do citado artº 34º, de forma expressa, *autorização judicial* para a realização de escutas ou para a intromissão na correspondência, a sujeição a *autorização judicial* pela lei processual justifica-se pelo princípio da proporcionalidade, face à “*especial danosidade social*” desta intromissão nas *comunicações e na correspondência*, implicando, assim, esta especial danosidade o controlo judicial. (ved. Jorge Miranda . Rui Medeiros, *Constituição Portuguesa Anotada*, Tomo I, 2ª edição, págs. 775 e 776).

O legislador constitucional no artº 32º, nº 8 fulmina com a nulidade todas as provas obtidas, além do mais, com abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações.

\*

Assente em tais princípios, importa então saber se a ingerência levada a efeito pelo Ministério Público nos meios de comunicação em causa nos autos, obedeceu às exigências e formalidades legais aplicáveis?

3.2. Do regime jurídico aplicável à *ingerência* nas comunicações em suporte digital.

Como vimos, o Digno recorrente assenta a sua argumentação distinguindo entre mensagens de correio electrónico abertas ou fechadas para efeitos de determinação do regime legal aplicável, pugnando no sentido de que a recolha de correio electrónico *aberto* está sujeita às regras que conformam a apreensão de *meros documentos*, e por isso, sem necessidade de intervenção do juiz de instrução criminal.

Entende por isso que a recolha de prova levada a efeito não traduz uma intromissão abusiva na vida privada ou nas telecomunicações e por isso não pode a apreensão ser declarada nula.

Vejamos:

Como é sabido, antes de 2007, a doutrina e jurisprudência tendencialmente consideravam aplicável ao *correio electrónico* a distinção tradicional formulada a propósito da *correspondência física*, entre mensagens abertas e lidas pelo seu destinatário, e mensagens ainda fechadas.

Fazendo esta distinção, o correio electrónico ainda “em trânsito” só poderia ser validamente interceptado com observância dos requisitos aplicáveis ao regime das escutas telefónicas, previstos nos artigos 187º a 189º (na numeração do CPP anterior), e que implicava a *autorização do Juiz de Instrução Criminal*.

Quando a mensagem se encontrava já na esfera de conhecimento do destinatário, tratava-se então de uma mensagem de correio electrónico já *aberta e lida*, de forma idêntica ao que sucedia com a correspondência física já aberta, sendo a apreensão autorizada, ordenada ou validada por despacho da *autoridade judiciária*<sup>[2]</sup> entendendo-se não haver nesta situação razões que justificassem a atribuição de uma maior protecção do que aquela que é conferida à *apreensão* de meros documentos prevista nos artº 178º do CPP.

Com a Reforma de 2007, levada a cabo pela Lei nº 48/2007, de 29 de Agosto, foi acrescentado um novo número ao actual artº 189º do CPP, passando 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 guardadas em suporte digital, e à interceptação das comunicações entre presentes*” (sublinhado nosso).

Desta norma legal, resulta que o legislador estendeu o regime das escutas telefónicas a duas realidades diferentes: por um lado, regula as comunicações/

conversações, em tempo real, realizadas através de um meio técnico diferente do telefone e, por outro lado, regula as conversações/comunicações electrónicas (ou seja, dados informáticos) mesmo que se encontrem guardadas em suporte digital, não distinguindo entre mensagens abertas/fechadas.

O regime das escutas telefónicas agora aplicável à “transmissão das conversações ou comunicações electrónicas” determina que só podem ser autorizadas por despacho fundamentado do *juiz de instrução* e mediante requerimento do Ministério Público ( artº 187º, nº 1 do CPP).

Somos assim a entender que o legislador com esta alteração, sujeitando expressamente o correio electrónico ao regime das intercepções telefónicas, quis estender a protecção conferida às comunicações que exigem, sob pena de nulidade, autorização ao juiz, ao correio electrónico, independentemente de o destinatário dele ter ou não tomado conhecimento.

