ACÓRDÃO Nº 687/2021

Processo n.º 830/2021
Plenário
Relatora: Conselheira Mariana Canotilho

I. RELATÓRIO

1. O Presidente da República vem, ao abrigo do artigo 278.º, n.º 1, da Constituição da República Portuguesa, submeter à apreciação deste Tribunal, em processo de fiscalização preventiva da constitucionalidade, as normas constantes do artigo 5.º - "*na parte em que altera o artigo 17º da Lei n.º 109/2009, de 15 de setembro*" - do Decreto n.º 167/XIV, que «*transpõe a Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, alterando o Código Penal, o Código de Processo Penal, a Lei n.º 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime, e outros atos legislativos*», aprovado pela Assembleia da República (doravante, «AR»), em 20 de julho de 2021, publicado no Diário da Assembleia da República, Série II-A, número 177, de 29 de julho de 2021, que lhe foi enviado para promulgação como lei e recebido em 4 de agosto de 2021.

2. Os preceitos ora questionados do Decreto n.º 167/XIV da Assembleia da República têm o seguinte teor:

> «Artigo 5.º
>
> Alteração à Lei n.º 109/2009, de 15 de setembro
>
> Os artigos 3.º, 6.º, 17.º, 19.º, 20.º, 21.º, 25.º e 30.º da Lei n.º 109/2009, de 15 de setembro, passam a ter a seguinte redação:
>
> (...)
>
> Artigo 17.º
>
> Apreensão de mensagens de correio eletrónico ou de natureza semelhante
>
> 1 – Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontradas, armazenadas nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou de natureza semelhante que sejam necessárias à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a sua apreensão.
>
> 2 – O órgão de polícia criminal pode efetuar as apreensões referidas no número anterior, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 15.º, bem como quando haja urgência ou perigo na demora, devendo tal apreensão ser validada pela autoridade judiciária no prazo máximo de 72 horas.
>
> 3 – À apreensão de mensagens de correio eletrónico e de natureza semelhante aplica-se o disposto nos n.os 5 a 8 do artigo anterior.
>
> 4 – O Ministério Público apresenta ao juiz, sob pena de nulidade, as mensagens de correio eletrónico ou de natureza semelhante cuja apreensão tiver ordenado ou validado e que considere serem de grande interesse

para a descoberta da verdade ou para a prova, ponderando o juiz a sua junção aos autos tendo em conta os interesses do caso concreto.

5 – Os suportes técnicos que contenham as mensagens apreendidas cuja junção não tenha sido determinada pelo juiz são guardados em envelope lacrado, à ordem do tribunal, e destruídos após o trânsito em julgado da decisão que puser termo ao processo.

6 – No que não se encontrar previsto nos números anteriores, é aplicável, com as necessárias adaptações, o regime da apreensão de correspondência previsto no Código de Processo Penal».

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

3. Os fundamentos apresentados no pedido para sustentar a inconstitucionalidade dos preceitos impugnados são os seguintes:

«[…]

1º

Pelo Decreto nº 167/XIV, a Assembleia da República aprovou a lei relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, alterando o Código Penal, o Código de Processo Penal, a Lei n.º 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime, e outros atos legislativos.

2º

O Decreto em causa procede à transposição de Diretiva europeia. Contudo, e como se admite na exposição de motivos da própria proposta de lei, o legislador aproveitou a oportunidade para alterar normas não diretamente visadas pela Diretiva.

3º

É o caso da alteração ao artigo 17º da Lei do Cibercrime. Com efeito, como referido na exposição de motivos: "Noutro plano, e ainda que se trate de um aspeto não respeitante à transposição da Diretiva (UE) 2019/713, aproveita-se o ensejo para ajustar o artigo 17.º da Lei do Cibercrime, cujo teor tem gerado conflitos jurisprudenciais que prejudicam a economia processual e geram dúvidas desnecessárias.

Este ajustamento tem como propósito clarificar o modelo de apreensão de correio eletrónico e da respetiva validação judicial.

Visa-se, por um lado, esclarecer que a apreensão de mensagens de correio eletrónico ou de natureza similar está sujeita a um regime autónomo, que vigora em paralelo com o regime da apreensão de correspondência previsto no Código de Processo Penal. Este último regime apenas se aplica à apreensão de mensagens de correio eletrónico ou de natureza similar a título subsidiário, e com as necessárias adaptações.

Visa-se, por outro lado, esclarecer que a apreensão de mensagens de correio eletrónico ou de natureza similar guardadas num determinado dispositivo, embora incidindo sobre dados informáticos de conteúdo especial, não é tecnicamente diferente da apreensão de outro tipo de dados informáticos. Assim, deve o Ministério Público, após análise do respetivo conteúdo, apresentar ao juiz as mensagens de correio eletrónico ou de natureza similar cuja apreensão tiver ordenado ou validado e que considere serem de grande interesse para a descoberta da verdade ou para a prova, ponderando o juiz a sua junção aos autos tendo em conta os interesses do caso concreto.

Esta solução procura replicar, no domínio das mensagens de correio eletrónico ou de natureza similar, a solução presentemente aplicável aos dados e documentos informáticos cujo conteúdo possa revelar dados pessoais ou íntimos, pondo em causa a privacidade do respetivo titular ou de terceiro, nos termos do n.º 3 do artigo 16.º da Lei do Cibercrime".

4º

É o seguinte o conteúdo da alteração em causa:

"Artigo 17.º

Apreensão de mensagens de correio eletrónico ou de natureza semelhante

1 – Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontradas, armazenadas nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou de natureza semelhante que sejam necessárias à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a sua apreensão.

2 – O órgão de polícia criminal pode efetuar as apreensões referidas no número anterior, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 15.º, bem como quando haja urgência ou perigo na demora, devendo tal apreensão ser validada pela autoridade judiciária no prazo máximo de 72 horas.

3 – À apreensão de mensagens de correio eletrónico e de natureza semelhante aplica-se o disposto nos n.ºs 5 a 8 do artigo anterior.

4 – O Ministério Público apresenta ao juiz, sob pena de nulidade, as mensagens de correio eletrónico ou de natureza semelhante cuja apreensão tiver ordenado ou validado e que considere serem de grande interesse para a descoberta da verdade ou para a prova, ponderando o juiz a sua junção aos autos tendo em conta os interesses do caso concreto.

5 – Os suportes técnicos que contenham as mensagens apreendidas cuja junção não tenha sido determinada pelo juiz são guardados em envelope lacrado, à ordem do tribunal, e destruídos após o trânsito em julgado da decisão que puser termo ao processo.

6 – No que não se encontrar previsto nos números anteriores, é aplicável, com as necessárias adaptações, o regime da apreensão de correspondência previsto no Código de Processo Penal".

5º

Deste modo, como se vê, a alteração em causa não constitui um mero "ajustamento", mas a uma mudança substancial no paradigma de acesso ao conteúdo das comunicações eletrónicas, admitindo-se que esse acesso caiba, em primeira linha, ao Ministério Público, que só posteriormente o apresenta ao juiz.

6º

O Tribunal Constitucional tem dedicado atenção recente, numa leitura estrita, ao acesso por parte de entidades públicas às comunicações, sejam no seu conteúdo, sejam os metadados (vd. Acórdão TC n.º 464/2019).

7º

Por outro lado, como bem alerta a Comissão Nacional de Proteção de Dados no seu parecer (Parecer 2021/74), jurisprudência recente do Tribunal de Justiça da União Europeia, em caso semelhante, entendeu que o Ministério Público, por deter a ação penal, não possui a independência requerida para apreciar a necessidade de acesso ao conteúdo das comunicações, razão pela qual essa tarefa deve ser cometida ao juiz.

8º

O regime aprovado parece divergir, por outro lado, do disposto no artigo 179º do Código do Processo Penal, no qual a intervenção do juiz ab initio é indispensável. Esta é também a opinião expressa pela Comissão Nacional de Proteção de Dados no seu parecer.

9º

Com efeito, é o seguinte o conteúdo do artigo 179º do Código do Processo Penal:

"Artigo 179.º

Apreensão de correspondência

1 - Sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho, a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência, quando tiver fundadas razões para crer que:

a) A correspondência foi expedida pelo suspeito ou lhe é dirigida, mesmo que sob nome diverso ou através de pessoa diversa;

b) Está em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos; e

c) A diligência se revelará de grande interesse para a descoberta da verdade ou para a prova.

2 - É proibida, sob pena de nulidade, a apreensão e qualquer outra forma de controlo da correspondência entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que aquela constitui objeto ou elemento de um crime.

3 - O juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida. Se a considerar relevante para a prova, fá-la juntar ao processo; caso contrário, restitui-a a quem de direito, não podendo ela ser utilizada como meio de prova, e fica ligado por dever de segredo relativamente àquilo de que tiver tomado conhecimento e não tiver interesse para a prova.

10º

Torna-se, pois, claro que o regime agora aprovado se parece afastar, substancialmente, do disposto no Código de Processo Penal em matéria de correspondência, onde é sempre exigida a intervenção do juiz.

11º

O legislador justificou, em parte, na exposição de motivos, a necessidade da presente alteração com a resolução "conflitos jurisprudenciais". Se é certo que a jurisprudência nem sempre tem sido linear na aplicação desta norma (vd., entre outros, Ac. do Tribunal da Relação de Guimarães de 29-03-2011), também é verdade que alguma jurisprudência parece apelidar a confusão de "aparente" (vd. Ac. do Tribunal da Relação de Lisboa de 06-02-2018). Seja como for, seria importante assegurar que a tais alegados "conflitos jurisprudenciais" não fosse agora acrescentada a dúvida de eventual não conformidade constitucional do regime aprovado.

12º

Por outro lado, a nova redação dada ao artigo 17º aproxima-se, é certo, do regime em vigor no artigo 16º. Sucede que, como alerta a Comissão Nacional de Proteção de Dados, o artigo 16º refere-se a dados informáticos, o que – de modo diverso do que parece resultar da exposição de motivos -não inclui necessariamente dados pessoais nem o conteúdo das comunicações, razão que justifica um regime menos exigente.

13º

Não por acaso, o legislador tratou em artigos diversos da apreensão de dados informáticos e da apreensão de correio eletrónico e registos de comunicações de natureza semelhante, justamente por esta última dever justificar um regime mais rigoroso de acesso.

14º

Ora, a admitir-se esta interpretação, o regime em causa seria assim suscetível de introduzir novas restrições ao disposto no artigo 34º, em especial no seu número 4, e no artigo 35º, todos da Constituição. Tais restrições, nesse caso, poderiam não respeitar os termos estritos do citado n.º 4 do artigo 34º, na interpretação que lhe tem sido dada pelo Tribunal Constitucional, o disposto no artigo 35º, nem a exigência de proporcionalidade resultante do regime material dos direitos, liberdades e garantias, constante do n.º 2 do artigo 18º da Constituição.

Ante o exposto, perante as dúvidas suscitadas, parece oportuno clarificar, antecipadamente, a potencial não conformidade constitucional deste novo regime, e a compreensível preocupação que pode suscitar em termos de investigação criminal.

[…]»

Com tais fundamentos, o Presidente da República requer ao Tribunal Constitucional a apreciação preventiva da constitucionalidade das normas do artigo 5.º do Decreto n.º 167/XIV, na parte em que altera o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, em virtude de o considerar potencialmente desconforme com a Constituição, por violação do direito à inviolabilidade do domicílio e da correspondência, na interpretação que lhe tem sido dada pelo Tribunal Constitucional, e do direito à utilização da informática, nos termos expostos.

-

4. Notificado para o efeito previsto no artigo 54.º da Lei de Organização, Funcionamento e Processo do Tribunal Constitucional (doravante, «LTC»), o Presidente da Assembleia da República ofereceu o merecimento dos autos, enviando em anexo uma nota sobre os trabalhos preparatórios, elaborada pelos Serviços de Apoio à Comissão Parlamentar de Assuntos Constitucionais, Direitos, Liberdades e Garantias e informando que os trabalhos preparatórios que conduziram à aprovação do Decreto em questão se encontram disponíveis na página de Internet do Parlamento.

O Presidente da Assembleia da República juntou ainda aos autos uma pronúncia da direção do Grupo Parlamentar do Partido Socialista, que apresenta argumentos no sentido da conformidade constitucional das normas questionadas. Os fundamentos para tal posição são, em síntese, os seguintes:

«A pronúncia do Grupo Parlamentar do Partido Socialista sobre o requerimento feito pelo Exmo. Senhor Presidente da República visando a apreciação da conformidade com a Constituição da norma constante do artigo 5.° do Decreto n.° 167/XIV da Assembleia da República, na parte em que altera o artigo 17.° da Lei n.° 109/2009, de 15 de setembro, evidencia, resumidamente, o seguinte:

i) *O artigo 17.º é uma norma processual penal inserida num regime jurídico relativo ao cibercrime e orientado para a investigação de crimes revestidos de especial ofensividade, pelo que a apreensão de correio eletrónico permitida é apenas aquela necessária à produção de prova desses crimes no âmbito de um processo penal já instaurado —não se trata, assim, de permitir o "acesso livre" pelo ministério público ao correio eletrónico pessoal dos cidadãos.*

ii) *A solução constante do artigo 17.º não viola o princípio da reserva de juiz no acesso a correspondência informática porquanto (i) o artigo 17.º não é a norma-regra sobre acesso a mensagens de correio eletrónico — tal acesso continuará, em regra, a carecer de prévia decisão judicial, nos termos do artigo 179.º do Código de Processo Penal para o qual o n.º 6 do artigo 17.º remete; (ii) o artigo 17.º limita-se a criar uma solução excecional para hipóteses em que as mensagens de correio eletrónico sejam conhecidas no âmbito de uma outra pesquisa informática validamente determinada e que já está a ocorrer; (iii) as hipóteses previstas no artigo 17.º pressupõem sempre um controlo judicial orientado para a avaliação da legalidade, necessidade e proporcionalidade das apreensões realizadas, não se tratando, por isso, nunca de uma "solução sem juiz"; (iv) o sigilo da correspondência que é objeto da proteção reforçada do artigo 34.º da Constituição refere-se à comunicação "fechada" e à interceptação de fluxos comunicacionais que estão a acontecer, não abrangendo a chamada comunicação "já aberta" associada ao armazenamento de dados resultantes de comunicações prévias; (v) numa estrutura de máxima acusatoriedade como é a portuguesa, reconhece-se ao ministério público o estatuto de autoridade judiciária regida por critérios de legalidade e objetividade e atribui-se-lhe o papel de titular da ação penal que faz dele o "dominus" do inquérito, não podendo tal atribuição ser esvaziada pela outorga ao juiz das opções sobre a investigação, ainda que as decisões que mais gravosamente limitem direitos fundamentais devam ser sujeitas ao controlo do juiz de instrução.*

iii) *O parecer da CNPD e o Acórdão do TJUE invocados como fundantes das dúvidas sobre a conformidade constitucional referem-se sobretudo ao acesso sem prévia autorização judicial a dados de tráfego (não se referem,*

portanto, como sucede no artigo 17.º, a dados de conteúdo de correspondência que não está em trânsito, isto é, que já foi recebida pelo destinatário)».

Elaborado o memorando a que alude o artigo 58.º, n.º 2, da LTC, e fixada a orientação do Tribunal, importa decidir conforme dispõe o artigo 59.º da mesma Lei.

II – FUNDAMENTAÇÃO

A) Conhecimento do pedido

5. Considerando a legitimidade do requerente, a circunstância de o pedido conter todas as indicações a que se refere o artigo 51.º, n.º 1, da LTC e a observância dos prazos aplicáveis (artigo 278.º, n.º 3, da Constituição e artigos 54.º, 56.º, n.º 4, 57.º, n.ºs 1 e 2, e 58.º da LTC), nada obsta ao conhecimento da questão de constitucionalidade formulada nos presentes autos.

B) Normas a apreciar e respetivo enquadramento

6. A análise da questão de constitucionalidade agora colocada ao Tribunal Constitucional exige a consideração do quadro sistémico traçado pela *Lei do Cibercrime* – cujo artigo 17.º é significativamente alterado pelos preceitos legais questionados –, bem como pelo acervo normativo resultante da interconexão entre tal lei, o Código de Processo Penal (CPP) e as normas relevantes – paramétricas e de direito ordinário –, vigentes no espaço europeu.

A Lei n.º 109/2009, de 15 de setembro, denominada *Lei do Cibercrime*, que o Decreto em que se insere a norma questionada vem alterar, transpôs para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adaptou o direito interno à Convenção sobre Cibercrime do Conselho da Europa, adotada em Budapeste em 23 de novembro de 2001 (aprovada pela Resolução da Assembleia da República n.º 88/2009, de 10 de julho de 2009 e ratificada pelo Decreto n.º 91/2009, de 15 de setembro). Ao mesmo tempo, revogou a anterior legislação sobre a matéria, nomeadamente, a Lei n.º 109/1991, de 17 de agosto, denominada *Lei da Criminalidade Informática*.

A Lei n.º 109/2009 foi inovadora, na medida em que instituiu, pela primeira vez, regras jurídicas específicas referentes à recolha de prova em suporte eletrónico. Até então, a investigação dos crimes relacionados com a informática fazia-se com recurso às normas pertinentes, interpretadas com as necessárias adaptações, do Código de Processo Penal. Com a aprovação desta lei, o legislador procurou reunir num único diploma todas as normas respeitantes à *criminalidade informática*: normas de direito substantivo, normas de direito processual e normas relativas à cooperação judiciária em matéria penal.

Assim, do ponto de vista estrutural, a *Lei do Cibercrime* contém disposições introdutórias e definições legais, bem como um capítulo dedicado a *normas penais de natureza material*, onde são consagrados diversos tipos penais especificamente relacionados com a criminalidade informática; além disso, a Lei n.º 109/2009 estabelece, em capítulo autónomo, e como já se mencionou, um conjunto de *normas de natureza adjetiva* (designadas como "disposições processuais"), consagrando uma série de novos *meios de obtenção de prova*. Finalmente, um capítulo sobre cooperação internacional contém normas que complementam as disposições da Lei da Cooperação Judiciária em Matéria Penal.

7. Nos termos do artigo 11.º da *Lei do Cibercrime* – a primeira disposição normativa constante do Capítulo III – as disposições processuais dela constantes apresentam-se como de aplicação tendencialmente privativa aos crimes nela consagrados. Todavia, como resulta do disposto nas diversas alíneas do n.º 1 do artigo 11.º de tal diploma, designadamente na sua alínea *c)*, e como decorre do artigo 14.º, n.º 2, alínea c), da Convenção de Budapeste sobre o Cibercrime, aquelas disposições são, na realidade, aplicáveis a *todo e qualquer crime*, desde que se mostre necessária a *recolha de prova em suporte eletrónico*. Assim, "*as regras de direito probatório previstas no diploma não são assim meras normas processuais sobre* cibercrimes *ou sequer apenas relativas a crimes praticados em* sistemas informáticos*, mas correspondem a um regime consideravelmente mais abrangente sobre* prova eletrónica *em processo penal aplicável a qualquer crime*" (P. DÁ MESQUITA, "Prolegómeno sobre prova electrónica e intercepção de telecomunicações no direito processual penal português - o Código e a Lei do Cibercrime", in *Processo Penal, Prova e Sistema Judiciário*, Wolters Kluwer Portugal/Coimbra Editora, 1.ª edição, 2010, p. 98). Por esta razão, uma argumentação nos termos da qual as normas processuais penais constantes da *Lei do Cibercrime* teriam a natureza de normas excecionais, *orientadas para a investigação de crimes revestidos de especial ofensividade* não pode proceder. Ou, pelo menos, não pode ter-se por inequívoca a veracidade de tal argumentação, havendo espaço para interpretações diferentes, que permitam a extensão da aplicação do regime previsto no artigo 17.º a outros crimes, desde que se tenha por indispensável a recolha de prova em suporte eletrónico.

Efetivamente, o legislador nacional escolheu, ao aprovar a *Lei do Cibercrime*, consagrar normas de direito probatório de espetro geral num diploma extravagante, ao invés de rever e adaptar o CPP aos novos tempos. Se isto era assim em 2009, é particularmente premente nos dias de hoje, e a norma em análise prossegue esse caminho.

Ora, desta forma, tendo em consideração os processos de digitalização e desmaterialização que dominam a sociedade contemporânea, o âmbito de aplicação efetivo das normas adjetivas da Lei n.º 109/2009 revela-se substancialmente mais amplo do que poderia parecer numa primeira análise, como adiante se explicitará. De facto, a *prova em suporte eletrónico* tenderá a ser uma realidade material omnipresente na vida comunitária, mais ainda do que já sucedia aquando da aprovação da versão inicial das normas questionadas; notem-se, entre muitos outros fatores de incremento da *vida digital,* o aumento das interações entre Estado e cidadãos com recurso à *Internet*, bem como o crescimento do teletrabalho, em particular no cenário pandémico – e estes exemplos constituem apenas duas das mais recentes manifestações da extensão a novos domínios da vida em sociedade das referidas digitalização e desmaterialização. Na presente análise, dever-se-á, pois, ter em atenção que os preceitos questionados são passíveis de aplicação à investigação de *qualquer crime*, e não apenas aos crimes diretamente relacionados com a utilização da informática.

8. Ainda no Capítulo III da Lei n.º 109/2009, e no que particularmente releva para a presente análise, encontramos os artigos 15.º a 17.º, que visam regular a matéria relativa à *pesquisa* (artigo 15.º) e subsequente *apreensão* (artigo 16.º) de dados ou documentos informáticos, *previamente armazenados num sistema informático*, estabelecendo-se um *regime especial*, no artigo 17.º, agora em causa, para a *apreensão de correio eletrónico e registos de comunicações de natureza semelhante*.

Assim, o artigo 15.º da *Lei do Cibercrime* regula a *pesquisa* de *sistemas informáticos*, com vista a obter *dados informáticos específicos e determinados* nele armazenados; ou seja, as normas contidas em tal artigo estabelecem as regras do que pode designar-se por "busca informática". Por regra, é a autoridade judiciária competente — o juiz ou o Ministério Público, consoante a fase processual em questão — que autoriza ou ordena a realização da pesquisa, devendo, sempre que possível, presidir à diligência (artigo 15.º, n.º 1). No âmbito de tais pesquisas, é possível, nos termos do artigo 16.º da Lei n.º 109/2009, a *apreensão* de dados, ordenada por despacho da mesma autoridade judiciária, sempre que tal seja necessário à produção de prova. Contudo, a lei individualiza duas situações específicas, cuja sensibilidade e relevância jurídico-constitucional justifica a previsão de um regime normativo particular

– por um lado, as apreensões de um conjunto de *dados sensíveis*; por outro, as apreensões de *mensagens de correio eletrónico ou semelhantes*. A apreensão de dados de especial sensibilidade encontra-se regulada no n.º 3 do artigo 16.º da *Lei do Cibercrime*, que prevê que, nas situações em que 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*, os mesmos devem ser, sob pena de nulidade, apresentados ao juiz, que ponderará a sua junção aos autos, tendo em conta os interesses do caso concreto. Além disto, a lei estabelece ainda a aplicabilidade, com as adaptações necessárias, das regras específicas previstas no Código de Processo Penal e demais legislação para as apreensões de dados em sistemas informáticos utilizados para o exercício da advocacia e das atividades médica, bancária e de jornalismo, bem como do regime de segredo profissional ou de funcionário e de segredo de Estado.

Quanto ao regime especial consagrado para a apreensão de correio eletrónico ou similar, constante da versão em vigor do artigo 17.º da *Lei do Cibercrime*, e que constitui o objeto do presente processo, será analisado *infra*. Adiante-se, desde já, que se exige a intervenção obrigatória do juiz que, nos termos da norma referida, pode autorizar ou ordenar, por despacho, a apreensão quando tal se afigure ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se o regime da apreensão de correspondência previsto no Código de Processo Penal.