Cada vez mais, nesta forma de comunicação pela sua própria forma de funcionamento, se impõe uma protecção reforçada de inviolabilidade, expressando o legislador tal reforço através precisamente da exigência de intervenção do juiz de instrução na obtenção das comunicações e conversações através de correio electrónico *armazenado em suporte digital*, independentemente de o destinatário dele ter ou não tomado conhecimento.

Temos assim que até à entrada em vigor da Lei do Cibercrime, em 2009, o artº 189º do CPP, que remetia para o regime das escutas telefónicas, era a única disposição legal que previa a admissibilidade da recolha de prova digital. Como sabemos, esta reforma de 2007 foi objecto de um juízo crítico por parte da doutrina e jurisprudência, insurgindo-se o Prof. Costa Andrade precisamente com o facto de o legislador ter estendido o regime das escutas telefónicas ao *email* guardado no computador do destinatário, afirmando que “...o preceito vem onerar e dificultar desmesuradamente a investigação criminal, assegurando a estes documentos uma tutela mais consistente do que a oferecida pelo regime das buscas. Regime a que, em princípio, seriam (e deveriam) ser submetidas as intromissões nestes “documentos”, não fora o gesto menos pensado do legislador de 2007 a aditar o inciso “mesmo que se encontrem guardados em suporte digital”. 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 uma verdadeira redução teleológica *in mala partem*. Sendo como tal, constitucionalmente insustentável”- (sublinhado nosso)

(-in “bruscamente no verão passado”, a reforma do Código de Processo Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente, publicada pela primeira vez na Revista de Legislação e Jurisprudência em 2008. Este texto foi depois publicado, em 2009, pela Coimbra Editora).

Também alguma Jurisprudência teceu duras críticas a propósito da ampliação do artº 189º, nº 1, segunda parte, considerando ter sido infeliz, uma vez que incluíram no regime das escutas telefónicas o produto do acto comunicacional, que nada tinha a ver com a intromissão nas telecomunicações, tratando-se antes de meros arquivos digitais.

Não aplicavam tal normativo quando estivesse em causa a apreensão de correio electrónico ou outras formas de transmissão de dados por via telemática, desde que já recebidos/lidos e armazenados pelo destinatário, equiparando-os ao arquivo físico recebido, lido e guardado.

Neste sentido, entre outros, o acórdão do TRG, de 12.10.2009, acórdão do TRP de 27.01.2010, acórdão do TRC de 29.03.2006 e os acórdãos do TRL de 20.03.2000 e 15.07.2008, todos inseridos no site [www.dgsi.pt](http://www.dgsi.pt).

3.3. Do regime do artº 17º da Lei do Cibercrime e da sua reemissão para o artº 179º do CPP.

Em 2009, com a aprovação da Lei do Cibercrime (Lei 109/2009 de 25 de Setembro) foi introduzida, pela primeira vez no nosso ordenamento, um regime jurídico de prova digital que veio alterar esta abordagem.

A Lei nº 109/2009, de 25 de Setembro, transpôs para a ordem jurídica interna a Decisão Quadro nº 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, adaptando o direito interno à Convenção Sobre Cibercrime do Conselho da Europa.

Tal como referia Paulo Dá Mesquita, “até 2009, existia a necessidade de se proceder a uma “reconstrução conceptual complexa, com um enquadramento teórico que se adaptasse à ruptura epistemológica introduzida pela novas tecnologias no processamento, captação e memória das comunicações” (Paulo Dá Mesquita, *Processo Penal, Prova e Sistema Jurídico*, Coimbra Editora, 2011, pp 84 e 85.

Havia, pois, a necessidade de criar mecanismos processuais *especificamente* destinados a garantir e regular o modo de obtenção da chamada *prova digital*. Quanto ao seu objecto e atento o disposto no artº 1, a presente lei estabelece

disposições penais materiais e processuais, bem como as disposições relativas à Cooperação Internacional em matéria penal, relativas ao domínio do Cibercrime e da recolha de prova em suporte digital.

Relativamente ao âmbito de aplicação das disposições processuais, estabelece no n.º 1 do art.º 11.º que tais disposições se aplicam a processos relativos a crimes:

“a) Previstos na presente lei;

b) Cometidos por meio de sistemas informáticos; ou

c) Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico”.

O art.º 17.º da Lei do Cibercrime, com pertinência no caso dos autos, veio regular a “*Apreensão de correio electrónico e registos de comunicações de natureza semelhante*”, nos termos seguintes:

“Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutra 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 prevista no Código de Processo Penal”(sublinhado nosso).

Este preceito remete para o regime de “*apreensão de correspondência*” que se mostra previsto no art.º 179.º do CPP.

Esta remissão mostra-se realizada em quatro pontos que são:

- A referência à nulidade, em caso de inobservância dos requisitos:

“Sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho, a apreensão (de correspondência) -179.º, n.º 1;

- Quando se trate de correspondência electrónica que foi expedida pelo suspeito ou lhe é dirigida, mesmo que sob nome diverso -179.º,1.a);

- A apreensão de correspondência electrónica entre o arguido e o seu defensor é proibida (179.º, n.º 2);

-O Juiz (que ordenou ou autorizou a diligência) deverá ser o primeiro a tomar conhecimento do conteúdo da correspondência (179, n.º 3).

Considerando o âmbito de aplicação do regime processual, delimitado no art.º 11.º desta Lei especial, somos a entender que a remissão para o regime do Código de Processo Penal não abrange a exigência prevista no n.º 1, al. b) deste preceito, de se tratar de crime previsto com pena superior a três anos.

O legislador criou assim um regime específico de “*Apreensão de correio electrónico e registo de comunicações de natureza semelhante*”, que visou submeter ao regime da *apreensão da correspondência* previsto no artº 179º do CPP.

Em face das referidas disposições legais, consideramos 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, devendo ser o juiz a primeira pessoa a tomar conhecimento do conteúdo da correspondência.

O regime de *apreensão de correio electrónico e registos de comunicação de natureza semelhante* passa assim a ser regulado directamente pelo artº 17º da Lei do Cibercrime e, subsidiariamente (por remessa expressa do mesmo), pelos pressupostos e requisitos legais relativos à apreensão de correspondência, prevista no artigo 179º do CPP.

Somos a concluir que a ingerência na comunicação armazenada em suporte digital, passou a ser regulada a partir de 2009, pelas disposições processuais previstas na lei do Cibercrime, e já não pelo artº 189º, nº 1 do CPP.

\*

Como vimos, o recorrente centra a sua pretensão de ver revogado o despacho judicial que anulou a apreensão de correio electrónico levada a efeito pelo Ministério Público sem autorização judicial, por considerar que o regime do artº 17º da Lei do Cibercrime só se aplica se estiver em causa a “*apreensão de correspondência*”, conceito que exige que se esteja perante um processo comunicacional não concluído, isto é, que a mensagem tenha sido expedida pelo remetente e não tenha ainda entrado no domínio cognitivo do destinatário.

Ou seja, o recorrente entende que o artº 179º do CPP é aplicável à *correspondência* enquanto ela não for aberta pelo destinatário, pelo que, as mensagens de correio electrónico já lidas pelo destinatário não consubstanciam verdadeira correspondência, ficando excluída do âmbito do artº 17º da Lei do Cibercrime.

E estando a correspondência já aberta pelo seu destinatário, a esta correspondência é aplicável o regime geral do artº 178º do CPP.

Sendo esta a linha de argumentação, entende o Ministério Público que a *apreensão* dessas mensagens de correio electrónico estaria tão somente sujeita ao regime de “*Apreensão de dados informáticos*”, situação prevista no artº 16º da Lei do Cibercrime, cabendo ao próprio Ministério Público ordenar ou autorizar a apreensão dos mesmos.

Pois bem,

O artº 16º prevê o regime de “*Apreensão de dados informáticos*”, acabando por ser uma adaptação á realidade digital das tradicionais apreensões, reguladas pelos artigos 177º e sgs. do CPP, sendo a *autoridade judiciária* que tem competência para autorizar ou ordenar a realização da apreensão.

Procura-se nesta pesquisa informática “dados ou documentos informáticos” de um determinado sistema informático que serviram ou foram destinados a servir a prática de um crime.