9. A *Lei do Cibercrime* suscitou dificuldades interpretativas várias e foi objeto de crítica e divergência, no plano da doutrina. Questiona-se, desde logo, a regulação desta matéria em legislação avulsa (não apenas a Lei n.º 109/2009, em si mesma, mas também a Lei n.º 32/2008, de 17 de julho, que transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações), cuja interpretação integrada com as disposições do Código de Processo Penal se revela, amiúde, problemática: "*persistindo numa estranha lógica legislativa, que tem resistido incólume ao irremediável volver dos tempos, o legislador nacional continua a manter em vigor três diplomas legais diferentes para regular aspetos parcelares da mesma realidade concreta. Esta trilogia, para além de acentuar o atual paradigma da descodificação e de negar a desejável centralidade normativa do Código de Processo Penal, contribui para a assimetria, para a incoerência das soluções legais e, sobretudo, para o seu indesejável e nefasto insucesso prático. A prova digital – essencial no mundo hodierno – continua mergulhada num verdadeiro pântano prático e, sobretudo, normativo, que só poderá ser superado mediante uma intervenção legislativa coerente, global e, cientificamente, sustentável*" (J. CONDE CORREIA, "Prova Digital: as leis que temos e a lei que devíamos ter", in *Revista do Ministério Público*, n.º 139, Julho-Setembro de 2014, p. 30-31).

10. No que especificamente se relaciona com o regime jurídico de *apreensão do correio eletrónico*, ou semelhante, plasmado no artigo 17.º, também se acumulam dúvidas e posições divergentes.

Em primeiro lugar, discute-se se o paralelismo legalmente estabelecido com o regime processual penal que regula a apreensão de correspondência deve aplicar-se a *todo* o correio eletrónico, ou apenas às situações em que este não foi ainda lido pelo destinatário, aplicando-se ao correio lido o regime da simples apreensão de documentos. Até à aprovação da lei, posições havia, até, que afastavam qualquer equivalência entre as mensagens de correio eletrónico recebidas num sistema informático e o *conceito tradicional de correspondência ou de carta* (veja-se, neste sentido, R. BRAVO, "Da não equiparação do conceito de correio-electrónico ao conceito tradicional de correspondência por carta", in *Revista Polícia e Justiça*, III Série, N.º 7, janeiro-junho de 2006, Coimbra Editora).

A *Lei do Cibercrime* veio clarificar a existência de tal paralelismo, sem que, porém, se afastassem todas as dúvidas respeitantes à interseção entre os regimes processuais respeitantes à intercetação de telecomunicações, à apreensão de correspondência e à apreensão de documentos. Assim, questiona-se, nomeadamente, se, a partir do momento da leitura, a mensagem de correio eletrónico, ou similar, não

passa a ser um documento eletrónico como qualquer outro, estabelecendo-se como objeto idóneo de 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. Vários autores, especialmente em escritos mais antigos, inclinam-se no sentido desta última solução.

Nestes termos, no sentido da equiparação entre correio eletrónico lido pelo destinatário e simples documentos, afirma-se que "*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. E, como tal, sujeito ao mesmo regime em que se encontra um qualquer ficheiro produzido pelo utilizador do computador e nele arquivado. Podendo, como tal, figurar como objeto idóneo da busca, em sentido tradicional*" (M. COSTA ANDRADE, "Comentário ao artigo 194.º do Código Penal", in *Comentário Conimbricense do Código Penal*, Tomo I, 2.ª Edição, Coimbra Editora, maio de 2012, ponto 27). Posição idêntica explica que "*no art. 17.º, apesar da redação pouco clara, a remissão para as regras do processo penal sobre apreensão de correspondência parece implicar que a mesma reconduz o intérprete à teleologia do regime processual sobre a apreensão de correspondência, pelo que não são objeto da sua tutela especial, nomeadamente, mensagens de correio eletrónico já acedidas pelo destinatário*" (P. DÁ MESQUITA, "Prolegómeno sobre prova electrónica e intercepção de telecomunicações no direito processual penal português - o Código e a Lei do Cibercrime", in *Processo Penal, Prova e Sistema Judiciário*, Wolters Kluwer Portugal/Coimbra Editora, 1.ª edição, 2010, p. 118)

Todavia, esta posição não é consensual; há quem defenda uma maior garantia mesmo do correio eletrónico já lido, entendendo que "*a Lei do Cibercrime consagra uma distinção de regime para o e-mail armazenado, que nem equipara à proteção da interceção do e-mail enquanto comunicação, nem à (falta de) proteção dos normais escritos. De facto, reconhece esta lei um* plus *de proteção a arquivos que já foram comunicação, em nome da salvaguarda da privacidade da autodeterminação informacional, remetendo para o regime de correspondência.* (...) *O que a Lei n.º 109/2009 faz é reconhecer ao correio eletrónico apenas dois momentos, com separação entre um e outro desde a leitura do e-mail pelo destinatário, mas conferindo, ao mesmo tempo, proteção acrescida ao segundo momento, de armazenamento, fazendo coincidir os requisitos previstos para o regime da correspondência*" (ANA RITA CASTANHEIRA NEVES, *As ingerências nas comunicações electrónicas em protecção penal: natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra Editora, 2011, p. 276-277).

Nesta linha, alguma doutrina tem evoluído para uma posição que desconsidera a distinção entre correio eletrónico lido e não lido pelo destinatário, com suporte na letra do artigo 17.º da *Lei do Cibercrime,* que não contém qualquer divisão concetual ou de âmbito de aplicação; justifica-se esta orientação, desde logo, com as dificuldades técnicas e a possibilidade de equívocos que tal diferenciação comporta. A consagração de um regime jurídico único, especificamente desenhado para a figura do correio eletrónico, permite, aliás, ultrapassar incongruências e antinomias que resultariam de um tratamento jurídico diferenciado entre as mensagens guardadas no sistema informático do visado e as mensagens armazenadas em nuvem, ou no sistema informático do prestador do serviço. Assim, tem-se caminhado em direção a uma disciplina tendencialmente unitária da apreensão de correio eletrónico em processo penal, permitindo enfrentar as questões levantadas por tal realidade, levando em consideração os bens jurídico-constitucionalmente tutelados que a propósito dela devem ser convocados (como a privacidade, o sigilo da correspondência, a autodeterminação informativa, a proteção conferida aos dados pessoais e aos dados informáticos), e contribuindo para ultrapassar os desencontros provocados pelo "*enquadramento categorial e normativo* dos e-mails *nas fases e ao tempo em que se encontram guardados no* e-mail account *do* provider*: tanto na fase intermédia, em que a mensagem não foi ainda chamada nem aberta ou lida pelo destinatário; como na fase final, nas constelações em que, depois de aberto e lido, o e-*mail *é depositado no* server *do* provider*, a que só é possível aceder através da* internet*, isto é, através de um ato de telecomunicação*" (M. COSTA ANDRADE, "Comentário ao artigo 194.º do Código Penal", in *Comentário Conimbricense do Código Penal*, Tomo I, 2.ª Edição, Coimbra Editora, maio de 2012, ponto 28). Efetivamente, a verdade é que é, hoje, possível "*com um simples clique, marcar como lida uma mensagem de correio eletrónico não lida e vice-versa. O sujeito pode aceder ao correio eletrónico através de vários dispositivos e em uns deles a mensagem surgir como lida e noutros como não lida, dependendo do tipo de sincronização existente entre os diversos dispositivos. A fronteira entre correio eletrónico*

lido e não lido é, assim, difícil de estabelecer. O legislador, reconhecendo o anacronismo e a inadequação daquela distinção de regimes, optou por atribuir uma tutela acrescida à mensagem em formato digital, submetendo-a ao regime do artigo 17.º, independentemente de ter ou não sido lida pelo seu destinatário (SÓNIA FIDALGO, "A apreensão de correio electrónico e a utilização noutro processo das mensagens apreendidas", in *Revista Portuguesa de Ciência Criminal*, Ano 29, n.º 1, janeiro-abril de 2019, Gestlegal, p. 69).

Por esta razão, e atendendo igualmente aos bens jurídico-constitucionais e aos direitos fundamentais em causa, bem como à necessidade de uma compreensão atualista da tutela jusconstitucional conferida pela CRP nesta matéria, atender-se-á ao regime jurídico de apreensão de correio eletrónico sem proceder a este tipo de distinções.

11. Por outro lado, e com evidente interesse para a questão de constitucionalidade que se analisará no presente processo, questiona-se também, no que respeita à aplicação do disposto no artigo 17.º da *Lei do Cibercrime*, a obrigatoriedade de despacho judicial prévio, que autorize ou ordene a apreensão de mensagens de correio eletrónico, bem como a necessidade de o juiz ser o primeiro a tomar conhecimento do conteúdo das mensagens de correio eletrónico ou semelhantes apreendidas. Quanto a estes pontos, as divergências são significativas, no plano doutrinal.

Para alguns autores, a apreensão só pode ser feita na sequência de despacho judicial prévio: "*A lei exige claramente um despacho judicial prévio a qualquer apreensão. Poderá questionar-se as dificuldades que tal exigência levanta na prática, mas não poderá dizer-se que a lei não faz esta exigência*" (cfr. SÓNIA FIDALGO, "A apreensão de correio electrónico e a utilização noutro processo das mensagens apreendidas", in *Revista Portuguesa de Ciência Criminal*, Ano 29, n.º 1, janeiro-abril de 2019, Gestlegal, p. 67 e ainda, no mesmo sentido, ANA RITA CASTANHEIRA NEVES, *As ingerências nas comunicações electrónicas em protecção penal: natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra Editora, 2011, p. 275).

Outros, porém, entendem que a lei é omissa a este propósito e permite interpretações possibilitadoras de uma apreensão cautelar ou provisória das mensagens de correio eletrónico, sem despacho judicial *prévio*, desde que haja, depois, despacho judicial que ordene a junção aos autos das mensagens apreendidas. Ou seja, nesses casos, "*o despacho judicial deverá ser ulterior à chegada das mensagens ao conhecimento de quem está a conduzir a investigação. Por idênticas razões, terá que entender-se que a única exigência legal para a sua apreensão provisória é a da existência de uma forma legítima de acesso ao meio informático em que estavam armazenadas. Esta apreensão é provisória porque caso o juiz entenda dever autorizar a apreensão, a mensagem em causa será efetivamente apreendida e junta ao processo. Caso assim não entenda, então a apreensão não se mantém, devendo o suporte das mensagens em causa ser devolvido ou, se a apreensão tiver sido feita por cópia, destruído. Este regime vai ao encontro das exigências práticas dos casos concretos, permitindo flexibilizar o procedimento a este propósito*" (P. VERDELHO, "A nova Lei do Cibercrime", in *Scientia Iuridica*, Tomo LVIII, n.º 320, outubro-dezembro de 2009, Universidade do Minho, p. 743).

A divergência estende-se, como acima se explicou, à questão de saber se o juiz tem que tomar, forçosamente, conhecimento do conteúdo das mensagens em primeiro lugar. Nos termos de uma das posições doutrinais em confronto, "*a letra da lei aponta antes para a possibilidade de quem procede à pesquisa encaminha para o juiz mensagens concretas, com relevância para o caso concreto, que aquele depois apreenderá ou não*". Chama-se ainda a atenção para o facto de este regime não divergir *"estruturalmente daquele que se prevê no Código de Processo Penal para a apreensão de correspondência*" (neste sentido, de novo, cfr. P. VERDELHO, "A nova Lei do Cibercrime", in *Scientia Iuridica*, Tomo LVIII, n.º 320, outubro-dezembro de 2009, Universidade do Minho, p. 744 e 745), e para a incoerência em sede do sistema de tutela de direitos fundamentais no âmbito processual penal que resultaria de solução contrária, na medida em que "*nos casos mais graves para a privacidade dos artigos 16.º, n.º 3, e 18.º, os OPC's e o Ministério Público podem e devem tomar primeiro conhecimento do conteúdo*" (assim, R. CARDOSO, "Apreensão de correio electrónico e registos de

comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX", in *Revista do Ministério Público,* janeiro-março de 2018, p. 197-199). Em sentido oposto, pode defender-se que, numa interpretação mais próxima da letra do artigo 17.º da *Lei do Cibercrime*, e uma vez que se aplica o regime de apreensão da correspondência, previsto no artigo 179.º do Código de Processo Penal, "*quando se apreende correio eletrónico ou de registos de comunicações de natureza semelhante, aplicando-se obrigatoriamente* mutatis mutandis *o regime da apreensão de correspondência, o juiz é o primeiro a tomar conhecimento do seu conteúdo*" (cfr. A. DIAS RAMOS, *A prova digital em processo penal: o correio eletrónico*, 2.ª Edição, Chiado Editora, 2017). A análise da questão de constitucionalidade ora em causa atenderá a estas divergências em dois planos; em primeiro lugar, tendo presente que a nova redação do regime jurídico constante do artigo 17.º da *Lei do Cibercrime* visa, entre outras finalidades, superar estas interpretações dissonantes. Em segundo lugar, refletindo sobre se - tendo em consideração as normas constitucionais relevantes, em especial as relativas às garantias processuais em sede de processo penal - a superação, por via legislativa, das dissonâncias interpretativas relatadas pode fazer-se escolhendo qualquer um dos caminhos doutrinalmente propostos, ou se a Constituição impõe um determinado rumo.

12. O Decreto n.º 167/XIV promove um conjunto vasto de alterações em diversos diplomas – entre os quais se destaca o Código Penal, o Código Processo Penal e a Lei n.º 109/2009 – procurando adaptar a ordem interna às recentes imposições do Direito da União Europeia em matéria penal. Com efeito, apesar de a Exposição de Motivos da Proposta de Lei n.º 98/XIV/2.ª reconhecer que "*ordem jurídica interna est[á], genericamente, conforme à Diretiva (EU) 2019/713*", o legislador identificou "*algumas lacunas de punibilidade, que se propõe colmatar*". As alterações agora introduzidas na mencionada Lei n.º 109/2009 justificam-se, pois, antes de mais, pela necessidade de proceder a ajustes e adaptações, para conformar plenamente a ordem jurídica portuguesa com os preceitos da Diretiva (UE) 2019/713, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, que substitui a Decisão-Quadro 2001/413/JAI do Conselho (Diretiva (UE) 2019/713), e coloca aos Estados-Membros um conjunto de imposições em matéria penal.

O Governo apresentou, pois, a Proposta de Lei n.º 98/XIV/2ª, ao abrigo da sua iniciativa legislativa, nos termos do disposto nos artigos 167.º, n.º 1, e 197.º, n.º 1, alínea *d)*, da CRP, com o propósito expresso de proceder à transposição para a ordem jurídica interna da Diretiva acima mencionada. Destacam-se, neste seguimento, segundo a respetiva Exposição de Motivos, como principais modificações introduzidas pelo Decreto n.º 167/XIV, advindas da Diretiva (UE) 2019/713: (i) o alargamento do leque de crimes relativamente aos quais se admite a responsabilização penal das pessoas coletivas (cfr. artigo 11.º, n.º 2, do Código Penal), passando a incluir nessa sede um conjunto de crimes associados à fenomenologia da fraude e da contrafação de meios de pagamento que não em numerário; (ii) a previsão de novos tipos legais na *Lei do Cibercrime,* através dos novos artigos 3.º-A a 3.º-D, englobando toda a matéria relativa à contrafação ou falsificação de todos os instrumentos de pagamento (corpóreos e não corpóreos) que não em numerário; (iii) o ajustamento das molduras penais de algumas condutas já previstas, através da alteração do artigo 6.º da *Lei do Cibercrime*; (iv) o aditamento das condutas descritas no artigo 5.º da Diretiva (distinção entre «*apropriação ilegítima*» e «*obtenção ilícita*»), introduzindo um novo artigo 3.º-E à *Lei do Cibercrime*; (v) e o ajustamento do ponto de contacto para fins de cooperação internacional, previsto no artigo 21.º da *Lei do Cibercrime*, onde passa a figurar o Ministério Público, atenta a natureza da informação a trocar.

Todavia, a redação proposta do artigo 17.º da *Lei do Cibercrime* não constitui uma exigência imposta pela transposição da Diretiva (UE) 2019/713, correspondendo, antes, a um desejo do legislador de clarificação e alteração da norma até agora vigente em matéria de apreensão de *correio eletrónico*. Efetivamente, no que respeita à alteração do artigo 17.º da *Lei do Cibercrime*, que é objeto do presente pedido de fiscalização preventiva, pode ler-se na parte que ora releva da Exposição de Motivos da Proposta de Lei:

> «Noutro plano, e ainda que se trate de um aspeto não respeitante à transposição da Diretiva (UE) 2019/713, aproveita-se o ensejo para ajustar o artigo 17.º da Lei do Cibercrime, cujo teor tem gerado conflitos jurisprudenciais que prejudicam a economia processual e geram dúvidas desnecessárias.
>
> Este ajustamento tem como propósito clarificar o modelo de apreensão de correio eletrónico e da respetiva validação judicial.
>
> Visa-se, por um lado, esclarecer que a apreensão de mensagens de correio eletrónico ou de natureza similar está sujeita a um regime autónomo, que vigora em paralelo com o regime da apreensão de correspondência previsto no Código de Processo Penal. Este último regime apenas se aplica à apreensão de mensagens de correio eletrónico ou de natureza similar a título subsidiário, e com as necessárias adaptações.
>
> Visa-se, por outro lado, esclarecer que a apreensão de mensagens de correio eletrónico ou de natureza similar guardadas num determinado dispositivo, embora incidindo sobre dados informáticos de conteúdo especial, não é tecnicamente diferente da apreensão de outro tipo de dados informáticos.
>
> Assim, deve o Ministério Público, após análise do respetivo conteúdo, apresentar ao juiz as mensagens de correio eletrónico ou de natureza similar cuja apreensão tiver ordenado ou validado e que considere serem de grande interesse para a descoberta da verdade ou para a prova, ponderando o juiz a sua junção aos autos tendo em conta os interesses do caso concreto.
>
> Esta solução procura replicar, no domínio das mensagens de correio eletrónico ou de natureza similar, a solução presentemente aplicável aos dados e documentos informáticos cujo conteúdo possa revelar dados pessoais ou íntimos, pondo em causa a privacidade do respetivo titular ou de terceiro, nos termos do n.º 3 do artigo 16.º da Lei do Cibercrime.»

Deste modo, e como resulta evidente do texto transcrito, a alteração do artigo 17.º da *Lei do Cibercrime* prende-se com a necessidade, identificada pelo legislador, de procurar resolver alegados *conflitos jurisprudenciais* causados pelo teor daquela norma, assim como de *clarificar o regime jurídico* relativo à apreensão de correio eletrónico e respetiva validação judicial.

Na verdade, no que respeita à motivação das alterações em causa, a *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*, aprovada pela Resolução do Conselho de Ministros n.º 92/2019, 23 de maio de 2019, indiciava já tais propósitos. Lê-se no respetivo Eixo 4 que se pretende:

> «[a]valiar no âmbito da cibercriminalidade [d]a necessidade de ajustamento das normas processuais penais aos desafios globais que a mesma coloca e, em particular quanto a eventual acesso transfronteiriço a dados (prova digital), a eventual cooperação com operadores de comunicações estrangeiros e a agilização de ações de investigação online, incluindo as que possam enquadrar-se no contexto de ações encobertas, nos termos da lei; [p]onderar a atualização do existente enquadramento legal da retenção de dados e o enquadramento legal da apreensão do correio eletrónico e outras comunicações de natureza semelhante».

13. Atentos os motivos expostos pelo legislador, cabe esclarecer o seguinte: é evidentemente legítimo, no que respeita à segurança e determinabilidade na aplicação da lei processual penal, a criação de um regime jurídico próprio, e autónomo, especificamente respeitante à apreensão de mensagens de correio eletrónico ou de natureza similar, podendo remeter-se o regime de apreensão da correspondência previsto no Código de Processo Penal para a condição de legislação subsidiária. Isso não invalida, porém, a necessidade de respeito pelas normas jurídico-constitucionais relevantes, em particular as que dizem respeito a direitos fundamentais e às garantias em processo penal, bem como as que consagram princípios fundantes do Estado de direito, como o princípio da proporcionalidade. Ou seja, pode criar-se *um novo regime*, mas não *qualquer regime*.

Por outro lado, no que respeita aos alegados "*conflitos jurisprudenciais que prejudicam a economia processual e geram dúvidas desnecessárias*" em torno do artigo 17.º da *Lei do Cibercrime*, que também justificariam a referida alteração legislativa, analisada a jurisprudência dos tribunais superiores, verifica-se que, amiúde,

as diferenças de fundamentação e pronúncia resultam dos distintos contornos e da problemática concretamente em causa em cada um dos acórdãos (veja-se, por exemplo, a este propósito, o Acórdão do Supremo Tribunal de Justiça de 20 de janeiro de 2021, no Processo 454/17.6T9LMG-E.C1-A.S1, disponível, bem como todos os que em seguida se referirão, em www.dgsi.pt).

14. Atento o enquadramento que acaba de se descrever, é, pois, indispensável analisar as alterações introduzidas pelo artigo 5.º do Decreto n.º 167/XIV, da Assembleia da República, no que respeita ao regime jurídico relativo à apreensão de correio eletrónico e registos de comunicações de natureza semelhante, regulado pelo artigo 17.º da *Lei do Cibercrime*.

A versão atual da norma consagra o seguinte:

> «Artigo 17.º
>
> Apreensão de correio eletrónico e registos de comunicações de natureza semelhante
>
> 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 eletrónico 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».

Por seu turno, a nova redação do artigo 17.º, contendo os preceitos normativos questionados, e que deverão ser objeto de análise pelo Tribunal Constitucional, dispõe neste sentido:

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

Do confronto entre ambas as versões do artigo em causa ressaltam alterações relevantes no regime jurídico por ele instituído, que correspondem à intenção de mudança expressa pelo legislador na

Exposição de Motivos do diploma, acima transcrita.

15. Tais alterações respeitam, em primeiro lugar, ao *órgão competente* e às *formalidades* exigíveis para apreensão de correio eletrónico ou semelhante. Onde a atual versão da lei prevê uma *competência exclusiva do juiz,* a versão constante do Decreto em análise refere-se à *autoridade judiciária competente*. Daqui resulta, pois, uma (nova) repartição da competência em causa entre o Juiz, o Ministério Público, em fase de inquérito, nos termos do n.º 1 do artigo 17.º, e os Órgãos de Polícia Criminal, sem prévia autorização judicial, nas situações previstas no n.º 2 do artigo 17.º, de natureza cautelar.

Nestes termos, nos casos em que tenha sido o Ministério Público a ordenar ou validar a apreensão, deve este apresentar ao juiz, sob pena de nulidade, as mensagens de correio eletrónico que repute de *grande interesse para a descoberta da verdade ou para a prova*, ponderando este a sua junção aos autos (artigo 17.º, n.º 4) – à semelhança do disposto no n.º 3 do artigo 179.º do CPP, que também atribui ao juiz a competência para determinar a junção da correspondência apreendida ao processo. Por outro lado, os Órgãos de Polícia Criminal podem apreender correio eletrónico ou similar, nas situações de pesquisa informática executada nos termos do artigo 15.º da própria *Lei do Cibercrime*, ou quando haja urgência ou perigo na demora, exigindo-se ulterior validação *pela autoridade judiciária*, no prazo máximo de 72 horas.