E, caso, no decurso da *pesquisa informática* ou de outro acesso legítimo a um sistema informático, sejam apreendidos dados ou documentos informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto (nº 3 do artº 16º)

Por sua vez, o artº 17º, sob a epigrafe “Apreensão de correio electrónico e registos de comunicações de natureza semelhante”, estabelece o seguinte: “Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutra 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 de apreensão de correspondência previsto no Código de Processo Penal”.

Importa desde já referir, acrescentando ao já supra referido nesta matéria da *ingerência* nas comunicações em suporte digital, que somos a entender, com o devido respeito por opinião diversa, que não esteve no espírito do legislador transpor para o correio electrónico a distinção, por referência ao correio tradicional, de correio aberto ou fechado.

No artº 17º não vem estabelecida qualquer distinção entre mensagens de correio electrónico e/ou registos de comunicações de natureza semelhante, armazenadas em sistema informático, já acedidas, ou não, pelo respectivo destinatário, sendo que não podia o legislador ignorar a polémica a propósito instalada pela Reforma de 2007 do CPP a que acima demos nota.

Perante esta controvérsia, só se pode entender que o legislador tomou uma posição clara de submeter toda a “*apreensão de correio electrónico e registos*”

*de comunicações de natureza semelhante*” ao regime da apreensão da correspondência, independentemente de as mensagens se encontrarem abertas ou fechadas, fazendo sujeitar a apreensão a autorização judicial, conforme o deixou consignado no artº 17º da Lei do Cibercrime.

Como bem refere David Silva Ramalho, reportando-se ao artº 17º da Lei do Cibercrime “...o legislador tornou clara a sua intenção de submeter toda a *apreensão de correio electrónico e registos de comunicações de natureza semelhante* ao regime da apreensão da correspondência, independentemente de as mensagens se encontrarem lidas ou não lidas. Particularmente expressivo desta opção (...) é o próprio facto de o legislador se referir a *registos de comunicações*, o que indicia que a tutela é conferida mesmo após a comunicação ter terminado e permanecer apenas o ficheiro recebido e aberto”. (Ramalho, David Silva, in *Métodos ocultos de Investigação Criminal em Ambiente Digital*, Coimbra, Almedina, 2017, p. 278).

O elemento literal previsto no artº 17º com a expressão “armazenados” pressupõe também que a comunicação já foi recebida/lida e, consequentemente, armazenada.

Somos também a entender que o legislador não quis admitir qualquer distinção entre correio electrónico fechado ou aberto, por considerar igualmente não existirem razões para considerar diminuídas as exigências garantísticas do correio electrónico quando aberto relativamente ao correio electrónico fechado, atenta a natureza própria destas comunicações.

Neste sentido decidiu o acórdão do TRL de 20.12.2011, referindo que “...não nos parece que haja sido intenção do legislador, atendendo aos princípios e escopo subjacentes, fazer qualquer distinção nos sobreditos preceitos entre “correspondência aberta ou fechada”, mas apenas a salvaguarda jurisdicional, com respeito de direitos fundamentais, v.g. o da reserva da vida privada, de meios de prova através dos quais se acede ou há o perigo de aceder com alto grau de probabilidade a informação de natureza íntima ou com ela conexos” (P. nº 36/11.6PJOER-A.L1.5, disponível em [www.dgsi.pt](http://www.dgsi.pt)).

Também acerca da irrelevância da distinção entre correspondência fechada ou aberta no âmbito das comunicações electrónicas, veja-se o douto Acórdão do STJ de 29.09.2006, P. 06P2321, que acompanhamos, decidindo:

“Quer as mensagens tenham sido lidas ou não pelo destinatário, o que nem sempre se torna de distinção fácil, sobretudo se e quando algum do software de gestão de correio electrónico possibilita marcar como aberta ou não aberta uma mensagem, por vontade do seu destinatário, independentemente de ter sido ou não lida, aquele tem sempre o direito a não ver essa correspondência devassada por alguém, sem a sua autorização, constituindo a leitura dessa

correspondência intromissão absolutamente ilegítima, atentado ao direito à inviolabilidade da mesma, consagrado no artº 34º, nº 4 da CRP” (disponível em [www.dgsi.pt](http://www.dgsi.pt)).