Em segundo lugar, há mudanças relevantes no que toca à definição *do objeto* das apreensões. Na redação atual, podem ser apreendidas mensagens de correio eletrónico, ou semelhante, que se revelem *de grande interesse para a descoberta da verdade ou para a prova*; porém, na redação agora proposta, alarga-se o objeto a todo o conjunto de *mensagens necessárias à produção de prova, tendo em vista a descoberta da verdade*, ponderação esta que poderá ser feita por qualquer dos órgãos com competência para efetuar a apreensão.

Além do que se assinalou, cabe ainda notar que a remissão, em bloco, para o disposto no artigo 179.º do CPP – que contém o regime jurídico aplicável à *apreensão de correspondência* –, presente na atual redação do artigo 17.º da *Lei do Cibercrime*, será substituída, na versão aqui em crise, por uma previsão de *aplicação subsidiária*, e com *as necessárias adaptações* do disposto naquela norma do Código de Processo Penal.

16. Assim, parece resultar da análise empreendida que as alterações propostas pretendem criar um *regime jurídico autónomo,* relativo à apreensão de mensagens de correio eletrónico ou de natureza semelhante, com paralelismos significativos com o regime consagrado no artigo 178.º do CPP, relativo às apreensões de objetos relacionados com a prática de um facto ilícito típico, deixados pelo agente no local do crime ou quaisquer outros suscetíveis de servir a prova.

De facto, e como acima se assinalou, a alteração mais significativa consiste no alargamento da competência do Ministério Público que, enquanto autoridade judiciária competente em sede de inquérito, passa a poder autorizar, ordenar e até mesmo validar a apreensão de mensagens de correio eletrónico. Do mesmo modo, e em coerência com o estabelecido nos artigos 55.º e 249.º do CPP quanto à competência dos Órgãos de Polícia Criminal, a estes é atribuída a faculdade de praticar, no âmbito da apreensão de correio eletrónico, os atos destinados a assegurar os meios de prova, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 15.º, *bem como* (o que parece indiciar uma condição *alternativa* e não *cumulativa*) nos casos de urgência ou perigo na demora – atos estes sujeitos, como sempre se imporia, a ulterior validação *da autoridade judiciária*. Nestes termos, não só o Ministério Público passa a ter, em fase de inquérito, e à luz da nova redação do n.º 1 do artigo 17.º da *Lei do Cibercrime*, competência para uma intervenção prévia à apreensão – *ordenando-a ou autorizando-a*, por despacho, *em vez* do Juiz de Instrução Criminal -, como o n.º 2 do mesmo artigo admite também uma intervenção *ex post*, *validando*, no prazo de 72 horas, a apreensão realizada pelo Órgão de Polícia Criminal. Note-se, ainda, que, em qualquer dos casos, as normas questionadas não

preveem um *prazo* para apresentação pelo Ministério Público ao juiz das mensagens de correio eletrónico ou de natureza semelhantes cuja apreensão tenham ordenado (*ex ante*) ou validado (*ex post*).

Ora, este regime jurídico, na sua *autonomia*, expressamente pretendida pelo legislador, aproxima-se mais do regime jurídico previsto na legislação processual penal para a apreensão de objetos, *lato sensu*, consagrado no artigo 178.º do CPP, do que do disposto no artigo 179.º do CPP quanto à apreensão de *correspondência*, pese embora este último continuar a funcionar – por força da remissão em bloco feita no n.º 6 da redação proposta para o artigo 17.º da *Lei do Cibercrime* – como legislação subsidiária. Paralelamente, o legislador inspira-se no disposto no n.º 3 do artigo 179.º do CPP quando, no (novo) n.º 4 do artigo 17.º, estabelece que caberá ao juiz aferir da pertinência da junção ao processo das mensagens apreendidas. Este paralelismo parece, assim, também, permitir estender às situações de apreensão de correio eletrónico ou similar uma das mais relevantes garantias referentes às situações de apreensão de correspondência, a saber, a consagração da nulidade como sanção associada à ausência de despacho do juiz (cfr. artigo 179.º, n.º 1, do CPP). Pretende-se com isto assinalar que a intromissão na correspondência, pelo potencial de afetação de direitos fundamentais que apresenta, merece uma tutela mais exigente por parte do legislador.

Em suma, com esta nova versão do artigo 17.º, constante do Decreto aqui em causa, constrói-se, para a específica situação de *apreensão de correio eletrónico ou similar*, um *regime híbrido*, que combina elementos significativos do regime consagrado no artigo 178.º do CPP, relativo às apreensões de objetos relacionados com a prática de um facto ilícito, com parte da disciplina jurídica respeitante à apreensão de correspondência, constante do artigo 179.º CPP. O novo regime legal determina um reforço da competência do Ministério Público, em fase de inquérito, dispensando a intervenção do juiz para a apreensão de mensagens de correio eletrónico ou de natureza semelhante, ficando esta reservada, apenas, para a eventual junção aos autos de mensagens de correio eletrónico selecionadas.

17. A Proposta de Lei foi apreciada em sede parlamentar pela Comissão dos Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República, em conexão com a Comissão de Orçamento e Finanças, tendo ambas emitido pareceres favoráveis, no dia 23 de junho de 2021.

No âmbito dos trabalhos da Comissão dos Assuntos Constitucionais, Direitos, Liberdades e Garantias foram consultadas diversas entidades, que também emitiram, maioritariamente, opinião favorável sobre a Proposta de Lei. Com particular interesse para o presente processo, cabe dar nota, em primeiro lugar, do parecer do Conselho Superior do Ministério Público, de 8 de junho de 2021, no qual se pode ler, no que respeita especificamente à nova redação do artigo 17.º da *Lei do Cibercrime*:

> «Trata-se de uma alteração alheia ao propósito principal do projeto legislativo, mas que se afigura muito positiva. Por um lado, esta norma tem gerado grandes críticas, pelas enormes divergências interpretativas que tem gerado, na doutrina e na jurisprudência. Por outro lado, havendo uma intervenção legislativa nesta Lei (que é a primeira, desde que foi publicada em 2009), julga-se ser apropriado aproveitar esta iniciativa legislativa para ajustar um regime legal que é claramente problemático, por suscitar recorrentemente divergentes decisões, nos processos reais, nos tribunais, com claro prejuízo para a eficácia do sistema e para a justiça do caso concreto.
>
> A redação da proposta visa enquadrar de forma mais adequada a apreensão de mensagens de correio eletrónico ou de natureza similar, no contexto do regime geral das apreensões de dados informáticos. Trata-se de uma opção legislativa muito positiva, uma vez que, numa perspetiva técnica e operativa, a apreensão de mensagens de correio eletrónico ou de natureza similar não difere da apreensão de dados em geral. É certo que incide sobre conteúdos específicos - e sensíveis -, mas a proposta legislativa introduz um complexo sistema de salvaguardas que vão ao encontro dessa especificidade.
>
> Atendendo à natureza específica deste tipo de mensagens, o regime proposto introduz um modelo que aproxima a lei do modelo constitucional, de atribuição ao Ministério Público da competência para investigar

crimes e recolher e selecionar a respetiva prova. Por outro lado, reserva para o juiz de instrução a função de garantir que os direitos, liberdades e garantias dos cidadãos são observadas durante a investigação.

O modelo operativo proposto também é coerente com o modelo das interceções telefónicas - o que não acontece com o regime vigente, que é disfuncional. Na verdade, o modelo atual consagra (e bem) um modelo de clara iniciativa do Ministério Público quanto a interceções telefónicas e interceções de comunicações eletrónicas de todas as naturezas, mas depois tolhe por completo a iniciativa do Ministério Público na apreensão de registos de correio eletrónico, já recebido.

Na prática, o modelo agora preconizado por esta Proposta de Lei vai ao encontro das sugestões e da interpretação da doutrina mais preponderante a este respeito, ao mesmo tempo que garante a essencial intervenção judicial.»

Por seu turno, o Conselho Superior da Magistratura submeteu o seu parecer a 24 de junho de 2021, no qual concluiu, na parte que ora releva, que "[*a*] *presente Proposta de Lei procede a uma correta transposição para a ordem jurídica interna [d]a Diretiva*", e que "*a presente iniciativa legislativa constitui uma proposta de alterações pontuais à legislação já existente, as quais entenderam-se ser as necessárias para superar lacunas ou para esclarecer divergências de interpretações*."

18. Em sentido contrário, e de forma bastante contundente, a Comissão Nacional de Proteção de Dados (CNPD) entendeu, no seu parecer 2021/74, mencionado também pelo autor do presente pedido de fiscalização da constitucionalidade, que as alterações propostas ao artigo 17.º da Lei do Cibercrime se afiguram como problemáticas, a vários títulos, tendo apresentado os seguintes fundamentos principais:

«17. Resulta, na perspetiva da CNPD, evidente, que o artigo 17.º da Lei do Cibercrime arquiteta um sistema de validação da apreensão de mensagens de correio eletrónico (ou registos de comunicações de natureza semelhante) em (quase) tudo coincidente com o previsto no artigo 179.º do CPP. Sendo o objeto da Lei do Cibercrime o "estabelec[imento d]as 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 electrónico", ela constitui, quanto aos elementos de prova em suporte eletrónico verdadeira lex specialis por contraponto ao CPP. Ainda assim, o legislador optou por concretizar a restrição do direito constitucional à inviolabilidade da correspondência, previsto no artigo 34.º da Constituição da República Portuguesa (CRP), com uma cláusula que praticamente replica o n.º 1 do artigo 179.º do CPP, salvo quando à tripla condição que neste inciso se aponta como condição para fundamentar a autorização ou ordem de apreensão.

18. Ora, se se aceita que uma alteração legislativa possa servir para superar "conflitos jurisprudenciais que prejudicam a economia processual e geram dúvidas desnecessárias", já se apontam maiores dificuldades a admitir que essa modificação possa pretender superar esses problemas pela via da menorização de direitos fundamentais constitucionalmente consagrados - em particular, um direito fundamental que tem precisamente por objeto a reserva do conteúdo das comunicações.

19. Também se pode compreender "que a apreensão de mensagens de correio eletrónico ou de natureza similar guardadas num determinado dispositivo, embora incidindo sobre dados informáticos de conteúdo especial, não é tecnicamente diferente da apreensão de outro tipo de dados informáticos", mas esta conclusão já se torna incompreensível se se destinar a justificar a equiparação de dados pessoais e dados não pessoais. Com efeito, a CRP reserva não só uma esfera de proteção para a reserva da intimidade da vida privada, como melhor a concretiza no direito à inviolabilidade da correspondência, e ainda singulariza a proteção de dados pessoais neste catálogo de preceitos "diretamente aplicáveis".

20. Seria, por isso, injustificado, desde logo no plano constitucional, consagrar na legislação a indistinção entre dados pessoais e dados não pessoais. Ademais, tal constituiria uma latente violação do reconhecimento que é devido ao direito ao respeito pela vida privada e familiar como se encontra positivado no artigo 8.º da Convenção Europeia dos Direitos do Homem e, bem assim, pelos artigos 7.º e 8.º da Carta dos Direitos

Fundamentais da União Europeia, respetivamente quanto ao respeito pela vida privada e familiar e à proteção de dados pessoais.

21. Temos, portanto, que um tal objetivo, declarado na exposição de motivos, contraria quer a Constituição, quer os compromissos internacionais do Estado português, sendo insondável a razão para a sua inclusão na Lei do Cibercrime.

22. E nem se diga, como é avançado no Projeto, que o que se pretende é a equiparação ao regime da apreensão de dados informáticos, constante do artigo 16.º, especificamente o previsto no n.º 3. Desde logo, a apreensão de dados informáticos, ao contrário do correio eletrónico e dos registos de comunicações do artigo 17.º, não tem necessariamente que envolver dados pessoais ou reveladores da dimensão da vida privada dos visados, sendo essa a razão para que o sobredito n.º 3 do artigo 16.º acautele potenciais casos em que tal aconteça, reforçando-se as garantias dos cidadãos através da obrigatória intervenção do Juiz.

23. Depois, porque, ao contrário das comunicações, será habitual encontrar esta informação (i.e., os dados informáticos) não vedada ou fechada (ou com indicação semelhante), dependendo o conhecimento da existência de dados pessoais ou íntimos do contacto direto e inevitável com o conteúdo desses dados informáticos ainda antes da potencial intervenção do Juiz.

24. Finalmente, por degradar o regime aplicável às comunicações, não deveria ser visto como o meio óbvio e idóneo para fazer face aos requisitos constitucionais que os n.ºs 2 e 3 do artigo 18.º da CRP colocam sempre que se pretenda limitar ou restringir os direitos, liberdades e garantias. Sobretudo quando tal degradação se aparta, em medida desproporcionada, do regime previsto no CPP para a apreensão de correspondência, o qual era, até agora, perfeitamente aplicável aos casos previstos no artigo 17.º da Lei do Cibercrime.

25. Uma última nota, quanto à exposição de motivos, no que concerne à desconsideração processual da indicação "de as mensagens de correio eletrónico ou de natureza similar estarem identificadas como «abertas» ou «fechadas» uma vez que, ao contrário do que sucede quanto à correspondência em papel, tal identificação pode ser livremente feita pelo seu detentor." (…).

26. Não se contesta a asserção final de que é hoje possível a qualquer destinatário de mensagens deste tipo apor-lhes a identificação de fechadas (ou não lidas). O que se torna incompreensível é como é que o legislador retira desta circunstância a consequência da inevitável degradação do direito fundamental à inviolabilidade da correspondência. E isto em termos completamente novos, desqualificando situações em que, de facto, as comunicações ainda não tivessem sido conhecidas pelo visado, desconsiderando, por esta via, a necessidade de intervenção do juiz e colocando nas mãos do Ministério Público, quando não mesmo do órgão de polícia criminal, a possibilidade de efetuar a apreensão dessa correspondência.

27. O princípio da proporcionalidade, a que alude o n.º 2 do artigo 18.º da CRP, parece exigir a inclusão do juiz de instrução criminal nesta operação de validação das apreensões, mantendo um regime idêntico ao do artigo 179.º do CPP, e seguramente sempre que as mensagens se encontrem com a indicação de "fechada/não lida". E nem se diga que a intervenção do juiz de instrução nos moldes propostos fere ou pode vir a ferir a estrutura acusatória do processo criminal, porquanto ela é meramente decalcada do regime do CPP, cuja conformidade com a CRP não é questionada.

28. Sem prejuízo de eventuais matizes que pudessem ser introduzidos por referência às especificidades das mensagens cuja apreensão vem prevista no artigo 17.º da Lei do Cibercrime, operar uma presunção desta gravidade, sempre em desfavor de qualquer pessoa que veja esse tipo de correspondência apreendida, afigura-se desproporcionado e, portanto, violador dos princípios constitucionais que regem as restrições dos direitos, liberdades e garantias.

(...)

I. Conclusão

50. Com os fundamentos acima expostos, entende a CNPD que:

a. As alterações ao artigo 17.º da Lei do Cibercrime, tal como se encontram no projeto de proposta de lei em análise, representam uma manifesta degradação do nível de proteção dos cidadãos num domínio crítico da sua esfera privada, como é o das comunicações;

b. Ao divergir incontroversamente do regime previsto no artigo 179.º do CPP, o Projeto de Proposta de Lei introduz restrições adicionais e não fundamentadas aos direitos, liberdades e garantias à inviolabilidade das comunicações e, reflexamente, à proteção de dados pessoais, como vêm consagrados nos artigos 34.° e 35.° da CRP, respetivamente;

c. Admitir que o Ministério Público possa, sem prévio controlo do Juiz de Instrução Criminal, ordenar ou validar a apreensão de comunicações eletrónicas ou de registos similares desprotege excessivamente as pessoas eventualmente suspeitas ou que tenham incidentalmente interagido com esses suspeitos, sendo que a exigência de intervenção do Juiz de Instrução, nos mesmos termos do artigo 179.° do CPP, nunca pode ser vista como desvirtuadora do princípio acusatório que preside ao processo penal em Portugal;

d. De resto, e atento o teor do recente acórdão do TJUE, de 2 de março, no processo C-746/18, onde se afasta a possibilidade de uma entidade em tudo semelhante - nos poderes e na dependência hierárquica - ao Ministério Público português poder aceder aos dados de tráfego e de localização, no quadro de um processo penal e em concretização das exceções previstas no n.° 1 do artigo 15.° da Diretiva 2002/58/CE, sem prévia autorização de um Juiz ou entidade independente, só pode ter-se por inadmissível a alteração proposta para o artigo 17.° da Lei do Cibercrime, por manifesta contradição com o disposto no artigo 52.° da Carta dos Direitos Fundamentais da UE (e sem prescindir do disposto no n.° 2 do artigo 18.° da CRP)».

C) Elementos relevantes

C.1) Direito da União Europeia e do Conselho da Europa

19. Ainda que, como expressamente reconhece o legislador na Exposição de Motivos acima transcrita, a nova redação do artigo 17.º da *Lei do Cibercrime* não resulte diretamente de exigências decorrentes da transposição de diretivas da União Europeia, não pode olvidar-se que a Lei n.º 109/2009 tem que ser interpretada à luz do contexto de internormatividade e interconstitucionalidade que esteve na sua génese e que define o seu horizonte aplicativo (uma vez que transpôs para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, relativa a ataques contra sistemas de informação, e adaptou o direito interno à Convenção sobre Cibercrime do Conselho da Europa).

Deste modo, afigura-se incontornável o enquadramento da discussão da matéria dos presentes autos no domínio do direito do espaço europeu – quer da União Europeia, quer do Conselho da Europa –, importando conhecer e atender aos *standards* de proteção que deles resulta para os direitos fundamentais aqui em causa, designadamente, a *privacidade*, entendida em sentido lato, e com particular relevância no domínio da proteção de dados e utilização da informática. A jurisprudência do Tribunal de Justiça da União Europeia ("TJUE") e do Tribunal Europeu dos Direitos do Homem ("TEDH") oferece, neste domínio, um relevante conjunto de informações e orientações que o Tribunal Constitucional, animado pela necessidade de proceder a uma interpretação do texto constitucional articulada com os parâmetros europeus, não pode deixar de considerar na análise que lhe é solicitada nos presentes autos.

20. O Decreto n.º 167/XIV visa, no essencial, e como já se disse, proceder à transposição para a ordem jurídica interna da Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário (Diretiva), a qual substitui a Decisão-Quadro 2001/413/JAI do Conselho, que havia sido

transposta pela Lei n.º 59/2007, de 4 de setembro, que procedeu à vigésima terceira alteração ao Código Penal.

Além disso, importa ainda mencionar, nesta sede, pela relevância que assumem na matéria em discussão nos presentes autos de fiscalização preventiva: (i) a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, sucessivamente alterada pela Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006 e pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 – adotada com o intuito de harmonizar a legislação dos Estados-Membros e garantir um nível equivalente de proteção dos direitos fundamentais, nomeadamente o *direito à privacidade*, no âmbito do tratamento de dados pessoais no setor das comunicações eletrónicas (n.º 1 do artigo 1.º), transposta para a ordem interna pela Lei n.º 41/2004, de 18 de agosto, e pela Lei n.º 46/2012, de 29 de agosto; e (ii) a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações (que veio a ser considerada inválida pelo TJUE, no seu Acórdão de 8 de abril de 2014, Processos apensos C-293/12 e C-594/12, *Digital Rights Ireland e Seitlinger e o.*), transposta para a ordem interna pela Lei n.º 32/2008, de 17 de julho.

Para além das diretivas que especificamente visam uniformizar os regimes jurídicos de conservação de dados no setor das comunicações eletrónicas, não é despicienda a disciplina que se retira do Regulamento Geral sobre a Proteção de Dados (Regulamento UE 2016/679 — RGPD), no que tange à proteção conferida *às pessoas singulares* a respeito do tratamento de dados pessoais. Destaca-se, nesta sede, a disposição que prevê que os dados que permitam identificar pessoas singulares, apenas podem ser *recolhidos para satisfazer finalidades determinadas, explícitas e legítimas, e não podem ser tratados posteriormente de uma forma incompatível com essas finalidades* (artigo 5.º, n.º 1, alínea *b)* RGDP).

Não se ignora, naturalmente, que nos termos do artigo 1.º, n.º 3, da Diretiva 2002/58/CE, e do artigo 2.º do RGPD, o âmbito de aplicação da legislação europeia, nesta matéria, não inclui o processo penal. Contudo, afigura-se, ainda assim, que do acervo legal e jurisprudencial da União Europeia acerca de temáticas paralelas à que ora nos ocupa resulta a paulatina construção de *standards* de tutela jusfundamental no que respeita ao tratamento de dados pessoais e de dados relativos às comunicações, no âmbito da utilização da informática que não deve ser ignorado.

21. No plano jusfundamental, a matéria em causa suscita a invocação dos artigos 7.º, 8.º e 52.º, n.º 1 da Carta dos Direitos Fundamentais da União Europeia ("CDFUE") — a que o Tratado atribui valor paramétrico quanto às normas emanadas pelas instituições, nos termos do n.º 1 do artigo 6.º do Tratado da União Europeia ("TUE") —, que consagram, respetivamente: (i) o direito de todas as pessoas ao respeito pela *sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações*; (ii) o direito de todas as pessoas à *proteção dos dados de caráter pessoal que lhes digam respeito* – os quais devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei, ficando o cumprimento destas regras sujeito a fiscalização por parte de uma autoridade independente; e (iii) a garantia de que qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela CDFUE deve ser *prevista por lei* e respeitar o *conteúdo essencial desses direitos e liberdades*, na observância do *princípio da proporcionalidade*, o que implica que essas restrições só possam ser introduzidas se forem *necessárias* e *corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União*, ou à *necessidade de proteção dos direitos e liberdades de terceiros.* A *proteção dos dados pessoais* é, além disso, um direito fundamental igualmente consagrado no artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia ("TFUE").

Assume, por último, relevância a consagração no artigo 8.º da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais ("CEDH"), do direito de qualquer pessoa ao

respeito da *sua vida privada e familiar, do seu domicílio e da sua correspondência.* Daqui decorre a proibição de *haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.*

22. A matéria objeto de regulação pelas normas fiscalizadas não é, diretamente, objeto de qualquer acórdão do TJUE e/ou do TEDH. Sem prejuízo disso, a jurisprudência europeia emitida no quadro das Diretivas 2002/58/CE e 2006/24/CE, a propósito da conservação e transmissão de dados provenientes de comunicações eletrónicas, ou da interceção de comunicações em massa, por referência aos parâmetros de tutela fundamentais consagrados nos artigos 7.º e 8.º da CDFUE e 8.º da CEDH, oferece importantes pistas quanto à densificação, feita por aqueles tribunais superiores, dos respetivos *standards* jusconstitucionais de proteção dos cidadãos nos domínios da privacidade e das comunicações eletrónicas – os quais assumem especial interesse na discussão objeto dos presentes autos. Com efeito, identifica-se, nesse acervo jurisprudencial, um conjunto de princípios e requisitos claramente exigidos pelo TJUE e pelo TEDH que, em larga medida, são transponíveis, com as devidas adaptações, para a problemática da *apreensão de mensagens de correio eletrónico e outras de natureza similar*, para fins de investigação, deteção e repressão de infrações penais. Essa jurisprudência é o ponto axial da densificação dos conceitos do catálogo de direitos da União e referência incontornável na construção de *standards* de proteção de direitos fundamentais num espaço de interconstitucionalidade.