Mais recentemente, o acórdão do TRP de 12.09.2012 decidiu quanto às SMS neste mesmo sentido: “A jurisprudência tem equiparado as mensagens SMS a cartas de correio, distinguindo se ainda estão fechadas ou se foram já abertas pelo destinatário”.

“Porém, a Lei do Cibercrime alterou esta abordagem: a leitura de mensagens guardas em cartão de telemóvel por um agente policial sem autorização do seu dono ou do Juiz de Instrução Criminal é prova proibida (em nada relevando que as mesmas tivessem sido ou não abertas e lidas pelo destinatário, pois que a lei não distingue entre essas duas situações.” (in [www.dgsi.pt](http://www.dgsi.pt)).

Noutra perspectiva, podemos dizer que se o artº 17º da Lei do Cibercrime tivesse o seu âmbito de aplicação circunscrito à apreensão de correio electrónico ainda não conhecido pelo destinatário, ou seja, ao correio electrónico que já entrou no servidor do destinatário mas não foi ainda aberto, então a exigência de tutela jurisdicional para salvaguarda de direitos fundamentais (reserva e intimidade da vida privada) ficaria reduzida ao mínimo, correndo-se o risco de a autorização judicial deixar de ser necessária se, chegados ao local o buscado, momentos antes tivesse aberto a mensagem de correio electrónico, ficando assim sem protecção o grosso da correspondência electrónica.

Acrescendo ainda, na tese defendida pelo recorrente, em relação às comunicações electrónicas sempre haveria que enfrentar o problema de não ser possível, com rigor, determinar quando é que uma mensagem de correio electrónica foi lida ou não, pois como informam os técnicos nesta área, não existem programas informáticos forenses que determinem essa operação, existindo sempre a possibilidade de marcar uma mensagem como não lida, mesmo após ter sido lida. O que nos dá a dimensão de que o correio electrónico e o correio tradicional são realidades tão diversas para poderem seguir lado a lado o mesmo regime.

Por fim, referir que a lei parece não ignorar que cada vez mais os cidadãos guardam nos seus computadores em ambiente laboral documentos escritos, fotografias da família ou gravações sonoras, que são susceptíveis de revelar segredos da vida íntima, a impor um reforço de tutela de protecção relativamente às comunicações electrónicas.

Assim, em face de tudo o que se deixa exposto, diremos, em síntese conclusiva, que a lei do Cibercrime criou em relação à apreensão de “*correio electrónico e registos de comunicações de natureza semelhante*” um regime específico e unitário, que visou submeter ao regime da *apreensão da correspondência*, independentemente de as mensagens se encontrarem abertas ou fechadas.

Deste modo, somos a entender 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, devendo ser o juiz a primeira pessoa a tomar conhecimento do conteúdo da correspondência, conforme remissão expressa para o artº 179º do CPP.

Assim, independentemente de a correspondência ter sido ou não aberta ou ter sido ou não lida, a pessoa a quem é dirigida tem sempre o direito de não ver essa correspondência devassada por terceiros.

No caso dos autos, a apreensão levada a efeito pelo Ministério Público, onde se inclui a apreensão de correio electrónico, não se reconduz, contrariamente ao que vem afirmado, a uma situação de *mera apreensão de dados informáticos* a que se reporta o artº 16º do Cibercrime.

Nunca seria pelo facto de poder haver correio electrónico armazenado ou ainda não lido que se poderia converter uma situação de *apreensão de dados informáticos* nos termos do artº 16º, autorizada pelo Ministério Público, numa situação de *apreensão de comunicações electrónicas*, e pretender que o Juiz de Instrução à *posteriori*, sem ser numa situação de urgência, viesse a autorizar a apreensão do correio electrónico no âmbito do artº 17º da Lei do Cibercrime, sendo que de forma muito clara, como resulta dos autos, mais concretamente do despacho do MºPº de 13.03.2017 (elencado em 2.3.3.), visava-se no âmbito da busca autorizada pelo MP a apreensão de mensagens de correio electrónico e registos de comunicações de natureza semelhante relativos ao suspeito.