Ora, de acordo com o Tribunal de Justiça, para avaliação da conformidade com os direitos fundamentais das *medidas de conservação de dados,* há que convocar não apenas a proteção conferida pela norma do artigo 7.º da CDFUE, mas também a do artigo 8.º, sempre que tais dados possam ser ligados à identificação de uma pessoa. Ou seja, o *standard* de proteção aplicável quando estão em causa dados de um processo de comunicação entre pessoas que se situem na sua esfera privada (permitindo a sua identificação ou a obtenção de outras informações *pessoais*, normalmente reservadas) resulta da interpretação combinada dos direitos à *privacidade* e à *proteção de dados pessoais*. Este entendimento funda-se não apenas na constatação de que os dois direitos estão indissociavelmente ligados (Acórdão de 9 de novembro de 2010, *Volker,* procs. C-92/09 e C-93/09, n.º 47), como também na admissão expressa, por parte do TJUE, de que a *"conservação dos dados está abrangida pelo âmbito de aplicação do artigo 8.º desta, uma vez que constitui um tratamento de dados pessoais na aceção deste artigo e deve, assim, necessariamente, respeitar as exigências de proteção de dados resultantes deste artigo"* — Acórdão de 8 de abril de 2014, *Digital Rights Ireland,* procs. C-293/12 e C-594/12, n.º 29.

Além disso, é importante recordar que o artigo 7.º da CDFUE, relativo ao respeito pela vida privada e familiar, ao domicílio e às comunicações, reproduz o disposto no artigo 8.º da CEDH, devendo ser interpretado com o mesmo sentido e alcance, nos termos do n.º 3 do artigo 52.º da CDFUE. O que implica, pois, que o regime das suas restrições seja semelhante, como de resto concluiu o Tribunal de Justiça no Acórdão de 15 de novembro de 2011, *Dereci*, proc. C-256/11, n.º 70: *"o artigo 7.° da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»), relativo ao direito ao respeito da vida privada e familiar, consagra direitos correspondentes aos que são garantidos pelo artigo 8.°, n.º 1, da CEDH e que se deve, portanto, dar ao artigo 7.° da Carta o mesmo sentido e o mesmo alcance que o sentido e o alcance dados ao artigo 8.°, n.º 1, da CEDH, conforme interpretado pela jurisprudência do Tribunal Europeu dos Direitos do Homem"*. Neste quadro, entendeu-se mobilizável, para densificação do artigo 7.º da CDFUE, o regime do n.º 2 do artigo 8.º da CEDH: *"Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros"*. Simplesmente, ao contrário do que sucede na CEDH, a Carta autonomizou o direito à proteção de dados pessoais (no artigo 8.º da CDFUE), sem deixar de lhe reconhecer uma relação indissociável entre

ambos (Acórdão de 9 de novembro de 2010, *Volker,* procs. C-92/09 e C-93/09, n.º 47; C. SARMENTO E CASTRO, "Anotação ao artigo 8.º", in *Carta dos Direitos Fundamentais da União Europeia Comentada,* coord. A. SILVEIRA e M. CANOTILHO, Almedina, 2013, p. 121; S. PEREZ FERNANDES, "Anotação ao artigo 7.º", in *Carta dos Direitos Fundamentais da União Europeia Comentada,* coord. A. SILVEIRA e M. CANOTILHO, Almedina, 2013, p. 105).

23. A aplicação da Diretiva 2002/58/CE (sobre tratamento de dados pessoais e proteção da privacidade no sector das comunicações eletrónicas) suscitou um conjunto de questões pertinentes sobre a possibilidade de restrições ou limitações aos direitos nela consagrados e às correspetivas obrigações estaduais, que podem ser úteis para a ponderação a levar a cabo no presente processo. Questionou-se, desde logo, o alcance da proibição de formas de interceção ou vigilância de comunicações, sem o consentimento dos utilizadores. Naturalmente, a própria ordem jurídica europeia prevê condições segundo as quais será possível derrogar o nível de proteção consagrado como regra. Contudo, a diversidade e amplitude das medidas derrogatórias adotadas pelos Estados-Membros ao abrigo desta norma revelaram-se muito problemáticas, em particular no campo da prevenção, investigação, deteção e repressão de infrações penais, no qual foram aprovados, pelos vários países, regimes bastante distintos de acesso à informação. Por esse motivo, o legislador europeu aprovou, em 2006, a Diretiva n.º 2006/24/CE, que visava, precisamente, concretizar o âmbito das restrições autorizadas aos direitos fixados na Diretiva 2002/58/CE e especificar o nível mínimo de proteção garantido, em qualquer caso, em relação aos direitos fundamentais em questão. Porém, esta Diretiva veio a ser declarada inválida pelo TJUE, precisamente por este Tribunal ter entendido que aquela permitia uma restrição desproporcionada dos direitos ao respeito pela vida privada e familiar e à proteção de dados pessoais, consagrados, respetivamente, nos artigos 7.º e 8.º da CDFUE (Acórdão *Digital Rights Ireland*, n.ºs 26 a 29); e por se considerar que o conjunto de crimes cuja investigação ou repressão pode admitir o acesso aos dados se estabelecia de forma indeterminada (n.ºs 41 a 43).

Dessa jurisprudência (a que se soma o Acórdão *Tele2*, de 21 de dezembro de 2016, proc. C-203/15 e C-698/15) resultam dois eixos fundamentais para a presente análise. Em primeiro lugar, o Tribunal do Luxemburgo impôs um conjunto de condições relativas ao armazenamento de dados, designadamente, o respeito pelos princípios da *necessidade* da conservação dos dados, e da *determinabilidade* das normas que regulam tais medidas de conservação. Em segundo lugar, e com significativa relevância para a matéria que aqui nos ocupa, no que respeita ao acesso aos dados pelas autoridades nacionais competentes para deteção, prevenção e combate à criminalidade, o Tribunal de Justiça entendeu que uma interpretação adequada do disposto no artigo 15.º da Diretiva 2002/58/CE, em conjugação com a proteção jusfundamental conferida pelas normas dos artigos 7.º e 8.º da CDFUE, não admite o acesso generalizado aos dados conservados – implicando, pelo contrário a existência de um *controlo prévio*, levado a cabo por um *órgão jurisdicional* ou por uma *entidade* administrativa *independente*, na sequência de um *pedido fundamentado* da autoridade nacional competente. Este entendimento foi reiterado no Acórdão de 6 de outubro de 2020, Processo C-623/17 - *Privacy International*, tendo o Tribunal de Justiça insistido na ideia de respeito pelo *princípio da proporcionalidade*, recordando que na origem da Diretiva 2002/58, está, justamente, uma intenção do legislador da União de assegurar a continuação de um *elevado nível de proteção dos dados pessoais e da privacidade no que diz respeito a todos os serviços de comunicações eletrónicas, independentemente da tecnologia utilizada* (n.º 55, CFR. exposição de motivos da proposta de diretiva do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas [COM(2000) 385 final]). 60).

24. Ou seja, tendo em conta tudo o que até agora se narrou, ressaltam da jurisprudência do TJUE acima descrita várias linhas argumentativas que, não obstante as já assinaladas diferenças quanto ao *âmbito de aplicação* da legislação em causa, não poderão ser ignoradas na ponderação a levar a cabo no

presente processo, importando discutir em que medida podem ou devem as mesmas regras de princípio ser mobilizadas em matéria de *apreensão* do correio eletrónico ou similar.

Em primeiro lugar, resulta evidente que a CDFUE não é compatível com práticas de recolha e conservação de dados de ordem *indiferenciada e generalizada*, sem uma qualquer *seleção prévia,* segundo *critérios objetivos*. Ora, isto deve levar-nos a questionar se, na generalidade dos casos, é compatível com o direito da União a apreensão de *todas* as mensagens de correio eletrónico (que poderão, mesmo no caso de computadores de uso estritamente pessoal, atingir números na casa dos largos milhares), devendo a seleção do conjunto de mensagens apreendidas limitar-se *ao estritamente necessário* para investigação e repressão da criminalidade. Em segundo lugar, e com evidente importância no presente processo, resulta da jurisprudência exposta que o acesso pelas autoridades nacionais a dados de comunicação, ainda que para combate à criminalidade, deverá ser sempre sujeito a *controlo judicial* ou de *entidade* administrativa *independente* – ideia que veio a ser retomada no recente acórdão de 2 de março de 2021, Processo C-746/18, *Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques)*, adiante analisado, o qual se debruça, justamente, sobre a questão de saber que entidades, ao certo, podem figurar neste papel de *controlo prévio*, designadamente saber se o Ministério Público pode desempenhar tal tarefa.

25. Finalmente, destaca-se, na análise em curso, com especial relevo no debate que subjaz às questões de constitucionalidade colocadas em sede da presente fiscalização preventiva, o recente Acórdão do Tribunal de Justiça, de 2 de março de 2021, Processo C-746/18, *Prokuratuur* (*Conditions d'accès aux données relatives aux communications électroniques*), atrás já referenciado. Prolatado, igualmente, quanto ao tratamento dos dados pessoais no setor das comunicações eletrónicas e da Diretiva 2002/58/CE, em concreto no que respeita ao acesso de uma autoridade pública aos dados de tráfego e aos dados de localização para fins de instrução penal, a sua importância prende-se especificamente com a terceira questão prejudicial nele colocada, por via da qual o órgão jurisdicional de reenvio convida o Tribunal de Justiça a precisar os critérios que uma autoridade administrativa deve satisfazer para poder ser considerada independente, na aceção do Acórdão *Tele2*. Ou seja, no caso *Prokuratuur*, o órgão jurisdicional de reenvio perguntou, concretamente, se o artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.°, 11.° e 52.°, n.° 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que atribui competência ao Ministério Público - cuja missão é dirigir a instrução penal e exercer, sendo caso disso, a ação pública num processo posterior - para autorizar o acesso de uma autoridade pública aos dados de tráfego e aos dados de localização para fins de instrução penal.

Perante esta interrogação, o Tribunal começa por esclarecer que essa fiscalização prévia exige que o órgão jurisdicional ou a entidade encarregada de efetuar a referida fiscalização "*disponha de todas as atribuições e apresente todas as garantias necessárias com vista a assegurar uma conciliação dos diferentes interesses e direitos em causa*" (n.º 52). Esta exigência será acentuada pelo facto de se tratar, no processo C-746/18, de um inquérito penal, o que, no entender do Tribunal implica que *"tal fiscalização exige que esse órgão jurisdicional ou essa entidade possa assegurar um justo equilíbrio entre, por um lado, os interesses ligados às necessidades do inquérito no âmbito da luta contra a criminalidade e, por outro, os direitos fundamentais ao respeito da vida privada e à proteção dos dados pessoais das pessoas às quais o acesso diz respeito"* (n.º 52, destaque acrescentado).

Ou seja, conforme esclarece o TJUE, a exigência de independência que a autoridade encarregada de exercer a fiscalização prévia deve satisfazer impõe que essa autoridade tenha a "*qualidade de terceiro em relação à autoridade que pede o acesso aos dados*" (n.º 54, destaque acrescentado), circunstância indispensável para que esteja em condições de exercer essa fiscalização de maneira *"objetiva e imparcial*", ao abrigo de qualquer influência externa. Isto significa, no domínio penal, como salientou o Tribunal, "*que a autoridade encarregada dessa fiscalização prévia, por um lado, não esteja envolvida na condução do inquérito penal em causa e, por outro, tenha uma posição de neutralidade relativamente às partes no processo penal*" (n.º 54, destaque

acrescentado). Neste exato sentido se pronunciou o Advogado-Geral Giovanni Pitruzzella, nas suas conclusões (cfr. n.º 105 e 126).

Por esta razão, entendeu o Tribunal que, no caso, tal competência não pode ser atribuída ao Ministério Público (n.º 57), considerando que este, quando dirige o inquérito e exerce, sendo caso disso, a ação pública, não assume uma posição de neutralidade, não estando em condições de realizar o enunciado controlo prévio. É que, como sublinha o Tribunal "*o Ministério Público tem por missão, não decidir com total independência um litígio mas submetê-lo, se necessário, ao órgão jurisdicional competente, enquanto parte no processo que exerce a ação penal*" (n.º 55); deste modo, nem mesmo a circunstância de ser obrigado a verificar os elementos incriminatórios e ilibatórios, a garantir a legalidade da instrução do processo e a agir unicamente nos termos da lei e segundo a sua convicção basta para lhe conferir o estatuto de *terceiro* em relação aos interesses em causa (n.º 56).

Por outro lado, e quanto à questão de saber se a falta de fiscalização prévia efetuada por uma autoridade independente poderia ser *suprida por uma fiscalização posterior*, exercida *por um órgão jurisdicional* (cenário hipotético colocado pelo órgão jurisdicional de reenvio), veio o TJUE reforçar que, salvo em caso de *urgência* devidamente justificada (e mesmo nesta exceção o controlo posterior há de ser efetuado em prazos curtos), a fiscalização independente deve ser efetuada previamente a qualquer acesso, (n.º 58). E isto é assim, justamente, porque, como salientou o Advogado-Geral no n.º 128 das suas conclusões, "*essa fiscalização posterior não permitiria responder ao objetivo de uma fiscalização prévia, que consiste em impedir que seja autorizado um acesso aos dados em causa que ultrapasse os limites do estritamente necessário*" (n.º 58).

A proximidade desta discussão – espelhada no caso *Prokuratuur*, que correu termos no TJUE, e no caso *Big Brother Watch,* no TEDH –, é incontornável face à discussão dos autos, e nem a circunstância de se tratar de autorizações relativamente a ações e objetos não inteiramente coincidentes com os da problemática aqui especificamente em causa torna menos pertinente a consideração das reflexões dos Tribunais do Luxemburgo e de Estrasburgo quanto a dois polos problematizantes fundamentais: (i) a aptidão do Ministério Público para atuar como *terceiro imparcial ou neutral relativamente ao litígio*, capaz de levar a cabo uma ação de controlo prévio das restrições a direitos fundamentais; e (ii) a imperatividade da intervenção jurisdicional numa fase prévia à restrição desses mesmos direitos fundamentais ou à suficiência da sua ratificação *ex post*.

C.2) Jurisprudência constitucional

26. Finalmente, ainda dentro da consideração de elementos de relevo para o desenho do quadro sistémico e interpretativo-concetual que deverá constituir o contexto valorativo da presente questão de constitucionalidade, cabe um breve périplo pela jurisprudência constitucional relevante, em torno de dois eixos fundamentais: *i)* a tutela jurídico-constitucional da privacidade, da correspondência, das telecomunicações e dos dados informáticos; e *ii)* a divisão de competências, no que respeita a diligências efetuadas em sede de inquérito, entre Ministério Público e Juiz de Instrução Criminal, com particular atenção à especial garantia constitucional respeitante a atos que se prendam diretamente com direitos fundamentais.

Quanto ao primeiro eixo, o Tribunal Constitucional tem-se pronunciado com clareza acerca de um conjunto de matérias relativas ao acesso das autoridades públicas a *dados de comunicação* (dados de base, dados de tráfego, ou dados de conteúdo, consoante o caso concretamente em apreço). Um breve excurso por tal jurisprudência permite-nos definir linhas argumentativas fundamentais, que a análise valorativa que nesta sede se levará a cabo não pode deixar de considerar. Além disso, fica claro nessa análise que o Tribunal Constitucional tem procurado fazer uma interpretação sistemicamente adequada das normas relativas a este tipo de problemática, tomando em consideração que estas temáticas se

colocam num espaço de interconstitucionalidade europeu, e atendendo, por isso, à jurisprudência do TJUE e do TEDH.

Assim, em primeiro lugar, o Tribunal tem explicado que, em matérias como a que aqui está em causa, e independentemente de se reconhecer que a proteção jusconstitucional relativa à privacidade dos cidadãos, entendida em sentido lato, resulta da interpretação conjugada de distintas normas da CRP, nas situações – como é o caso da tutela das *comunicações* – em que o legislador constituinte tenha entendido tratar de modo particular uma determinada realidade, conferindo-lhe um lugar próprio, e evidenciado, no texto constitucional, dever-se-á atender, antes de mais, a tais disposições normativas específicas.

Isso mesmo se afirma há quase duas décadas, como pode ler-se no Acórdão n.º 241/2002:

> «A Constituição consagra, em diversos preceitos, um conjunto de direitos que protegem o que, lato sensu, se pode considerar a esfera da vida pessoal dos cidadãos.
>
> É o caso do disposto no artigo 26º nº 1 que reconhece o "direito à reserva da intimidade da vida privada", do artigo 34º que garante a inviolabilidade do "sigilo da correspondência e dos outros meios de comunicação privada" (nº 1) e proíbe "toda a ingerência das autoridades públicas (...) nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em processo criminal" (nº 4) e do artigo 32º nº 8 que, no âmbito das garantias do processo criminal, fulmina com a nulidade "todas as provas obtidas mediante (...) abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações".
>
> Independentemente da questão de saber se o sigilo das telecomunciações se inscreve sempre, numa relação de especialidade, com a tutela da vida privada (sendo embora seguro que o direito a tal sigilo garante o direito à reserva da intimidade da vida privada) certo é que aquele tem na Constituição um tratamento específico. E, situando-se o caso no âmbito das telecomunicações, é às normas constitucionais que às telecomunicações respeitam, que, antes do mais, haverá que atender para aferir da constitucionalidade da interpretação normativa em causa».

Mais ainda, em certas circunstâncias, a mesma realidade material (por exemplo, o correio eletrónico ou similar, que aqui nos ocupa) convocará a proteção conferida por distintas normas de direitos fundamentais consagradas, na CRP, dependendo dos elementos a ela respeitantes que concretamente estejam em causa.

Como se explicou no Acórdão n.º 464/2019:

> «Como se referiu, o objeto de proteção do sigilo de comunicações, consagrado no n.º 4 do artigo 34.º da Constituição, reporta-se exclusivamente à interatividade entre utilizadores, possibilitada por meios como o correio eletrónico, o chat ou a videoconferência (utilizador-utilizador). Já os dados de internet tratados para outro tipo de interatividade, nomeadamente a do utilizador com o computador e os respetivos programas (de organização, pesquisa e seleção de informação) e a navegação intra e inter documentos publicados nas páginas web, estão fora do âmbito de proteção daquele preceito constitucional.
>
> Todavia, como o tratamento informático dessa categoria de dados permite identificar o nome, morada e outros dados de identificação do utilizador, os mesmos são considerados "dados pessoais" protegidos pelo artigo 35.º da Constituição. O n.º 2 deste artigo atribui à lei a definição do conceito de dados pessoais, o que foi feito na alínea a) do artigo 3.º da Lei n.º 67/98, de 26 de outubro: «qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social». Portanto, a informação constante dos dados de tráfego, mesmo que separada de um processo de comunicação intersubjetiva, é considerada de caráter pessoal, pois permite identificar o respetivo titular.

> Subsiste assim, em relação a essa categoria específica de dados de tráfego, a pertinência na verificação da conformidade constitucional da norma à luz do direito fundamental à autodeterminação informativa, consagrado no artigo 35.º, n.ºs 1 e 4, da Constituição.»

27. Em segundo lugar, resulta da proteção constitucional reforçada atribuída à correspondência, telecomunicações os outros meios de comunicação privada, que decorre do artigo 34.º, n.ºs 1 e 4, da CRP, que a intenção do legislador constituinte foi a de limitar significativamente a possibilidade e a amplitude quer de restrições legais, quer de *atuações restritivas* das autoridades públicas, em tais domínios.

Isto mesmo explica o Acórdão n.º 486/2009, da seguinte forma:

> «A imposição constitucional (artigo 34.º, n.º 4, da C.R.P.) duma previsão legal prévia para as técnicas de ingerência das autoridades públicas nas telecomunicações no domínio do processo penal, visa limitar ao máximo a existência de espaços de discricionariedade daquelas autoridades, numa área de elevado risco de lesão grave dos direitos e liberdades dos cidadãos, enfatizando a exigência das leis restritivas do artigo 18.º, n.º 2 e 3, da C.R.P.
>
> O legislador constituinte procurou salvaguardar simultaneamente, por um lado, a segurança e a realização da justiça, e por outro lado, os direitos e liberdades individuais do cidadão, atribuindo a arbitragem entre ambos ao legislador: as medidas limitativas daqueles direitos que as entidades públicas que se movem no processo penal podem adoptar são apenas aquelas que o legislador tenha autorizado, e não todas as que se considerem necessárias e ajustadas ao caso. A medida das agressões aos direitos fundamentais dos cidadãos no âmbito do processo penal não é definida por aquelas autoridades públicas, nos seus actos concretos de ingerência, sendo obrigatório que corresponda aos modelos e técnicas de actuação previamente estabelecidos na lei.
>
> Neste domínio essas entidades só podem fazer o que o legislador lhes tiver permitido fazer».

Em terceiro lugar, a proteção constitucional das *telecomunicações* abrange um conjunto alargado de dados sobre a comunicação humana, incluindo não apenas os dados de conteúdo – ou seja, o conhecimento sobre o conteúdo concreto das mensagens transmitidas entre emissor e destinatário – como os chamados dados de tráfego, reveladores de uma série de elementos sobre o contexto em que ocorreu o processo comunicativo. Porém, como é evidente, em caso algum a proteção conferida a qualquer tipo de *metadados* poderá ser maior, ou mais intensa, do que a que a Constituição assegura ao *conteúdo* material da comunicação – pelo contrário. Nestes termos, recusa-se, desde já, qualquer argumentação segundo a qual se afastaria, nesta sede, a aplicação da jurisprudência deste Tribunal Constitucional e do TJUE relativa a dados de tráfego, por estarem em causa dados de conteúdo.

Como pode ler-se, a este propósito no Acórdão n.º 486/2009:

> «O sigilo das telecomunicações, garantido nos termos do artigo 34.º, n.º 1, da Constituição, abrange não só o conteúdo das comunicações, mas também o tráfego como tal (V. GOMES CANOTILHO/VITAL MOREIRA, ob.cit., pág. 538 e segs.).
>
> 'O que está em causa é assegurar o livre desenvolvimento da personalidade de cada um através da troca à distância, de informações, notícias, pensamentos e opiniões, à margem da devassa da publicidade' (COSTA ANDRADE, em 'Bruscamente no verão passado..., Ano 137.º, n.º 3951, Julho-Agosto 2008, p. 339).
>
> A privacidade da comunicação, como corolário da reserva da intimidade da vida privada, abrange não apenas a proibição de interferência, em tempo real, de uma chamada telefónica, como também a impossibilidade do ulterior acesso de terceiros a elementos que revelem as condições factuais em que decorreu uma comunicação (…).
>
> Efetivamente, num Estado de Direito democrático, assiste a qualquer cidadão o direito de telefonar quando e para quem quiser com a mesma privacidade que se confere ao conteúdo da sua conversa».

E como confirmou, mais tarde, o Acórdão n.º 403/2015:

> «(…) há um largo consenso na doutrina e na jurisprudência, de resto não se conhece posição contrária, no sentido de se incluir os dados de tráfego no conceito de comunicações constitucionalmente relevante para a proibição de ingerência. Quer dizer: o âmbito de proteção do artigo 34.º, n.º 4 abrange não apenas o conteúdo das telecomunicações, mas também os dados de tráfego.
>
> (…)
>
> O Tribunal Constitucional também já teve oportunidade de se pronunciar expressamente sobre este aspeto, tendo também equiparado a proteção dos dados de tráfego à proteção constitucionalmente concedida aos dados de conteúdo. Assim, no Acórdão n.º 241/02, em que refere expressamente que 'a proibição de ingerência nas telecomunicações, para além de vedar a escuta, interceção ou vigilância de chamadas, abrange, igualmente, os elementos de informação com elas conexionados, designadamente os que no caso foram fornecidos pelos operadores de telecomunicações'. A mesma interpretação foi retomada e amplamente desenvolvida no Acórdão n.º 486/2009 (…).
>
> (…)
>
> Por tudo isso, também se entende que a área de proteção do sigilo das comunicações consagrada no n.º 4 do artigo 34.º da CRP, compreende tanto o conteúdo da comunicação como os dados de tráfego atinentes ao processo de comunicação. (…)»

28. Em quarto lugar, o desenho jurídico-constitucional da proteção conferida à *comunicação humana*, entendida em sentido lato, veda a possibilidade de restrições dos direitos fundamentais a ela atinentes, exceto quando tais restrições se situem no âmbito do *processo penal*.

Nesse sentido, entendeu-se no Acórdão n.º 403/2015:

> «17. Ao definir o campo de incidência da lei restritiva do direito à inviolabilidade das comunicações pela "matéria de processo criminal" a Constituição ponderou e tomou posição (em parte) sobre o conflito entre os bens jurídicos protegidos por aquele direito fundamental e os valores comunitários, especialmente os da segurança, a cuja realização se dirige o processo penal. Não obstante as restrições legais ao direito à inviolabilidade das comunicações que o legislador está autorizado a estabelecer deverem obedecer à ponderação do princípio da proporcionalidade, a preferência abstrata pelo valor da segurança em prejuízo da privacidade das comunicações só pode valer em matéria de processo penal. É que a não inclusão de outras matérias do âmbito da restrição do direito à inviolabilidade das comunicações, não é contrária ao plano ordenador do sistema jurídico-constitucional. Ainda que se pudesse considerar, em abstrato, que há outras matérias em que o valor da segurança sobreleva os valores próprios do direito à inviolabilidade das comunicações, a falta de cobertura normativa da restrição em matérias extraprocessuais não frustra as intenções ordenadoras do atual sistema, porque há razões político-jurídicas que estão na base da abstenção do legislador constitucional».

Explicou-se, no mesmo aresto, que pode até falar-se, nesta matéria, numa *reserva absoluta de processo criminal*:

> «De facto, a referência ao processo criminal não é apenas uma indicação teleológica, mas também a localização da restrição à proibição de ingerência numa área estruturada normativamente em termos de oferecer garantias bastantes contra intromissões abusivas. Ao autorizar a ingerência das autoridades públicas nos meios de comunicação apenas em matéria de processo penal, e não para quaisquer outros efeitos, a Constituição quis garantir que o acesso a esses meios, para salvaguarda dos valores da "justiça" e da "segurança", fosse efetuado através de um instrumento processual que também proteja os direitos fundamentais das pessoas. Porque a ingerência nas comunicações põe em conflito um direito fundamental com outros direitos ou valores comunitários, considerou-se que a restrição daquele direito só seria autorizada

para realização dos valores da justiça, da descoberta da verdade material e restabelecimento da paz jurídica comunitária, os valores que ao processo criminal incumbe realizar. Assim, remeteu para o legislador processual penal a tarefa de "concordância prática" dos valores conflituantes na ingerência nas comunicações privadas: por um lado, a tutela do direito à inviolabilidade das comunicações; por outro, a viabilização da justiça penal. Na verdade, como escreve Figueiredo Dias, «o processo penal é um dos lugares por excelência em que tem de encontrar-se a solução do conflito entre as exigências comunitárias e a liberdade de realização da personalidade individual» (cfr. Direito Processual Penal, Coimbra Editora, 1974, pág. 59).

Assim, a referência ao processo criminal, encontrando-se estreitamente associada à Constituição, onde se detetam normas diretamente atinentes a essa matéria e que condensam os respetivos princípios estruturantes (artigo 32.º) - a ponto de se falar numa constituição processual criminal -, tem um sentido hermenêutico inequívoco, não podendo deixar de ser entendido como a "sequência de atos juridicamente preordenados praticados por pessoas legitimamente autorizadas em ordem à decisão sobre a prática de um crime e as suas consequências jurídicas"».

29. Nestes termos, o estado da arte, no que respeita à densificação jurisprudencial dos direitos fundamentais ao sigilo das comunicações intersubjetivas (nos termos do artigo 34.º da CRP) e à autodeterminação informativa (à luz do artigo 35.º da Constituição) pode ser resumido com recurso à síntese lograda do Acórdão n.º 464/2019. Afirma-se, no aresto, quanto ao primeiro:

«Em suma, o artigo 34.º da Constituição tem por propósito consagrar e proteger o direito fundamental à inviolabilidade do domicílio e da correspondência, ou seja, e *prima facie*, a liberdade de manter uma esfera de privacidade e sigilo, livre de interferência e ingerência estadual, quer no que respeita ao domicílio, quer – sendo esta a dimensão relevante para o caso *sub iudice* - quanto à comunicação. É, aliás, entendimento doutrinal sedimentado que o âmbito de proteção da norma constitucional abrange todos os meios de comunicação individual e privada, e toda a espécie de correspondência entre pessoas, em suporte físico ou eletrónico, incluindo não apenas o conteúdo da correspondência, mas o tráfego como tal (espécie, hora, duração, intensidade de utilização), excluindo-se apenas a categoria residual de dados pessoais, isolados de qualquer processo de comunicação, efetivo ou tentado.

(...)

Assim, importará considerar que o n.º 4 do artigo 34.º da Constituição protege tanto o processo comunicativo quanto o conteúdo da comunicação, sempre que – mas apenas quando – esteja em causa um efetivo processo comunicativo. Ou seja, terá de ter havido, pelo menos por uma das partes, a consciência e a vontade de "participar na transmissão à distância de dados ou notícias", mesmo que a comunicação não se tenha completado, por ausência ou rejeição de resposta pela outra parte.

Posição semelhante encontra-se na doutrina e jurisprudência alemãs, a propósito do âmbito de proteção do artigo 10.º da Lei Fundamental: «*Desenha-se aqui, no âmbito do Artigo 10.º, um nível diferenciado de proteção. O círculo mais estreito é constituído pelo núcleo essencial da privacidade, que é garantida não apenas dentro da habitação, mas também na comunicação à distância. De forma menos intensiva, mas também com um nível elevado de proteção, é protegido o conteúdo da comunicação, contra escutas, leituras ou outras formas de intromissão. No que respeita aos dados sobre as circunstâncias do processo comunicativo, designadamente, os dados de conexão, o Tribunal Constitucional federal enfatiza a importância da proteção efetiva dos direitos fundamentais*» (Mangoldt/Klein/Starck, GG – Grundgesetz Kommentar, Band 1, 7. Auflage, C. H. Beck, 2018, Art. 10, Abs. 2, 75, p. 1084).

Note-se, por fim, que a relevância comunicacional dos dados de tráfego não os descaracteriza enquanto dados pessoais ligados à privacidade dos indivíduos e ao livre desenvolvimento da respetiva personalidade – bens jurídicos tutelados pelo artigo 26.º, n.º 1, da Constituição –, tanto mais que o seu tratamento informático e acesso por terceiros atinge o direito de cada um controlar as informações que lhe dizem respeito, ou seja, o seu direito à autodeterminação informativa, consagrado no artigo 35.º da Constituição (cf. infra o n.º 10).»

Por sua vez, quanto ao direito à autodeterminação informativa, explica-se no Acórdão n.º 464/2019:

«A autodeterminação comunicativa, estando correlacionada com a autodeterminação informativa e sobrepondo-se parcialmente à mesma, todavia, não deixa de dela se distinguir.

Como se deixou claro no Acórdão n.º 403/2015:

«O objeto de proteção do direito à autodeterminação comunicativa reporta-se a comunicações individuais efetivamente realizadas ou tentadas e só essas é que estão cobertas pelo sigilo de comunicações. Naquele outro direito protege-se as informações pessoais recolhidas e tratadas por entidades públicas e privadas, cuja forma de tratamento e divulgação pode propiciar ofensas à privacidade das pessoas a que digam respeito» (cf. o respetivo ponto 13)

(...)

No âmbito da utilização da informática, as normas contidas no artigo 35.º da CRP reconhecem «o direito a conhecer a informação que sobre cada um de nós é tratada, e que se traduz, no essencial, no direito de saber que dados pessoais estão a ser recolhidos, utilizados conservados, comunicados e para que finalidade, e ainda por quem estão a ser tratados – o quê, por quem, para quê? – de modo a permitir aos cidadãos deter ou retomar o controlo sobre os seus dados. A este conjunto de pretensões jurídico-subjetivas, refletidas no n.º 1 do artigo 35.º, a doutrina portuguesa, por inspiração germânica, chamou direito à autodeterminação informativa, o qual, em certa medida, abrange ainda o direito à retificação ou atualização dos dados, ainda que esta seja já uma dimensão subjetiva que pressupõe a concretização daquelas dimensões» (cf. Filipa Urbano Calvão. «O direito fundamental à proteção dos dados pessoais e a privacidade 40 anos depois», Jornadas nos quarenta anos da Constituição da República Portuguesa, Impacto e Evolução, Universidade Católica Editora, Porto, 2017, p. 89).

(...)

Acresce que as pessoas têm não apenas o direito de saber o que a seu respeito consta dos registos informáticos, mas também o direito de que esses dados sejam salvaguardados contra a devassa ou difusão. Por sua vez, este último direito engloba vários direitos específicos: (a) a proibição de acesso de terceiros a dados pessoais (artigo 35.º, n.º 4, da Constituição); (b) proibição da interconexão de ficheiros de bases e bancos de dados pessoais (artigo 35.º, n.º 2, da Constituição).

Isto mostra claramente que a consagração constitucional da proteção de dados pessoais constitui um instrumento do livre desenvolvimento da pessoa humana numa sociedade democrática e uma condição para o gozo da liberdade e da afirmação da identidade pessoal. Como referem Gomes Canotilho e Vital Moreira, «o conjunto de direitos fundamentais relacionados com o tratamento informático de dados pessoais arranca de alguns «direitos-mãe» em sede de direitos, liberdades e garantias. É o caso do direito à dignidade da pessoa humana, do desenvolvimento da personalidade, da integridade pessoal e da autodeterminação informativa.

(...)

Na forma específica de proibição de acesso por terceiros, o direito à proteção de dados apresenta-se como um direito de garantia de um conjunto de valores fundamentais individuais – a liberdade e a privacidade – bens jurídicos englobados na autodeterminação individual, abrangendo duas dimensões: a dimensão negativa ou de abstenção do Estado de ingerência na esfera jurídica dos cidadãos e a dimensão positiva enquanto função ativa do Estado para prevenir tal ingerência por parte de terceiros. Na vertente da proibição de tratamento de dados pessoais suscetíveis de gerar discriminação, este direito fundamental está ainda diretamente ligado à garantia da igualdade entre os cidadãos, «(…) demonstrando que a proteção de dados pessoais não tem em si mesmo apenas um objetivo de tutela da privacidade, mas também uma importante função social de garantia da igualdade» (cf. Filipa Urbano Calvão, ob. cit., pág. 90)».

Feito este excurso jurisprudencial, fica razoavelmente evidente qual o *standard* de proteção que o Tribunal Constitucional é agora chamado a articular, na específica sede do *processo penal*, e no âmbito da

problemática da divisão de competências entre Ministério Público e Juiz.

30. Quanto ao segundo eixo acima considerado, respeitante à repartição de competências entre Juiz e Ministério Público, no âmbito do processo penal, este Tribunal tem mantido uma linha coerente, ao longo de décadas, e que pode resumir-se no seguinte segmento do Acórdão n.º 7/87: "*a intervenção do juiz (...) justifica-se "para salvaguardar a liberdade e a segurança dos cidadãos no decurso do processo-crime e para garantir que a prova canalizada para o processo foi obtida com respeito pelos direitos fundamentais*"". Ou seja, nestes termos, a exigência de *intervenção judicial* no inquérito, em relação a atos que configurem *intervenções restritivas* na esfera dos direitos fundamentais, define-se, desde os momentos iniciais da jurisprudência constitucional, como pilar incontornável da arquitetura sistémica que se foi construindo para o processo penal português.

Esta posição é consonante com vários posicionamentos doutrinais, com relevo para o de Figueiredo Dias, que ensina que os "*atos processuais singulares que, na sua pura objetividade externa, se traduzem a ataques a direitos, liberdades e garantias das pessoas constitucionalmente protegidos" devem inscrever-se na competência do Juiz de Instrução Criminal durante o inquérito*" (cfr. J. FIGUEIREDO DIAS, "Sobre os sujeitos processuais no novo Código de Processo Penal", in *O Novo Código de Processo Penal*, Almedina, Coimbra, 1988, p. 16, e ainda NUNO BRANDÃO, "O controlo de proibições de prova pelo juiz de instrução no decurso do inquérito", in *Revista Portuguesa de Ciência Criminal*, ano 29, n.º 1, janeiro-abril de 2019, p. 50).

A articulação entre a ação do Ministério Público e a do Juiz de Instrução Criminal, no respeito pelos respetivos estatutos jurídico-constitucionais, no sentido de encontrar soluções que permitam, na prática, conjugar o princípio do acusatório e a competência exclusiva do juiz para a prática de atos que diretamente contendem com direitos fundamentais, foi, naturalmente, objeto de muitíssimas pronúncias.

Assim, disse-se, por exemplo, no Acórdão n.º 23/90:

> «Por outras palavras e no concreto caso, o n.º 4 do artigo 32º 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").
>
> Intervenção do juiz que vale - e só vale no âmbito do núcleo da garantia constitucional.
>
> Assim ocorre em toda a fase de inquérito ao Ministério Público confiada pelo CPP actual, compreendendo o conjunto de diligências que visam investigar a existência de um crime, determinar os seus agentes e a responsabilidade deles, descobrir e recolher provas em ordem à decisão sobre a acusação (artigo 262º, n.º 1), justificando-se a intervenção do juiz-garante sempre que afectado aquele núcleo - consoante o elenco de situações descritas nos artigos 268.º e 269.º».

E reiterou-se, mais de uma década depois, no Acórdão nº 395/2004 (posição que seria ainda reafirmada no Acórdão n.º 67/2006):

> «[…] o reconhecimento da competência do Ministério Público para dirigir o inquérito não poderá ser visto desligadamente da autonomia que a Lei Fundamental lhe reconhece. Deste modo, caber-lhe-á a competência para decidir e proceder à prática dos actos de investigação ou de recolha das provas, com a única ressalva dos que importem ofensa ou restrição de direitos fundamentais que carecem, segundo os casos, de ser ordenados ou autorizados ou até realizados exclusivamente pelo juiz (cfr. art.ºs 268º e 269º do CPP).
>
> Mesmo no caso destes últimos actos, não deixa de ser reconhecido ao Ministério Público um poder de impulso processual ad actum, reconhecendo-se-lhe a faculdade de requerer a sua autorização e/ou a sua prática ao juiz competente».

Por estas razões, nas situações concretas em que evidentemente estava em causa uma intervenção restritiva das autoridades públicas em matéria de direitos fundamentais, este Tribunal não

hesitou em afirmar a necessidade incontornável de intervenção *prévia* do Juiz de Instrução Criminal, como fez nos Acórdãos n.º 155/2007 (que em seguida se cita) e n.º 228/2007 (que reiterou a decisão anterior sobre colheita coativa de vestígios biológicos de um arguido para determinação do seu perfil genético):

> «Face ao exposto, só pode concluir-se que, contendendo o acto em causa, de forma relevante, com direitos, liberdades e garantias fundamentais, 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, da prévia autorização do juiz de instrução. E, nem se diga que será suficiente, como aconteceu nos presentes autos, uma intervenção a posteriori daquele juiz, tomada na sequência de requerimento apresentado após a decisão do Ministério Público que determinou a realização dos exames que agora estão em causa, uma vez que a mesma não poderia desfazer a restrição de alguns dos direitos (v.g., o direito à integridade física ou o direito à reserva da vida privada) entretanto irremediavelmente afectados com a medida».

31. Mais recentemente, no Acórdão n.º 387/2019, também especificamente respeitante à matéria que nos ocupará – a repartição de competências entre o Ministério Público e o Juiz de Instrução Criminal que resulta de uma interpretação das disposições de processo penal à luz do artigo 32.º, n.º 4, da CRP –, após um importante percurso argumentativo, esclarecedor da interpretação constitucional sobre o princípio da *reserva de juiz,* traça-se a linha divisória da seguinte forma:

> «Antes do mais cumpre notar que entre as reservas de juiz no inquérito para intervenção restritiva em direitos fundamentais que se encontram previstas no CPP é possível distinguir a reserva para atos materiais (reserva de atos a praticar pelo juiz) e a reserva de atos decisórios (reserva de decisão judicial). Dentro dos atos decisórios é possível identificar a ordem judicial (ex. artigo 179.º, n.º 1, CPP), a autorização judicial (ex. artigo 179.º, n.º 1, CPP); a concordância judicial (ex. artigo 281.º, n.º 1, do CPP) e a confirmação (ou convalidação) judicial (ex. artigo 174.º, n.º 6, ou artigo 252.º, n.º 3, CPP ou artigo 4.º, n.º 5 da Lei n.º 5/2002, de 11 de janeiro).
>
> Em função do momento da intervenção do juiz podemos distinguir reservas prévias (primárias) e reservas subsequentes (secundárias). As primeiras traduzem a obrigatoriedade de intervenção do juiz em momento anterior à realização da medida. Nas segundas, diferentemente, o juiz intervém já depois do início da sua execução.
>
> Na configuração que constitucionalmente tomam, as reservas de juiz apresentam-se como concretizações dos direitos fundamentais e encontram a sua razão de ser no estatuto de independência que os juízes têm e na distância que mantêm relativamente à atividade investigatória.
>
> Subjacente à transferência de competências para autorizar certas medidas de investigação do titular do inquérito para um juiz, encontra-se a garantia de neutralidade judicial. A independência da magistratura judicial e o seu maior distanciamento em relação à atividade investigatória, conferem ao juiz de instrução uma maior disponibilidade funcional e estatutária para, com objetividade, decidir os limites toleráveis do sacrifício dos direitos fundamentais em favor do interesse da realização da justiça penal».

Por fim, no Acórdão n.º 121/2021, recordando a jurisprudência anterior, faz-se a seguinte síntese:

> «o Ministério Público emerge do desenho jurídico-constitucional como um órgão de justiça independente e autónomo que, entre outras atribuições, exerce "*a ação penal orientada pelo princípio da legalidade*" (artigo 219.º, n.º 1, da CRP). A partir desta atribuição constitucional específica, combinada com o princípio do acusatório, recorta-se o estatuto do Ministério Público enquanto único sujeito processual com intervenção *necessária* no processo (já que este pode ser arquivado sem que tenha ocorrido qualquer constituição de arguido ou intervenção judicial) e poder exclusivo de direção do inquérito. Alguma doutrina refere-se mesmo a uma *reserva de Ministério Público no processo penal*, que impõe o respeito pelas funções próprias e pela autonomia daquele, em

termos que determinam a exclusão, por violação da Constituição, de qualquer solução legal que coloque "*o Ministério Público na dependência processual do juiz*" (neste sentido, veja-se, P. Dá Mesquita, *Direcção do Inquérito Penal e Garantia Judiciária*, Coimbra Editora, Coimbra, 2003, p. 51-52).

Neste contexto, a intervenção do Juiz de Instrução Criminal em sede de inquérito deve pautar-se por um princípio da intervenção enquanto *juiz das liberdades* (e não como juiz de investigação), respeitando o modelo constitucional de divisão de funções entre a magistratura judicial e a magistratura do Ministério Público (cfr. artigos 32.º, n.º 4 e 5, e 219.º da CRP). Por isso, o momento adequado para apreciação jurisdicional dos atos do Ministério Público – que não estão, como é evidente, a ela imunes – terá lugar, em regra, e dentro da arquitetura do sistema, *na fase de instrução*, de acordo com os preceitos legais que a regem. Esta deve funcionar como um mecanismo de comprovação judicial da decisão de deduzir acusação ou de encerrar o inquérito, devendo igualmente ser de controlo exclusivo pelo Juiz de Instrução Criminal, cuja intervenção, limitada, na prévia fase de inquérito, lhe permite conduzi-la sem pré-juízos decisivos.

Assim, um excessivo protagonismo do Juiz de Instrução Criminal, *durante o inquérito*, que lhe atribuísse um âmbito de competência alargado, permitindo a reapreciação jurisdicional de todos, ou quase todos, os atos praticados pelo Ministério Público (sempre sem prejuízo de apreciação em sede de instrução, segundo as regras próprias dessa fase processual), significaria uma inversão do paradigma constitucionalmente estabelecido. De facto, isso equivaleria, em grande medida, a entregar a direção do inquérito ao Juiz, já não mais *juiz das liberdades*, mas sim *juiz da acusação*».

D) Questão de constitucionalidade

32. O objeto do presente pedido de fiscalização da constitucionalidade é constituído pela norma do artigo 5.º do Decreto n.º 167/XIV, na parte em que altera o artigo 17.º da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime).

Reproduz-se novamente, neste ponto, para maior facilidade argumentativa o teor da nova versão do artigo 17.º da Lei do Cibercrime:

«Artigo 17.º

Apreensão de mensagens de correio eletrónico ou de natureza semelhante

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

julgado da decisão que puser termo ao processo.

6. No que se não encontrar previsto nos números anteriores, é aplicável, com as necessárias adaptações, o regime da apreensão de correspondência previsto no Código de Processo Penal».

A solução legal consagrada por estas normas cria, assim, a possibilidade de apreensão de mensagens de *correio eletrónico*, que sejam conhecidas no decurso de uma medida de investigação criminal – a pesquisa informática – validamente determinada, por despacho da *autoridade judiciária competente*. Tendo em consideração o que acima se disse acerca do enquadramento da medida de apreensão de mensagens de correio eletrónico ou de natureza semelhante no contexto das disposições processuais penais da Lei do Cibercrime, levantam-se fundadas dúvidas interpretativas sobre se esta funcionará como regime regra de apreensão de tais mensagens, ou como regime subsidiário, para situações concretamente determinadas, aplicando-se, no mais, o disposto no artigo 179.º do Código de Processo Penal. De qualquer forma, sempre se poderá dizer que as normas questionadas se aplicarão a *todas* as mensagens encontradas no decurso de pesquisas informáticas, não atuando apenas – com exceção, parcial, do disposto no novo n.º 2 do artigo 17.º – em circunstâncias de excecional urgência ou perigo na demora que exijam uma atuação cautelar. Nestes termos, e independentemente da resposta a esta dúvida, o certo é que é expectável que o regime jurídico questionado venha a aplicar-se a um número significativo de apreensões de correio eletrónico, na medida em que não é inverosímil que uma parte significativa das pesquisas a sistemas informáticos venham a revelar a existência de mensagens de correio eletrónico ou de natureza semelhante.

Além disso, não decorre da Lei do Cibercrime qualquer delimitação do âmbito de aplicação das suas disposições processuais penais que a reserve, *em termos inequívocos*, à investigação de ações criminosas de especial gravidade, ou para as quais a lei substantiva preveja uma moldura penal superior a determinados limites mínimos. Chama, sobretudo, a atenção, a ausência de norma paralela à constante do artigo 9.º da Lei n.º 32/2008, que prevê, em relação à transmissão às autoridades públicas de dados de tráfego armazenados por fornecedores de serviços de comunicações eletrónicas ou de uma rede pública de comunicações que a mesma "*só pode ser autorizada, por despacho fundamentado do juiz de instrução, 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 no âmbito da investigação, deteção e repressão de crimes graves*".