Esta seria uma visão desgarrada dos bens e valores em protecção plasmados no artº 34º do CRP.

Conclui-se, assim, que o Ministério Público apreendeu *correio electrónico* com base num despacho que ordenava a realização de buscas no decurso de uma pesquisa informática, sem prévia autorização do juiz de instrução para aquele efeito, sendo por isso nulo o despacho.

4. Da nulidade do despacho do Ministério Público.

A lei, quer o artº 179º, nº 1 do CPP quer o artº 17º da Lei do Cibercrime sancionam com nulidade a violação das regras relativas à competência para a autorização de apreensão de correio electrónico, assim estando ferido de nulidade o despacho do MP, que nos termos do ato 120º, nº 1 do CPP foi tempestivamente invocada.

Nestes termos, tal despacho é nulo e toda a correspondência electrónica assim obtida pelo MP constitui prova proibida, insusceptível de valoração. A apreensão da correspondência electrónica ao arguido, no âmbito das buscas aqui em causa, ao não ter sido precedida da obrigatória autorização judicial, traduziu-se num método proibido de prova, nos termos conjugados do disposto no artº 17º da Lei do Cibercrime e no disposto no artº 179º e 126º, do CPP, e artº 32º, nº 8 da CRP.

Improcede, assim nesta parte o recurso.

#### 5. Quanto à alegada incompetência do juiz de Instrução.

Importa que se diga, como faz o despacho recorrido que “o que está em causa com a pretensão do arguido não é a autonomia do Ministério Público nem, muito menos, a titularidade do Inquérito, mas sim a defesa de direitos, liberdades e garantias dos cidadãos”

Chegados aqui e cientes de que a declaração de nulidade tem sempre carácter materialmente judicial, sendo na fase de inquérito que compete ao Juiz de Instrução a prática de todos os actos que contendem com direitos, liberdades e garantias individuais.

Neste caso, a apreciação da invocada invalidade da apreensão de correspondência electrónica realizada por ordem o MºPº, em violação do artº 17º da Lei do Cibercrime e dos artigos 179º, nº 1 e 269º, nº 1, al, d) do CPP, é, pois, da competência do Juiz de Instrução.

Temos assim por arredada toda a argumentação do Ministério Público no sentido de que o Juiz de Instrução violou, ao conhecer da nulidade em causa, o princípio do acusatório, e que ultrapassou a sua competência quanto à prática dos autos em fase de inquérito (cfr. arts. 268º e 269º, do CPP).

Assim se conclui que a apreciação da questão suscitada é da competência do Juiz de Instrução.

6. Termos em que pela sua correcção, nenhuma censura nos merece a decisão recorrida, improcedendo na totalidade o recurso.

\*

III-Decisão

Termos em que as Juízas da 3ª secção deste Tribunal da Relação de Lisboa acordam em negar provimento ao recurso interposto pelo Ministério Público, mantendo na íntegra a decisão recorrida.

Sem tributação por não ser devida. (cfr. nº 1, al. a) do artº 4º do Regulamento faz Custas processuais.

Notifique.

\*

Lisboa, 07/03/2018.

Elaborado, revisto e assinado pela relatora Conceição Gonçalves e assinado pela Desembargadora Maria Elisa Marques.

[1] Conforme jurisprudência fixada pela Acórdão do Plenário das secções do STJ de 19/10/1995, in D.R., I-A de 28/12/1995, é nas conclusões da motivação que se delimita o objecto do recurso, sem prejuízo, contudo, das questões do conhecimento oficioso, designadamente, a verificação da existência, ou não, dos vícios elencados no nº 2, do artº 410º, do Código de Processo Penal.

[2] (conforme “Definições legais” do artº 1º do CPP “Para efeito do disposto no presente Código considera-se: b) “Autoridade judiciária” o Juiz, o Juiz de Instrução e o Ministério Público, cada um relativamente aos actos processuais que cabem na sua competência).