33. Por outro lado, as normas em causa aplicam-se às mensagens que forem encontradas ou armazenadas quer no sistema informático objeto de pesquisa, quer "*noutro a que seja permitido o acesso legítimo a partir do primeiro*", alargando significativamente o perímetro em que podem estar localizadas. Além disso, as normas questionadas nada dizem sobre a natureza "aberta" ou "fechada" das referidas mensagens, não sendo, dessa forma, inequívoca e inteiramente determinada a sua aplicação apenas a comunicações já efetuadas e não, também, a fluxos comunicacionais que possam estar ainda a decorrer. De qualquer forma, e como se deu nota no ponto de enquadramento do objeto do pedido, a distinção, no âmbito das mensagens de correio eletrónico e similares, entre correio "aberto" e "fechado" levanta dificuldades técnicas e dogmáticas, e é, hoje, crescentemente rejeitada, caminhando-se para um regime jurídico-constitucional tendencialmente único, aplicável a este tipo de comunicação.

Além disso, a Lei n.º 41/2004, que transpõe para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, define, no seu artigo 2.º, alínea b), *correio eletrónico* como "*qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha*", o que parece adensar a dúvida sobre eventual paralelismo entre este tipo de mensagens e a correspondência postal já aberta.

34. O correio eletrónico é, pois, uma realidade complexa, convocando elementos atinentes à proteção jurídica da correspondência postal, bem como elementos relativos à tutela das telecomunicações, como se confirma pelas hesitações, divergências doutrinais, e evolução das conceções dogmáticas e jurisprudenciais sobre a aplicação a este tipo de mensagens das disposições processuais penais relativas quer à apreensão de correspondência, quer à apreensão de documentos, quer, ainda, à intercetação de telecomunicações.

De toda a maneira, é importante notar que está em causa, na apreensão das mensagens de correio eletrónico ou de natureza semelhante, acima de tudo, o acesso a *dados de conteúdo*, em termos análogos aos que estão em causa na correspondência; porém, inclui-se igualmente o acesso a *dados de tráfego*, em termos muito mais amplos do que estão em causa na comunicação postal. Efetivamente, a simples visualização de uma "caixa de correio eletrónico", sem que sequer se abra cada uma das mensagens individuais aí gravadas, pode permitir o conhecimento não apenas de elementos respeitantes à concreta comunicação ou mensagem (como, por exemplo, o "assunto"), como também de elementos relativos ao emissor e destinatário das mensagens, número de interações comunicativas, suas data e hora, volume de dados transmitidos, ou IP de origem, que se configuram como dados de tráfego. Ou seja, se no caso de apreensão de correspondência postal passa a ser do conhecimento das autoridades o remetente, o destinatário e a data do carimbo de correio, no caso do correio eletrónico a informação de tráfego disponível é bastante mais vasta, sendo possível saber, por exemplo, a data e hora específicas a que um e-mail foi enviado, se continha, ou não, documentos anexos, se se dirigia a mais destinatários (e quais) e se constituiu resposta a ou reencaminhamento de mensagens anteriores.

Por outro lado, é verosímil pensar que, em boa parte dos casos, a escolha das mensagens de correio eletrónico a apresentar ao juiz, para o controlo *ex post* previsto no n.º 4 da nova versão artigo 17.º da *Lei do Cibercrime*, exigirá algum tipo de pré-seleção por parte do Ministério Público, com recurso não só a dados de tráfego (emissor, destinatário), mas também a buscas através de palavras-chave que permitam delimitar o conjunto de mensagens relevantes através do seu assunto ou de trechos de conteúdo significativos. Nestes termos, e se é verdade que a intervenção nos direitos fundamentais aqui em causa não se transformou, por força das normas questionadas, num *espaço livre de controlo jurisdicional*, tal não evitará, porém, eventuais apreensões abusivas, nem a tomada de conhecimento indevida de dados de conteúdo e de tráfego relativos ao correio eletrónico de eventuais arguidos ou de terceiros, por parte do Ministério Público ou dos Órgãos de Polícia Criminal. Tais intervenções no domínio de direitos fundamentais não são passíveis de integral reparação, quando abusivas – ao contrário do que acontece, por exemplo, na maioria dos casos, com a apreensão de objetos, que podem ser devolvidos incólumes ao legítimo proprietário –, na medida em que a violação de privacidade que podem implicar, quer quanto à violação do sigilo das comunicações, quer quanto à reserva de dados pessoais, não pode ser desfeita. O que o Ministério Público ou o Órgão de Polícia Criminal atuante viu, indevidamente, não pode deixar de ser visto, mesmo que a informação não seja junta aos autos.

35. O n.º 2 do da versão questionada do artigo 17.º da *Lei do Cibercrime* consagra, como acima se deu nota, um regime investigatório especial, com uma parte cautelar, nos termos do qual o Órgão de Polícia Criminal pode efetuar as apreensões referidas no número anterior, sem prévia autorização da autoridade judiciária. Essa intervenção é possível, como já se referiu, "*no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 15.º, bem como quando haja urgência ou perigo na demora*", (sublinhado nosso), devendo ser validada *pela autoridade judiciária* no prazo máximo de 72 horas. Desta forma, na verdade, apenas a segunda parte da norma, que menciona a *urgência ou perigo na demora* estabelece um regime verdadeiramente cautelar, que justifique, por razões preventivas, a apreensão das mensagens de correio eletrónico sem intervenção judicial prévia. Os casos em que apenas esteja em causa "*pesquisa informática legitimamente ordenada e executada nos termos do artigo 15.º*" consagram uma regulamentação paralela à prevista no n.º 1 da versão ora questionada do artigo 17.º da *Lei do Cibercrime*, nos termos da qual, em fase de inquérito, se o Ministério Público tiver legitimamente ordenado a

pesquisa, também os Órgãos de Polícia Criminal podem, por si só, efetuar a apreensão, sendo esta posteriormente validada pelo próprio Ministério Público, sem *intervenção necessária* do Juiz de Investigação Criminal.

Assim, para a maioria das situações que cabem no seu âmbito de aplicação, as normas questionadas desenham um *regime regra*, que regerá a apreensão de mensagens de correio eletrónico ou de natureza similar, em condições de normalidade e previsibilidade do decurso do processo penal. É neste contexto que deverá avaliar-se o potencial de afetação dos direitos constitucionais potencialmente atingidos, nos termos que em seguida se explicarão.

36. Como se foi deixando antever, os direitos fundamentais potencialmente afetados pelas normas questionadas são os direitos à inviolabilidade da correspondência e das comunicações (consagrado no artigo 34.º, n.ºs 1 e 4, da CRP), e à proteção dos dados pessoais no âmbito da utilização da informática (nos termos do artigo 35.º, n.ºs 1 e 4, da CRP), enquanto refrações específicas do direito à reserva de intimidade da vida privada, (consagrado no artigo 26.º, n.º 1, da Constituição).

No caso do direito à inviolabilidade da correspondência e das comunicações, o n.º 1 do artigo 34.º da Constituição consagra a inviolabilidade do sigilo da correspondência e dos outros meios de comunicação privada, dispondo o seu n.º 4 uma *regra constitucional* específica, nos termos da qual "[é] proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal". Trata-se, como se afirmou, de uma refração do direito geral à reserva de intimidade da vida privada, consagrado no artigo 26.º, n.º 1, da Constituição.

No caso do direito à proteção dos dados pessoais no âmbito da utilização da informática, nos termos em que a jurisprudência constitucional o recortou, comporta, nos termos do artigo 35.º da Constituição *um direito fundamental à autodeterminação informativa,* que confere a cada pessoa a faculdade de controlar a informação disponível a seu respeito, no plano do acesso aos dados, o direito à sua contestação e ratificação, atualização e eliminação, bem como o direito a que esse dados pessoais sejam salvaguardados contra a devassa ou difusão, por parte de entidades públicas e privadas; assume especial relevância, neste plano, o conjunto de exigências jurídico-constitucionais relativas à possibilidade e finalidade de acesso legítimo a dados pessoais, entre as quais se contam o respeito pelos princípios da *adequação e proporcionalidade*.

37. A proteção constitucional conferida à *correspondência privada* compreende *todas* as variantes de correspondência entre indivíduos, desde as formas tradicionais de correspondência postal - cartas, postais, telegramas – até ao correio eletrónico, entendido como tráfego de informação privada, sob a forma escrita, figurativa ou equivalente, entre destinatários definidos e apenas acessível por estes, transmitido através de um suporte de *internet*. Tutela equivalente é conferida, para efeitos de aplicação do n.º 4 do artigo 34.º, às *telecomunicações*, envolvendo telefonemas, mensagens de voz, conversas por via de VoIP e similares, bem como, em geral, a quaisquer formas de *comunicação humana*, de caráter privado. Efetivamente, a diversidade das formas de transmissão da informação privada e dos respetivos suportes não justifica uma diferença de tutela jusconstitucional, na medida em que esta visa garantir, do ponto de vista *material*, a possibilidade de comunicação privada, enquanto refração do interesse individual na reserva de intimidade da vida privada.

No que se refere à extensão da proteção concedida por este direito fundamental, para além da garantia do *sigilo* da correspondência e de outros meios de comunicação privada, a Constituição protege igualmente os cidadãos contra toda a *ingerência* das autoridades públicas nesses domínios, embora ressalve – com grande importância, como se verá, para a presente análise –, os casos previstos na lei em matéria de processo criminal. A ingerência tanto pode consistir numa forma de acesso ao conteúdo da mensagem ou ato comunicacional – os chamados «dados de conteúdo» – como também aos elementos

funcionais da comunicação, designadamente direção, destinatários, data, via e percurso de uma determinada mensagem – os chamados «dados de tráfego» -, estando ambos, como se explicou, em causa no que respeita às normas questionadas.

38. As normas *sub judice* permitem a ingerência na correspondência eletrónica, podendo também, como se procurou mostrar, possibilitar o conhecimento de uma série de dados pessoais que, mesmo que não se entendam respeitantes a um processo de comunicação em curso, sempre serão protegidos pelo direito fundamental à proteção de dados no domínio da utilização da informática, previstos no artigo 35.º, n.ºs 1 e 4, da CRP, enquanto dimensão específica da reserva de intimidade da vida privada, tutelada pelo artigo 26.º, n.º 1, da Lei Fundamental.

Na verdade, as operações necessárias à apreensão de correio eletrónico ou de mensagens de natureza semelhante no decurso de uma pesquisa a um sistema informático importam um risco considerável — senão mesmo a inevitabilidade — de acesso a dados pessoais protegidos, relativos à correspondência do utilizador, bem como a dados de tráfego e de conteúdo abrangidos pela garantia constitucional de inviolabilidade do sigilo. Na generalidade dos casos, é, pois, dificilmente evitável que, no decurso da pesquisa a um computador, o investigador depare com o elenco das últimas mensagens de correio eletrónico e de natureza similar recebidas, identificadas a partir de elementos — como o remetente, o assunto e a data de receção — que estão inequivocamente compreendidos no âmbito da garantia constitucional do sigilo na correspondência. Em algumas situações, pode mesmo ocorrer que o conteúdo da mensagem se esgote, literal ou substancialmente, na identificação do respetivo assunto, pelo que os dados acessíveis incluirão *todos* os dados de conteúdo relevantes. Por esta razão, o regime do novo artigo 17.º da *Lei do Cibercrime* constitui, conjuntamente com o artigo 16.º, o *núcleo duro* da disciplina normativa do acesso a dados de natureza informática no âmbito do processo penal, eliminando – ao contrário, precisamente, do artigo 16.º - a exigência de intervenção primária do Juiz de Instrução Criminal, bem como a necessidade de este ser o primeiro a tomar conhecimento do conteúdo das mensagens apreendidas.

Ora, num universo social em que os sistemas informáticos adquirem progressivamente um papel mais presente na atividade humana, assumindo-se como instrumentos de comunicação e repositórios de informação de natureza pessoal e profissional, a pesquisa do seu conteúdo constitui invariavelmente uma intrusão na vida privada. No caso das mensagens de correio eletrónico, o acesso indiscriminado permite facilmente traçar um retrato fiel, e muito completo, da vida do utilizador em causa, agregando informação atinente aos distintos planos da vida de cada pessoa – as distintas *máscaras* com que cada um se apresenta no plano social, laboral e familiar. O potencial ablativo de liberdade e a gravidade da intromissão na esfera privada – e até na esfera íntima – da pessoa que decorre da simples visualização da respetiva caixa de correio eletrónico são, pois, de tal forma significativos, que devem mobilizar-se, neste campo, as mais intensas garantias que a Constituição confere à inviolabilidade das comunicações e à privacidade dos dados pessoais no domínio da informática; é essencial assegurar o cumprimento do dever estadual de abstenção, ou não ingerência, nestes domínios, a não ser em casos objetiva e rigorosamente delimitados, claramente justificados, e mediante atuação de órgãos que assegurem uma intervenção isenta e imparcial, e um elevado grau de proteção dos direitos fundamentais afetados. Efetivamente, a potencial amplitude das lesões de direitos fundamentais é, nesta matéria, muito elevada, "*também aqui, pela mesma razão da continuidade da presença do computador na vida contemporânea, tanto a nível individual como coletivo. Para um número exponencialmente crescente de pessoas, quase tudo passa pelo computador: desde os dados aparentemente mais anódinos (compras, vendas, planificação de negócios, contabilidade, trabalhos feitos, movimentos bancários, músicas, etc.), aos mais sensíveis (saúde, religião, correspondência, fotografias, etc.). Para muitos, o computador funciona como caderno diário, biblioteca, arquivo, repositório de gestos, ações, planos, gostos, etc. Por ser assim, o disco duro do computador oferece um espelho dos interesses pessoais, inclinações gostos, da situação económica e familiar, da saúde física e psíquica, dos valores, dos modelos de conduta e das normas interiorizadas*" (M. DA COSTA ANDRADE, *"Bruscamente, no Verão passado", a Reforma do Código de Processo Penal – Observações críticas sobre*

uma lei que podia e devia ter sido diferente, Coimbra Editora, 2009, p. 167). Todas estas observações valem, como é fácil compreender, para as mensagens de correio eletrónico e de natureza similar, pelo que se impõe todo o cuidado possível na apreciação de intervenções legislativas de natureza restritiva, como a que as normas em causa inequivocamente configuram.

39. Nestes termos, e atendendo a tudo o que anteriormente se explicou, o Tribunal Constitucional é, agora, confrontado, com a seguinte problemática:

- É admissível uma restrição aos direitos fundamentais ao *sigilo da correspondência e dos outros meios de comunicação privada* (consagrado no artigo 34.º, n.ºs 1 e 4, da CRP), à *proteção dos dados pessoais*, no domínio da utilização da informática (que decorre da norma do artigo 35.º, n.ºs 1 e 4, da CRP), núcleos de *reserva de intimidade da vida privada* especifica e intensamente tutelados pela Lei Fundamental, como a que se configura no regime jurídico instituído pelos preceitos questionados?

- Admitindo-se a possibilidade de restrição, abstratamente considerada, e situando-se a mesma, como é o caso, no âmbito do *processo penal*, a divisão de competências entre o Ministério Público e o Juiz de Instrução Criminal, em fase de inquérito, que resulta do regime analisado, cumpre as imposições jurídico-constitucionais relevantes, designadamente, o disposto no artigo 32.º, n.º 4, da CRP, quanto à competência exclusiva do Juiz de Instrução Criminal para a prática de atos que diretamente contendem com direitos fundamentais, e os princípios da necessidade e proporcionalidade (nos termos do artigo 18.º, n.º 2, da CRP)?

Como ao longo do texto se procurou esclarecer, a solução para a presente questão de inconstitucionalidade encontrar-se-á na interseção dos parâmetros constitucionais respeitantes à proteção do sigilo da correspondência, das telecomunicações e dos dados informáticos, da privacidade, e das garantias em sede de processo penal (nomeadamente, quanto à prática de atos instrutórios que se prendam diretamente com os direitos fundamentais), nos termos dos artigos 34.º, n.ºs 1 e 4, 26.º, n.º 1, 35.º, n.ºs 1 e 4, e 32.º, n.º 4, da CRP.

Vejamos.

40. No que respeita à proteção do sigilo da correspondência e das telecomunicações – ou seja, à tutela especial que a CRP dispensa à *privacidade* no domínio da *comunicação humana* –, resulta da jurisprudência constitucional acima mencionada que se configura, no âmbito de proteção conferido por esses direitos fundamentais, uma *reserva absoluta do processo penal*, surgindo este como o único domínio da vida comunitária em que o legislador constituinte entendeu haver fundamento bastante para permitir *restrições legais* e *intervenções restritivas* por parte das autoridades públicas.

Assim, a referência constitucional ao *processo criminal* remete para uma teleologia clara, que deve presidir ao desenho de tais restrições legais, numa área jusconstitucionalmente imune, em muitos outros planos, a intromissões. Ou seja, quando prevê uma tal delimitação para a possibilidade de ingerência das autoridades públicas nos meios de comunicação, a CRP dá ao intérprete indicações não apenas sobre a *finalidade* das restrições admissíveis – que tem de ser, incontornavelmente, a salvaguarda dos valores da justiça, da segurança e da legalidade democrática, que com o processo penal se pretende alcançar –, mas também sobre o *modo* de o fazer. Ora, esse modo, atento o disposto no artigo 32.º da CRP, não pode deixar de assegurar os direitos fundamentais das pessoas, as garantias de defesa e a presunção de inocência dos arguidos, e a proibição de provas obtidas mediante intromissão *abusiva* na vida privada, no domicílio, na correspondência ou nas telecomunicações, bem como a competência de *um juiz* para a prática dos *atos instrutórios que se prendam diretamente com os direitos fundamentais*. A amplitude da restrição constitucionalmente admissível deve, pois, encontrar-se na confluência de todas estas exigências. Assim, considerando o horizonte significante que a limitação ao *processo penal* das restrições às comunicações

privadas comporta, e o contexto aplicativo que tal referência naturalmente convoca, a Constituição convida o legislador a um fino exercício de *concordância prática* entre a viabilização da justiça penal – e da reafirmação contrafáctica da validade das normas jurídicas implicadas na prossecução da atividade criminosa, da busca da verdade material e do restabelecimento da paz social que com ela se visam realizar – e a manutenção do mais amplo espaço possível de liberdade e privacidade no âmbito das comunicações humanas, cuja importância incontornável para o livre desenvolvimento da personalidade e afirmação da dignidade da pessoa humana a Lei Fundamental reconhece e protege.

41. Partindo deste *standard*, jurisprudencialmente definido, importa assinalar as diferenças relevantes, bem como as respetivas linhas de continuidade com a situação que ora nos ocupa, para podermos aferir da conformidade constitucional da restrição em causa no presente caso.

Assim, em primeiro lugar, como já repetidamente se mencionou, as normas questionadas implicam, de facto, uma restrição legal aos direitos fundamentais à não ingerência das autoridades públicas na correspondência e telecomunicações, bem como à reserva de intimidade da vida privada e proteção de dados pessoais. Todavia, e ao contrário de outras situações anteriormente analisadas pelo Tribunal Constitucional, tal restrição situa-se no âmbito do *processo penal*.

A situação, nesse plano, da restrição, implica que ela só opera em contextos em que exista notícia de um crime (alegadamente) praticado em momento prévio. Como é natural, e como antes se procurou explicitar, a pré-existência de atividade criminosa altera não só os bens e valores jurídico-constitucionalmente relevantes a compatibilizar, como o peso de cada um deles no exercício de concordância prática que se impõe ao legislador; este dispõe, nestas circunstâncias, de uma margem de ponderação que a Constituição entendeu vedar-lhe noutros domínios, resolvendo *a priori*, e com recurso a uma *regra* constitucional, eventuais conflitos de direitos e valores jusfundamentais, no sentido da prevalência da tutela das comunicações.

Nestes termos, resulta claro que uma restrição de direitos fundamentais como a que está em causa no presente processo é *possível,* nos termos do n.º 4 do artigo 34.º da CRP, uma vez que o legislador constituinte entendeu que os valores jurídico-constitucionais em causa em sede de processo penal o justificam – mesmo tratando-se de direitos aos quais se atribuiu uma proteção de tal forma reforçada que não cedem noutras situações, pese embora possam, nesses outros contextos, estar igualmente em questão princípios e direitos fundamentais consagrados na Constituição (vejam-se as situações dos Acórdãos n.º 403/2015 e n.º 464/2019).

42. A avaliação da conformidade constitucional das normas questionadas exige, porém, um juízo que vá além da mera verificação da *possibilidade abstrata* de restrições aos direitos fundamentais em causa em sede de processo penal, exigindo a análise atenta do cumprimento das exigências constitucionais de *excecionalidade*, *determinabilidade* e *proporcionalidade*, bem como das demais regras e princípios constitucionais aplicáveis. Este exercício pressupõe a consideração das concretas condições de aplicação, definidas pelas normas objeto de fiscalização, tal como acima se descreveram.

Nestes termos, cabe assinalar que, como se referiu, a alteração introduzida ao regime jurídico de apreensão do correio eletrónico ou similar, resultante das normas questionadas, que se afigura mais desafiante, do ponto de vista jurídico-constitucional é a atribuição ao Ministério Público, em sede de inquérito, e na qualidade de *autoridade judiciária competente*, para autorizar ou ordenar a apreensão.

Efetivamente, resulta das disposições combinadas dos artigos 263.º, n.º 1, e 1.º, alínea b), do Código de Processo Penal, que o Ministério Público será, em regra, a *autoridade judiciária competente* para a prática de atos no inquérito, na medida em que lhe incumbe a direção desta fase processual. O mesmo não sucede nas restantes fases, designadamente, na instrução, cuja direção cabe, nos termos do artigo 288.º, n.º 1, do CPP, a um juiz.

Ora, Ministério Público e juiz (no caso, o Juiz de Instrução Criminal) têm, à luz da Constituição e da lei, natureza e funções substancialmente distintas. Ao primeiro compete, segundo o n.º 1 do artigo 219.º da CRP e o artigo 2.º do Estatuto do Ministério Público (doravante, "EMP", aprovado pela Lei n.º 68/2019, de 27 de agosto), representar o Estado e defender os interesses que a lei determinar, participar na execução da política criminal definida pelos órgãos de soberania, exercer a ação penal orientada pelo princípio da legalidade e defender a legalidade democrática.

A CRP prevê ainda que o Ministério Público goze de um *estatuto próprio* e de *autonomia* (artigo 219.º, n.º 2), o que pressupõe a sua vinculação a critérios de legalidade e objetividade e pela exclusiva sujeição dos magistrados do Ministério Público às obrigações decorrentes do respetivo Estatuto (artigo 3.º do EMP), e não aos demais órgãos do poder público. Contudo, a Constituição concebe o Ministério Público como uma magistratura *responsável* e *hierarquicamente subordinada* (artigo 219.º, n.º 4 da CRP e artigo 14.º do EMP), sujeita a ação disciplinar por parte da Procuradoria-Geral da República (artigo 219.º, n.º 5 da CRP).

Quanto aos juízes, são *titulares de órgãos de soberania*, com competência para *administrar a justiça em nome do povo*, assegurando *a defesa dos direitos e interesses legalmente protegidos dos cidadãos*, reprimindo a violação da legalidade democrática e dirimindo os conflitos de interesses públicos e privados (artigo 202.º, n.ºs 1 e 2 da CRP e artigos 1.º e 3.º do Estatuto dos Magistrados Judiciais – doravante "EMJ", constante da Lei n.º 21/85, de 30 de julho, com as alterações decorrentes, por último, da Lei n.º 2/2020, de 31 de março).

Os juízes desempenham as suas funções em condições de estrita *independência* (artigo 203.º da CRP), não estando sujeitos a quaisquer ordens ou instruções (artigo 4.º do EMJ), gozando das garantias de *irresponsabilidade, inamovibilidade*, e outras previstas na lei (artigos 4.º a 6.º do EMJ), e vinculados a exigências de atuação *imparcial*, *isenta e de respeito pelo princípio da igualdade* (nos termos do disposto nos artigos 6.º-B e 6.º-C do EMJ).

No plano específico do processo penal, o artigo 32.º, n.º 4, da CRP assegura que toda a instrução é da competência de um juiz, não podendo este delegar noutras entidades a prática dos atos instrutórios que se prendam diretamente com os direitos fundamentais.

43. De tudo o que acaba de expor-se, resulta um retrato distinto da natureza, funções, e garantias associadas à intervenção processual do juiz e do Ministério Público, bastante relevante para a presente análise.

É certo que, como já vimos, a Lei Fundamental permite expressamente *a ingerência das autoridades públicas* na comunicação, nas suas várias formas, nos casos *previstos na lei*, em sede de *processo penal*. Além disso, não resulta diretamente da norma do n.º 4 do artigo 34.º da CRP que tal ingerência deva ocorrer, necessariamente, mediante intervenção de uma autoridade judicial. A este propósito, disse-se no Acórdão n.º 4/2006:

> «O artigo 34.º da CRP, após proclamar, no n.º 1, a inviolabilidade do domicílio e do sigilo da correspondência e dos outros meios de comunicação privada, considera, no n.º 4, "*proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os demais casos previstos na lei em matéria de processo criminal*" (o inciso "*e nos demais meios de comunicação*" foi aditado pela revisão constitucional de 1997, tendo em vista as modernas formas de comunicação à distância, que não correspondem aos sentidos tradicionais de correspondência ou de telecomunicações). Da formulação literal do n.º 4 do artigo 34.º da CRP resulta a limitação direta da admissibilidade da "ingerência ... nas comunicações" ao âmbito do *processo criminal* e a sua sujeição a *reserva de lei*. Mas desse preceito constitucional já não resulta, ao menos de forma explícita e direta, a sujeição da "ingerência" a *reserva de decisão judicial*, como, diversamente, o precedente n.º 2 faz relativamente à entrada no domicílio dos cidadãos contra a sua vontade, que só pode ser ordenada "*pela autoridade judicial competente, nos casos e segundo as formas previstas na lei*".»

Neste prisma, poderia defender-se que a intervenção do Ministério Público, enquanto *autoridade judiciária competente*, na fase de inquérito, bastaria – atenta a sua *autonomia* e os estritos critérios de *legalidade* pelos quais deve pautar-se a sua intervenção processual – para assegurar a conformidade constitucional da solução legal prevista nas normas questionadas.

Sucede, porém, que, tratando-se, como se demonstrou, de *normas restritivas* de direitos, liberdades e garantias, a afetação de tais direitos deverá ser a *menor possível*, devendo limitar-se ao mínimo indispensável para assegurar uma efetiva prossecução dos bens e valores jusconstitucionais que fundamentam a restrição. Ora, considerando o impressivo e distinto retrato do juiz e do Ministério Público que resulta do texto constitucional e das disposições legais aplicáveis – vistos os seus diferentes estatutos e poderes – parece incontornável reconhecer que a *intervenção judicial* constitui uma *garantia adicional de ponderação* dos direitos e liberdades atingidos no decurso da investigação criminal (veja-se o que se disse nos Acórdãos n.os 42/2007, n.º 155/2007, n.º 228/2007 e n.º 213/2008).

Efetivamente, nos momentos processuais em que esteja em causa uma *atuação restritiva* das autoridades públicas no âmbito dos direitos fundamentais, a intervenção de um juiz – com as virtudes de *independência* e *imparcialidade* que tipicamente a caraterizam – é essencial para uma tutela efetiva desses direitos, mesmo nos casos em que estes devam parcialmente ceder, em nome da salvaguarda de outros bens jusconstitucionalmente consagrados. O juiz tem, nos termos da CRP, uma *competência exclusiva e não delegável* de garantia de direitos fundamentais no âmbito do processo criminal (à luz do artigo 32.º, n.º 4, do CPP), pelo que a lei apenas pode dispensar a sua intervenção em casos excecionais devidamente delimitados e justificados. Por outras palavras, tal dispensa é constitucionalmente admissível apenas em situações pontuais e definidas com rigor, em que não constitua um *meio excessivo* para prosseguir interesses particularmente relevantes de investigação criminal. Será o caso, por exemplo, de atuações preventivas ou cautelares, em que haja particular urgência ou perigo na demora no que toca à conservação de elementos probatórios, e desde que se assegure uma posterior validação judicial da atuação das autoridades competentes.

44. Assim, não se vê como possa afirmar-se que as normas questionadas satisfaçam as exigências de *excecionalidade*, *necessidade* e *proporcionalidade* que se impõem às leis restritivas de direitos fundamentais, por força do artigo 18.º, n.º 2, da CRP. Na verdade, não se veem razões para afastar a intervenção prévia do Juiz de Instrução Criminal, em fase de inquérito, no que respeita aos atos de apreensão do correio eletrónico ou similar, nem elas resultam dos motivos apresentados pelo legislador para fundamentar a alteração legislativa aqui em causa, que acima se descreveram.

A intervenção do Juiz de Instrução Criminal não pode, atentas as normas constitucionais e legais que a regem, ser olhada como um "obstáculo à produção de prova". Como é evidente, não é essa a sua função, nem é tal propósito que rege a atuação processual daquele. Ela visa, sim, assegurar um alto grau de concordância prática entre as finalidades, constitucionalmente protegidas, prosseguidas pelo processo penal, e os direitos fundamentais por este afetados, legitimando as intervenções restritivas na esfera jusfundamental dos cidadãos. Por isso, uma compreensão adequada da atuação do Juiz de Instrução Criminal na fase pré-acusatória tem de reconhecer a sua natureza de "*entidade exclusivamente competente para praticar, ordenar ou autorizar certos atos processuais singulares que, na sua pura objetividade externa, se traduzem em ataques a direitos, liberdades e garantias das pessoas constitucionalmente protegidos*" (J. FIGUEIREDO DIAS, "Sobre os sujeitos processuais no novo Código de Processo Penal", in *O Novo Código de Processo Penal*, Almedina, Coimbra, 1988, p. 16).

Por esta razão, não pode, também, argumentar-se que a exigência de intervenção judicial quando estejam em causa atos de inquérito que diretamente contendam com direitos fundamentais, consagrada na norma contida no n.º 4 do artigo 32.º, da CRP, aqui plenamente mobilizável, afeta a direção do inquérito por parte do Ministério Público, ferindo o exercício das competências que a Constituição lhe

reserva. Na verdade, o Juiz de Instrução Criminal não atua, neste plano, *ex officio*, mas sim, em regra, a requerimento daquele, nos termos do disposto no n.º 2 do artigo 268.º do Código de Processo Penal. Deste ponto de vista, a condução do inquérito e a decisão sobre a seleção, desenho, oportunidade, importância e relevância da prática de atos destinados à produção de prova e à descoberta da verdade material continuam a pertencer, em exclusivo, àquele órgão. Este elemento afigura-se, assim, decisivo, numa perspetiva de compatibilização de uma reserva de jurisdição preventiva com o princípio do acusatório. Ou seja, estando a atribuição da competência para a determinação ou autorização da apreensão de correio eletrónico ou de natureza semelhante, ao Juiz de Instrução Criminal, na dependência de requerimento do Ministério Público, ela não colide com a direção e o domínio do inquérito por esta entidade.

Por outro lado, o n.º 4 do mesmo artigo 268.º do CPP determina que tal atuação deve obedecer a um princípio de *celeridade* e redução do formalismo processual, que visa assegurar uma compatibilização plena entre a tutela de direitos fundamentais pelo Juiz de Instrução Criminal e as necessidades de eficiência e agilidade na condução da investigação criminal.

Finalmente, acrescente-se ainda que, numa matéria com um grau significativo de *indeterminabilidade* – especialmente problemática por nos encontrarmos em sede de processo criminal –, e atenta a dificuldade de determinação, no plano prático, do significado concreto de conceitos como "mensagens de natureza semelhante ao correio eletrónico", num contexto de permanente evolução tecnológica, a intervenção prévia à respetiva apreensão de um Juiz de Instrução Criminal afigura-se como essencial para tutela dos direitos, liberdades e garantias afetados.

45. Nestes termos, considerando todos os argumentos até agora aduzidos, não se duvida de que os interesses prosseguidos pela investigação criminal constituem razões legítimas para uma afetação restritiva dos direitos fundamentais à inviolabilidade da correspondência e sigilo das comunicações (artigo 34.º, n.ºs 1 e 4, da CRP), e à proteção dos dados pessoais, no domínio da utilização da informática (artigo 35.º, n.ºs 1 e 4 da Lei Fundamental), enquanto manifestações particular e intensamente tuteladas da *reserva de intimidade da vida privada* (n.º 1 do artigo 26.º da CRP). Contudo, a restrição de tais direitos especiais, que correspondem a refrações particularmente intensas e valiosas de um direito, mais geral, à privacidade, não pode deixar de respeitar não apenas as condições genericamente impostas pelo texto constitucional para qualquer lei restritiva de direitos fundamentais, nos termos do artigo 18.º, n.º 2, da CRP, como a exigência específica, em sede de processo criminal, de intervenção de um juiz, consagrada no artigo 32.º, n.º 4, da Constituição.

Na verdade, como se procurou explicar, a Lei Fundamental reconhece tal relevo aos interesses e aos valores que a investigação criminal visa salvaguardar que expressamente permite a restrição, quando o não faz noutros âmbitos. Todavia, também não se olvida que o potencial ablativo da liberdade dos cidadãos é particularmente elevado em sede de processo penal, pelo que a CRP impõe a *intervenção do Juiz de Instrução Criminal*, enquanto titular de órgão de soberania independente, imparcial, e especialmente vocacionado para a proteção dos direitos fundamentais, sempre que se revele necessário garantir que os direitos e liberdades dos cidadãos não sofrem compressões desadequadas, desnecessárias ou desproporcionais, e para prevenir que intervenções restritivas abusivas atinjam a sua esfera jusfundamental. Existe, pois, uma ligação muito estreita entre a autorização constitucional de restrição, prevista no n.º 4 do artigo 34.º da CRP, e a previsão de competência primária do Juiz de Instrução Criminal para a prática de atos que diretamente contendam com direitos fundamentais, estatuída no n.º 4 do artigo 32.º da Constituição. Por isso, e como se disse, uma solução legal que dispense a prévia autorização daquele para a prática de atos de investigação penal que importam a invasão da esfera privada dos cidadãos só será constitucionalmente legítima se existir uma justificação cabal, robusta e bem determinada, não podendo, em caso algum, exceder os limites apertados de uma *solução excecional*.

Ora, a solução sob escrutínio, não satisfaz, de modo algum, as exigências constitucionais de necessidade e proporcionalidade em sentido estrito das intervenções restritivas em matéria de direitos fundamentais, decorrente do artigo 18.º, n.º 2, da CRP, nem a específica imposição de intervenção de um Juiz de Instrução Criminal nos atos de inquérito que diretamente contendam com direitos fundamentais, consagrada no artigo 32.º, n.º 4, da CRP.

46. Conclui-se, pois, que a norma que constitui o objeto do presente recurso é inconstitucional por violação dos direitos fundamentais à inviolabilidade da correspondência e das comunicações (consagrado no artigo 34.º, n.º 1, da CRP), à proteção dos dados pessoais no âmbito da utilização da informática (nos termos do artigo 35.º, n.ºs 1 e 4, da CRP), enquanto refrações específicas do direito à reserva de intimidade da vida privada, (consagrado no artigo 26.º, n.º 1, da Constituição), em conjugação com o princípio da proporcionalidade (nos termos do artigo 18.º, n.º 2, da CRP) e com as garantias constitucionais de defesa em processo penal (previstas no artigo 32.º, n.º 4, da Lei Fundamental).

III. Decisão

Pelo exposto, o Tribunal decide, com referência ao Decreto n.º 167/XIV da Assembleia da República, publicado no Diário da Assembleia da República, Série II-A, número 177, de 29 de julho de 2021, e enviado ao Presidente da República para promulgação como lei, pronunciar-se pela inconstitucionalidade das normas constantes do seu artigo 5.º, na parte em que altera o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, por violação das normas constantes dos artigos 26.º, n.º 1, 34.º, n.º 1, 35.º, n.ºs 1 e 4, 32.º, n.º 4, e 18.º, n.º 2, da Constituição da República Portuguesa.

A Relatora atesta o voto de conformidade do Senhor Conselheiro Lino Ribeiro, que interveio por meios telemáticos, nos termos do disposto no artigo 15.º-A do Decreto-Lei n.º 10-A/2020, de 13 de março (aditado pelo artigo 3.º do Decreto-Lei n.º 20/2020, de 1 de maio).

Lisboa, 30 de agosto de 2021 - *Mariana Canotilho* - *José João Abrantes* - *José Teles Pereira* (com declaração conjunta com a Cons. Maria José Rangel) - *Maria José Rangel de Mesquita* (com declaração conjunta com o Conselheiro José Teles Pereira) - *Assunção Raimundo* - *João Pedro Caupers*

DECLARAÇÃO DE VOTO

[apresentada conjuntamente pelos Conselheiros José António Teles Pereira e Maria José Rangel de Mesquita]

1. Expressa a presente declaração a opinião particular dos seus subscritores. Na sua essência, corresponde a uma *declaração concorrente*[1] com o Acórdão, encontrando-se – concorrendo, pois – com este, desde logo, na decisão propriamente dita – na pronúncia pela inconstitucionalidade do artigo 5.º do Decreto n.º 167/XIV, da Assembleia da República, quanto à alteração pretendida introduzir no artigo 17.º da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime, LCc) – e nos parâmetros do juízo de inconstitucionalidade que justificam tal decisão – os artigos 26.º, n.º 1, 34.º, n.º 1, 35.º, n.ºs 1 e

4, 32.º, n.º 4, e 18.º, n.º 2, da Constituição da República Portuguesa (CRP). Essa concordância abrange, aliás, o grosso da argumentação desenvolvida na fundamentação. Estamos, pois, não obstante o que adiante vai dito, perante uma decisão unânime do Tribunal Constitucional, o que se sublinha como aspeto importante, num pronunciamento que envolve uma formação do plenário reduzida a metade dos membros do colégio.

Não estamos, todavia, perante uma decisão cuja totalidade dos argumentos possa ser por nós partilhada em todas as dimensões. Os subscritores desta declaração têm razões próprias, sustentando uma visão que diverge em certos trechos da argumentação do Tribunal, considerando importante, por razões de coerência com posições que anteriormente assumiram, designadamente nos Acórdãos n.ºs 403/2015 e 464/2019, enunciar no presente contexto a especificidade do respetivo entendimento, sendo certo que, tanto o Requerente (no artigo 6.º do pedido de fiscalização) como o texto do Acórdão aludem, como se efetivamente apresentasse relevância neste caso, à linha decisória formada por esses arestos de 2015 e 2019. Com efeito, consideramos essas decisões tributárias de uma diferente questão de base que convocou outros problemas, que não aportam um contributo significativo para o esclarecimento da questão de constitucionalidade especificamente colocada pela opção legislativa com a qual somos confrontados nesta fiscalização preventiva. Não nos revemos, pois, em certos trechos da fundamentação que, estamos em crer, induzem alguma confusão quanto às garantias do processo penal (a questão que está efetivamente em causa no artigo 17.º da LCc agora pretendido introduzir) e o problema genérico do tratamento de dados pessoais e da proteção da privacidade no sector das comunicações eletrónicas, designadamente no contexto da previsão de formas de acesso pelas autoridades públicas a dados guardados por fornecedores de serviços de comunicações.

Neste quadro, onde é forte a presença – e a interação com o Direito nacional – do Direito da União Europeia (DUE) e da jurisprudência do Tribunal de Justiça da União Europeia (TJUE), têm os subscritores desta declaração divergências significativas (em alguns casos mesmo muito significativas) com a perspetivação dessas questões adotada no Acórdão. Não podemos, pois, deixar de sublinhar a nossa perspetiva e o afastamento de certos pressupostos da argumentação do Tribunal.

2. A norma sindicada (vale tal referência para o conteúdo do artigo 17.º da LCc) integra-se, na sistemática do Diploma, tanto na versão em vigor como na introduzida pelo Decreto n.º 167/XIV, num Capítulo designado "Disposições processuais" (Capítulo III, artigos 11.º a 19.º). Este corresponde a *matéria de processo criminal*, ou seja, a normas de *direito processual penal*[2]. Assim se evidencia, diversamente do que como hipótese se aventa na exposição do Requerente (cfr. o respetivo ponto 14.º, com correspondência no pedido formulado a final), o desajustamento à situação, enquanto parâmetro de um possível desvalor constitucional, do n.º 4 do artigo 34.º da CRP. Com efeito, corresponde o artigo 17.º da LCc (na disposição vigente e na projectada), evidenciando um sentido linguístico indubitavelmente coincidente com o pensamento legislativo, ao recorte negativo, introduzido pelo trecho final do n.º 4 do artigo 34.º, da CRP (… *salvos os casos previstos na lei em matéria de processo criminal*), à proibição de ingerência sedeada no trecho inicial da norma ([*é*] *proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação*…).

Daí que as referências constantes do presente Acórdão, remetendo para a anterior jurisprudência do Tribunal relativa a *metadados* (concretamente ao Acórdão n.º 403/2015), abonando a asserção de existência de uma *reserva absoluta de processo criminal* quanto à previsão de formas de acesso pelas autoridades públicas a dados guardados por fornecedores de serviços de comunicações, não tenham cabimento numa fundamentação que se pretenda congruente com o sentido da norma visada pelo pedido formulado. Com efeito, estamos neste caso, desde logo, perante normas de *processo penal* – por isso o n.º 4 do artigo 34.º da CRP não constitui parâmetro do desvalor constitucional afirmado no dispositivo –, ao que acresce a circunstância de o Tribunal, tanto no Acórdão n.º 403/2015 como no Acórdão n.º 464/2019, não ter excluído em absoluto – e no presente Acórdão fala-se em *reserva absoluta* (cf. n.ºs 28 e 40) – o acesso a determinados dados (determinados *metadados*) conservados por fornecedores de serviços de comunicações[3] fora de um contexto que possamos identificar como

respeitante a normas de *processo criminal* [3], embora interpretável – é a posição sustentada pelos subscritores desta declaração e de outros e de outros Conselheiros que não integram a formação do colégio em que ora se discute o pedido – como não inconciliável, nas condições em causa nesses outros processos, com a expressão *em matéria de processo criminal*. Assim, o que se diz em algumas passagens do Acórdão a respeito da *reserva absoluta de processo criminal*, quando aqui (só) está em causa uma norma de processo penal – o que ninguém (o próprio Acórdão) discute –, só pode ter o "valor" de *obiter dictum*, tratando-se de "[…] *considerandos que o juiz* [*fez*] *(em princípio indevidamente) e que não* [*são*] *peça do raciocínio que conduz à decisão.* [*São*]*, por conseguinte,* […] *declarações enunciativas ou opinativas* […]"[4], que aqui temos dificuldade em deixar de encarar como descabidas.

2.1. Além de situar tematicamente o pedido – e de tornar patentes os fundamentos efetivamente apropriados à construção da decisão –, a natureza adjetiva (processual penal) do artigo 17.º integra a caraterização da realidade à qual se refere essa adjetivação: *correio eletrónico ou registos de comunicações de natureza semelhante* (no regime vigente), *mensagens de correio eletrónico ou de natureza semelhante* (no regime pretendido introduzir) – o mesmo sucede, aliás, relativamente às realidades visadas pelos antecedentes artigos 15.º e 16.º (*dados informáticos*) e com o subsequente artigo 18.º (*comunicações*), que o Decreto n.º 167/XIV não alterou. Vale esta constatação para sublinhar o significado daquilo que *ab initio* é acedido e alcançável pelo Ministério Público e pelos órgãos de polícia criminal, por força da nova versão do artigo 17.º, no quadro investigatório em causa na Lei do Cibercrime, postergando o sentido atuante da *reserva juiz*, expressa no artigo 32.º, n.º 4, da CRP, entendida esta como referida, não apenas, ao monopólio judicial *tanto da última como da primeira palavra* em atos investigatórios que se prendam com direitos fundamentais (Acórdão n.º 387/2019). É que, referindo-se as buscas e apreensões aqui em causa ao que usualmente se refere como *dados de conteúdo*, por oposição a dados circunstanciais de comunicações (os chamados *metadados*, tratados nos já referidos Acórdãos n.ºs 403/2015 e 464/2019), e a elementos recolhidos diretamente no sistema informático individual[5] do de um determinado usuário (ou a ele afecto) e não no sistema do operador de comunicações, torna-se evidente o grau de interferência e a potencialidade de comprometimento dos direitos fundamentais ao sigilo das comunicações e à privacidade de quem é diretamente abrangido pelas medidas previstas no artigo 17.º, e mesmo de terceiros, "apanhados" num acesso autorizado, num caso de *conhecimentos fortuitos,* por existirem elementos (dados de conteúdo), a esses terceiros referidos, armazenados no sistema que é pesquisado. É esta a realidade que agora se pretende subtrair a um controlo judicial *ab initio* e completo, no sentido de não mediado (*rectius*, filtrado) pela lógica investigatória que é protagonizada pelo Ministério Público. E esse é, com efeito, um desvalor assinalado pela jurisprudência do TJUE – num plano de apreciável congruência e paralelismo com o nosso texto constitucional, no artigo 32.º, n.º 4 – ao controlo do acesso pelas autoridades públicas a dados pessoais existentes em suporte informático, (conservados por prestadores de serviços de comunicações eletrónicas), designadamente no quadro da investigação penal: *"*[…] *a exigência* [*de*] *independência que a autoridade encarregada de exercer a fiscalização prévia, recordada no n.º 51 do presente acórdão*[6]*, deve satisfazer, impõe que essa autoridade tenha a qualidade de terceiro em relação à autoridade que pede o acesso aos dados, de modo que a primeira esteja em condições de exercer essa fiscalização de maneira objetiva e imparcial, ao abrigo de qualquer influência externa. Em especial, no domínio penal, a exigência de independência implica* […] *que a autoridade encarregada dessa fiscalização prévia, por um lado, não esteja envolvida na condução do inquérito penal em causa e, por outro, tenha uma posição de neutralidade relativamente às partes no processo penal.*" [ponto 54 do Acórdão de 02/03/2021 *H. K. /Prokuratuur* (C-746/18, ECLI:EU:C:2021:152)].

A respeito do âmbito de proteção constitucional do direito ao sigilo das telecomunicações duas notas adicionais se impõem no contexto do novo artigo 17.º da LCc.

2.1.1. A primeira sublinha ser exata a afirmação contida no Acórdão de que a proteção do sigilo das comunicações eletrónicas abrange, como não poderia deixar de ser, tanto os dados circunstanciais de comunicações pretéritas (os *dados de base, localização e tráfego*, *rectius, metadados*) como o próprio conteúdo dessas comunicações (os *dados de conteúdo*). E, com efeito, como se diz no presente aresto, nenhum respaldo obtém na jurisprudência constitucional qualquer afirmação contrária a esta,

sendo evidente que o conteúdo das próprias comunicações sempre representará um *plus* muito significativo de ofensividade, efetiva ou potencial, ao direito à incolumidade das telecomunicações e à privacidade colocada em causa pela intervenção nestas. Isso mesmo, aliás, obtém claro respaldo na jurisprudência do TJUE, desde o Acórdão *Digital Rights Ireland* (de 8/4/2014, C-293/12 e C-594/12, ECLI:EU:C:2014:238), circunstância que no contexto que ora nos interpela (em que estão em causa *dados de conteúdo*) deve ser destacada. Com efeito, em *Digital Rights* não deixou o Tribunal de Justiça de afirmar que o acesso ao *conteúdo das comunicações eletrónicas*, contrariamente ao que sucede com o acesso aos dados circunstanciais dessas comunicações[7], afeta o *conteúdo essencial do direito fundamental ao respeito da vida privada* (ponto 39 do Acórdão).

2.1.2. Como segunda nota a destacar, referimos a natureza do elemento acedido em vista da busca – da fonte da informação recolhida.

De facto, também neste aspeto existe uma particularidade relevante que nos fornece a exata medida do caráter intenso e insidioso da agressão à privacidade induzida pela recolha de elementos no quadro do artigo 17.º da LCc, e do salto qualitativo de perigosidade decorrente da relativização muito intensa de um efetivo controlo judicial resultante do regime ora pretendido introduzir.

É que o acesso aqui em causa refere-se à fonte primária continente de toda informação em suporte eletrónico possuída por alguém, refere-se, pois, em termos práticos, ao (ao que está contido no) seu *computador*, ao *telemóvel*, ao *tablet*, ao *smartphone* ou a qualquer dispositivo equivalente susceptível de conter o tipo de dados abrangidos, correspondendo esta incidência a uma realidade substancialmente distinta daquela que, através do sistema da operadora de telecomunicações, é susceptível de ser obtido relativamente a comunicações pretéritas.

O sentido dessa diferença substancial é de fácil apreensão por via da construção ficcional de um exemplo referido ao correio em suporte físico (cartas e outros objetos postais) assente numa situação cuja base é real, à qual acrescentámos uma construção ficcional hipotética que ilustra, por comparação, o argumento que pretendemos afirmar.

Em 2013, num artigo de Ron Nixon, publicado na edição de 3 de julho do jornal *New York Times*, foi descrita uma prática de muitas décadas do *U.S. Postal Service*, consistente em microfotografar as cartas e objetos postais (visualizando os endereços dos remetente e destinatário) guardando esse registo por tempo indeterminado[8]. Por via do acesso a esse sistema de armazenamento de informação é possível obter os *metadados* da actividade postal de alguém. Ora, ficcionando a hipótese, seguramente muito improvável, de alguém que guardasse num ficheiro físico, ordenado cronologicamente, todo o correio expedido (cópias) e recebido, acoplando os invólucros e a correspondência por estes contida, ilustramos a potencialidade intrusiva do acesso a esta fonte primária de informação (o tal ficheiro pessoal), comparativamente à anterior, na sua referenciação a alguém. Perigo que se amplia, exponencialmente – e esta é a circunstância verdadeiramente relevante na presente fiscalização –, pela sobreposição de um processamento eletrónico, inerente aos sistemas informáticos pesquisados, que permite, por si só, ou pelo emprego de ferramentas específicas, uma seleção concreta (parametrizada) da informação pretendida aceder[9].

É esta nova vertente de escala do problema, alargada, já num plano distinto do aqui em causa, à existência de enormes sistemas de armazenamento de informação, controlados por entidades exteriores àqueles a quem essa informação respeita e a detêm primariamente, que interpela expressivamente o nosso texto constitucional – aqui no quadro das garantias do processo criminal –, o Direito da União, e a jurisprudência respetiva.

3. É o entendimento particular dos subscritores deste voto, quanto à incidência no caso do DUE, que em muitos pontos não coincide com a do Acórdão, que determina, concorrentemente ao sentido decisório que a decisão do Tribunal expressa, a apresentação de uma visão particular, mas com potencial de projeção em situações que previsivelmente ocuparão o Tribunal. Lembramos que foi o

Acórdão que trouxe à liça essas questões, determinando a presente tomada de posição dos subscritores da presente declaração.

O nosso ponto de partida – ou de divergência com o texto do Acórdão – recupera o trecho final do ponto 20 deste, no qual se afirma "[…] *que nos termos do artigo 1.º, n.º 3, da Diretiva 2002/58/CE, e do artigo 2.º do RGPD, o âmbito de aplicação da legislação europeia, nesta matéria, não inclui o processo penal* […]", acrescentando-se que, "*ainda assim*", "[…] *do acervo legal e jurisprudencial da União Europeia acerca de temáticas paralelas à que ora nos ocupa resulta a paulatina construção de standards de tutela jusfundamental no que respeita ao tratamento de dados pessoais e de dados relativos às comunicações, no âmbito da utilização da informática que não deve ser ignorado*". Ora, as afirmações contidas neste trecho (e retomadas no ponto 22), não sendo inteiramente precisas na sua base, afetam o sentido conclusivo pretendido extrair (também nos pontos 24 e 25 do Acórdão), colocando na argumentação do Tribunal sentidos possíveis que uma ponderação rigorosa das especificidades, neste domínio, de normas de DUE não autoriza.

Cumpre, pois, proceder ao enquadramento – ao enquadramento que entendemos ser o mais adequado – da norma ora sindicada à luz do DUE.

3.1. Além do direito originário pertinente, em geral, em matéria de proteção de dados pessoais e da privacidade no setor das telecomunicações eletrónicas – artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE) e artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE) –, o acervo de direito derivado que densificou o direito à proteção de dados pessoais e privacidade integrou, até à entrada em vigor do *Regulamento (UE) n.º 2016/679* de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (*Regulamento Geral de Proteção de Dados* [RGPD], aplicável a partir de 25 de maio de 2018), três atos de direito derivado principais de harmonização das disposições legislativas nacionais: *i)* a *Diretiva 95/46/CE* do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (modificada pelo Regulamento (CE) n.º 1882/2003 do Parlamento Europeu e do Conselho de 29 de setembro de 2003); *ii)* a *Diretiva 2002/58/CE* do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (*Diretiva relativa à privacidade e às comunicações eletrónicas*); *iii)* a *Diretiva 2006/24/CE* do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de telecomunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Diretiva 2002/58/CE (*data retention*), em concreto aditando o n.º 1-A ao seu artigo 15.º – transpostas para ordem jurídica nacional, respetivamente, pela Lei n.º 67/98, de 26 de outubro (Lei de Proteção de Dados Pessoais [LPDP], revogada pela Lei n.º 58/2019, de 8 de agosto que, na sequência da adoção do RGPD, assegurou a execução deste na ordem jurídica nacional); pela Lei n.º 41/2004, de 18 de agosto (Lei da Privacidade nas Comunicações Eletrónicas [LPCE]), alterada pela Lei n.º 46/2012, de 29 de agosto; e pela Lei n.º 32/2008, de 17 de julho.

A terceira das diretivas indicadas – Diretiva 2006/24/CE (transposta pela Lei n.º 32/2008, de 17 de julho, ainda em vigor) – foi considerada inválida pelo TJUE no Acórdão, acima referido, *Digital Rights Ireland,*; a primeira – Diretiva n.º 95/46/CE (transposta à data, como se referiu, pela Lei n.º 67/98, de 26 de outubro) e que a referida Diretiva n.º 2002/58/CE visou especificar e complementar – foi revogada pelo RGPD (cf. art. 94.º e 95.º do RGPD) – pelo que hoje – e estamos a procurar sistematizar os dados de uma situação algo confusa –, das três diretivas enunciadas apenas se encontra em vigor a Diretiva 2002/58/CE, vigorando ainda o posterior RGPD.

3.2. A temática da proteção de dados pessoais e da privacidade no setor das telecomunicações eletrónicas foi objeto recorrente da jurisprudência do TJUE na vigência do referido quadro de direito originário e derivado, sucessivamente – no que releva em especial para os presentes autos – no mencionado acórdão *Digital Rights Ireland* e, ainda, nos acórdãos *Tele2/Watson* (acórdão de 21/12/2016,

C-203/15 e C-698/15, ECLI:EU:C:2016:970); *Ministerio Fiscal* (acórdão de 2/10/2018, C-207/16, ECLI:EU:C:2018:788); *Privacy International* (acórdão de 6/10/2020, C-623/17, ECLI:EU:C:2020:790); *La Quadrature du Net e o.* (acórdão de 6/10/2020, , C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791); e, ainda*, H. K. /Prokuratuur* (acórdão de 2/3/2021), já antes referido.

É importante referir o contexto "histórico" – chamemos-lhe assim – do aparecimento destas decisões, a partir de 2014 com *Digital Rights Ireland*. Com efeito, subsequentemente aos acontecimentos de 11 de setembro de 2001, iniciou-se em alguns países – desde logo nos Estados Unidos, mas também no Reino Unido – um processo que poderemos definir genericamente como de captação generalizada e massificada, por agências governamentais na área dos serviços de informações, de dados (*metadados*) relativos a comunicações pretéritas, com o subsequente armazenamento destes como instrumentos prospetivos de luta contra a ameaça do terrorismo. É esse o sentido das primeiras palavras de Edward Snowden no seu livro autobiográfico: "[*a*] *minha carreira na comunidade de informações (CI) americana durou sete curtos anos* […]. *Durante esses sete anos, no entanto, tive a oportunidade de participar na mais significativa mudança na história da espionagem americana – a mud*[10] *da vigilância de alvos individualizados* [*targeted surveillance*] *para a vigilância em massa de toda a po*[11]*ção* […]". Esta asserção é confirmada por diversos outros elementos publicados nos últimos anos.

3.2.1. No primeiro Acórdão que referimos – *Digital Rights Ireland* – o TJUE considerou inválida a Directiva 2006/24/CE, entendendo que o legislador da União excedeu os limites impostos pelo respeito do princípio da proporcionalidade à luz dos artigos 7.°, 8.° e 52.°, n.° 1, da CDFUE (cf. n.º 69).

Da fundamentação do acórdão decorre, por um lado, que a Diretiva 2006/24 visava, tão só, harmonizar as disposições nacionais relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou das redes públicas de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados – que ora não está em causa; e, por outro lado, que a imposição, a tais fornecedores de serviços, da obrigação (prevista no seu artigo 3.º), de conservarem os dados enumerados no artigo 5.° da mesma (*metadados,* não autorizando a Diretiva, como antes já antes se sublinhou em 2.1, a conservação do *conteúdo* da comunicação e das informações consultadas através de uma rede de comunicações eletrónicas), para, se necessário, os disponibilizarem às autoridades nacionais competentes, suscitava questões relativas à proteção da vida privada e das comunicações, à proteção de dados pessoais consagradas nos artigos 7.° e 8.º da CDFUE, assim como ao respeito da liberdade de expressão prevista no artigo 11.° da CDFUE (cfr. pontos 25, 26, 28).

Todavia, embora o TJUE tenha admitido que tal obrigação de conservação constitui uma ingerência particularmente grave naqueles direitos, considerou não ser esta suscetível de afetar o conteúdo dos dois primeiros (proteção da vida privada e das comunicações), *"*[…] *tendo em conta que, como resulta do seu artigo 1.°, n.° 2, esta diretiva não permite tomar conhecimento do conteúdo das comunicações eletrónicas, enquanto tal.*" (cfr. n.º 39); nem o conteúdo essencial do direito fundamental à proteção dos dados pessoais, uma vez que a Diretiva 2006/24 previa, "[…] *no seu artigo 7.°, uma regra relativa à proteção e à segurança dos dados* […]" (cfr. ponto 40)[12]; e, ainda, que essa ingerência "[…] *responde a um objetivo de interesse geral* […]"*,* já que o objetivo material da Diretiva "[…] *tem em vista garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de infrações graves, tal como definidas no direito interno de cada Estado-Membro*", isto é, "[…]*contribuir para a luta contra a criminalidade grave e, assim, em última análise, para a segurança pública.* (cfr. ponto 41.)

Não resulta, pois, do teor do aresto, o afastamento ou a desconformidade com o DUE da obrigação de conservação de dados – *metadados* e não dados de *conteúdo* – impostas aos fornecedores de serviços de comunicações eletrónicas passíveis de constituir uma ingerência em direitos fundamentais protegidos pela ordem jurídica da União – mas tão só de ingerências desproporcionadas – como desde logo o são quaisquer transferências em massa desses dados para autoridades públicas – face aos fins,

legítimos, consagrados, como a final concluiu – mas em domínio que, por respeitar a obrigações impostas a tais operadores, se afasta do tratamento de dados para os fins em causa neste processo (perseguição criminal).

3.2.2. Nos demais acórdãos, o TJUE versou, em especial, sobre a interpretação do artigo 15.º da Diretiva 2002/58/CE (isolada ou conjugadamente com outros preceitos de DUE, em especial os artigos 7.º e 8.º da CDFUE), que versa as sobre a "[*a*]*plicação de determinadas disposições da Diretiva 95/46/CE*" e cujo número 1 prevê que "[*o*]*s Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.ºs 1 a 4 do artigo 8.º e no artigo 9.º da presente diretiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.º 1 do artigo 13.º da Diretiva 95/46/CE. Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.ºs 1 e 2 do artigo 6.º do Tratado da União Europeia*".

Na jurisprudência decorrente desses arestos, o TJUE interpretou o DUE por referência a medidas restritivas nacionais – cuja adoção aquele preceito consente para os fins aí previstos – da mesma decorrendo, por um lado, a desconformidade com o mesmo de medidas restritivas nacionais de conservação e retenção de dados (desde logo, de localização e de tráfego) *em massa* (a chamada *bulk retention* ["*conservação generalizada e indiferenciada*", na expressão do Acórdão *La Quadrature du Net e o.,* ponto 168,]) e, por outro, a admissibilidade face ao DUE, verificadas certas condições fixadas nesse acervo jurisprudencial, de medidas restritivas de conservação, retenção e acesso especificamente direcionadas (*target retention*) – seja para efeitos de *salvaguarda da segurança nacional (ou seja, a segurança do Estado), da defesa, da segurança pública* (em especial, os acórdãos *Tele2/Watson, Privacy International* e *La Quadrature du Net e o.*), seja para efeitos de *prevenção, investigação, detecção e repressão de infracções penais* (em especial os acórdãos *Ministerio Fiscal* e *H.K./Prokuratuur*) ou *da utilização não autorizada do sistema de comunicações electrónicas,* tal como referido no n.º 1 do artigo 13.º da Directiva 95/46/CE – que previa que "[*o*]*s Estados membros podem tomar medidas legislativas destinadas a restringir o alcance de obrigações e direitos nela previstas sempre que tal restrição constitua uma medida necessária à proteção, entre outros fins aí previstos: a) Da segurança do Estado; b) Da defesa; c) Da segurança pública; d) Da prevenção, investigação, deteção e repressão de infrações penais e de violações da deontologia das profissões regulamentadas*".

Todavia – e deve sublinhar-se – a jurisprudência assim prolatada é referenciada a medidas restritivas de conservação, retenção e acesso a dados por via de obrigações impostas aos prestadores de serviços de comunicações eletrónicas. E assim é, também, no caso *H.K./Prokuratuur,* no qual – e é este o exato contexto do *supra* mencionado (cf. 2.1) desvalor assinalado pelo TJUE (a que o Acórdão confere relevância acrescida) – a questão da qualificação do Ministério Público estónio como autoridade administrativa independente (na aceção do ponto 120 do acórdão *Tele2/Watson)* se colocava relativamente à autorização do acesso da autoridade encarregada do inquérito a dados relativos às comunicações eletrónicas como os previstos no artigo 111.º, n.º 2, da Lei Relativa às Comunicações Eletrónicas – que justamente impõe aos prestadores de serviços de telefonia fixa e de telefonia móvel e da rede de telefonia fixa e de telefonia móvel devem conservar os [*meta*]dados [de tráfego e de localização] previstos em tal preceito (cfr. os pontos 23 e 9 do Acordão *H.K./Prokuratuur* – e a pronúncia do Tribunal nos pontos 46 a 59].

3.3 Ademais, à semelhança do disposto no referido artigo 13.º, n.º 1, da Diretiva 95/46/CE, também o artigo 23.º, n.º 1, alíneas a) a j), do RGPD (que a revogou), continua a prever a possibilidade de os Estados membros adotarem medidas legislativas que limitem o alcance das obrigações e dos direitos nele previstos, entre outros, para fins de "[…] *prevenção, investigação, deteção ou repressão de infrações*

penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública" (cfr. alínea *d*) do n.º 1 do artigo 23.º).

Além disso, a Diretiva 95/46/CE previa, no seu artigo 3.º, n.º 2, primeiro e segundo travessões, que "[*a*] *presente diretiva não se aplica ao tratamento de dados pessoais: – efetuado no exercício de atividades não sujeitas à aplicação do direito comunitário, tais como as previstas nos títulos V e VI do Tratado da União Europeia, e, em qualquer caso, ao tratamento de dados que tenha como objeto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse tratamento disser respeito a questões de segurança do Estado), e as atividades do Estado no domínio do direito penal, - efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas.*" (sublinhado acrescentado) e idêntico preceito consta hoje do artigo 2.º, n.º 2, do RGPD (*Âmbito de aplicação material*), o qual dispõe que o mesmo *não se aplica* ao tratamento de dados pessoais: "[…] *a) Efetuado no exercício de atividades não sujeitas à aplicação do Direito da União; b) Efetuado pelos Estados membros no exercício de atividades abrangidas pelo âmbito de aplicação do Título V, capítulo 2, do TUE* [ou seja, depois da entrada em vigor do Tratado de Lisboa, as Disposições específicas relativas à Política Externa e de Segurança Comum (Seção 1 – Disposições Comuns, arts. 23.º-41.º e Seção 2, Disposições relativas à Política Comum de Segurança e Defesa, arts. 42.º-46.º, todos do TUE)]; [...] *d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública* […]" (sublinhados acrescentados). Note-se que idêntico âmbito negativo de aplicação consta do n.º 3 do artigo 1.º (*Âmbito e objetivos*) da Diretiva 2002/58/CE [sendo a delimitação negativa do âmbito de aplicação do RGPD retomada no artigo 2.º, n.º 2, alíneas *a*), *b*) e *d*) da *Proposta de Regulamento relativo à privacidade e às comunicações eletrónicas* – COM (2017) 10 final de 10/1/2017, cujo processo legislativo ordinário se encontra ainda em curso, em fase de primeira leitura].

De tais preceitos de direito derivado decorre a distinção entre, por um lado, o âmbito negativo de aplicação da Diretiva 95/46/CE e do posterior RGPD que a revogou (artigos 3.º, n.º 2, primeiro travessão, e artigo 2.º, n.º 2, do RGPD, respetivamente) e, por outro lado, a credencial de DUE para a adoção, pelos Estados membros, de medidas legislativas nacionais que constituam limitações aos direitos e obrigações impostos pelas Diretivas e pelo RGPD (artigos 13.º, n.º 1, alíneas a) a g), da Diretiva 95/46/CE – e 15.º, n.º 1, da Diretiva 2002/58/CE que ao mesmo se refere – e artigo 23.º, n.º 1, alíneas a) a j), do RGPD).

Ora, esta última dimensão implica que tais limitações sejam (sempre) referenciadas à intervenção dos prestadores de serviços de telecomunicações eletrónicas aos quais os Estados, para os fins previstos pelo DUE, podem impor obrigações de conservação e de tratamento que se traduzem em medidas legislativas restritivas dos direitos e obrigações previstos naquele. E é sobre esta específica dimensão que versa a jurisprudência do TJUE nos referidos acórdãos *Tele2/Watson* e subsequentes.

Ao invés – e é esta a exata situação versada pela norma aqui sindicada – quando se trata de atuações do próprio Estado que, através dos seus órgãos e agentes competentes no domínio do exercício da ação penal (Ministério Público e órgãos de polícia criminal), adota medidas que se projetam diretamente sobre a pessoa objeto dessa ação penal e sobre os seus dados pessoais e privacidade (incluindo os dados pessoais decorrentes de mensagens de correio eletrónico ou de natureza semelhante cuja apreensão é consentida pela norma ora sindicada), sem qualquer intervenção ou mediação dos prestadores de serviços de comunicações eletrónicas no mercado interno, o paradigma e referente de DUE é outro, bem diverso. Tratando-se, *in casu,* de tratamento de dados (*lato sensu*) efetuado pelas autoridades nacionais competentes para efeitos de *prevenção, investigação, deteção e repressão de infrações penais* (especificamente no domínio do cibercrime mas que podem extravasar o mesmo – cf. alíneas *a*), *b*) e *c*) do n.º 1 do artigo 11.º) tal referente é o da exclusão de tais medidas do respetivo âmbito de aplicação – seja do âmbito de aplicação do RGPD, seja do âmbito de aplicação da Diretiva 2002/58/CE [ou da referida *Proposta de Regulamento relativo à privacidade e às comunicações eletrónicas*, que visa substituir a Diretiva 2006/24/CE julgada inválida pelo TJUE em *Digital Rights*].

Aplicam-se, por isso, neste domínio da atuação estadual direta, contra o que parece resultar do texto do Acórdão (sendo que nesta parte dele divergimos), não os parâmetros e a proteção decorrentes

da Diretiva 2002/58/CE ou do RGPD e sua interpretação pelo TJUE, mas sim os parâmetros pertinentes do direito (no que releva) constitucional nacional, interpretados à luz do DUE de harmonização aprovado nesse particular domínio em matéria de proteção de dados.

Esta diferença é aliás, bem assinalada pela jurisprudência do TJUE primeiro, no caso *Privacy International* (cf. ponto 48) e, depois, no caso *La Quadrature du Net e o.* (cf. ponto 103), quando aí se afirma:

"[…]

> *103. Em contrapartida, quando os Estados-Membros aplicam diretamente medidas que derrogam a confidencialidade das comunicações eletrónicas, sem imporem obrigações de tratamento aos prestadores de serviços de tais comunicações, a proteção dos dados das pessoas em causa não está abrangida pela Diretiva 2002/58, mas apenas pelo direito nacional, sem prejuízo da aplicação da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO 2016, L 119, p. 89), de tal modo que as medidas em causa devem respeitar, nomeadamente, o direito constitucional nacional e os requisitos da CEDH.*
>
> […]".

3.4. Do enquadramento que acabámos de enunciar, decorrem três conclusões principais, as quais, alternativamente ao Acórdão, aqui apresentamos.

Em primeiro lugar, a Diretiva 2002/58/CE e o seu artigo 15.º – e a sua interpretação pelo TJUE nos termos referidos – não constituem o referencial adequado para o enquadramento de DUE da questão objeto dos presentes autos, já que se referem ao tratamento de dados pelos prestadores de serviços de telecomunicações eletrónicas e por estes obtidos no quadro de tais serviços, e não ao tratamento de dados obtidos, diretamente, por autoridades estatais, *in casu,* o tratamento (apreensão e atos posteriores) pelas autoridades públicas competentes no quadro do exercício da ação penal pelo Estado (Ministério Público e Órgãos de polícia criminal).

Em segundo lugar, o RGPD também não constitui o referencial adequado para o enquadramento de DUE da questão objeto dos presentes autos, já que aquele instrumento expressamente dispõe que o mesmo *não se aplica* ao tratamento de dados pessoais efetuado pelas autoridades competentes para efeitos de *prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais*, incluindo a salvaguarda e a prevenção de ameaças à segurança pública (cf. artigo 2.º, n.º 2, alínea *d*), do RGPD) – neste sentido dispondo igualmente a Diretiva 2002/58/CE (cf. artigo 1.º, n.º 3, *in fine,* da mesma).

Em terceiro lugar, por força de tal exclusão – e inexistindo imposição de obrigações de tratamento aos prestadores de serviços de comunicações eletrónicas que convoquem a aplicação da Diretiva 2002/58/CE – a proteção dos dados das pessoas objeto da ação penal exercida pelo Estado decorre apenas do direito, *maxime* constitucional, nacional (e das fontes de direito internacional a que o Estados se tenham vinculado, como a CEDH ou, neste caso, também a Convenção de Budapeste), sem prejuízo da observância do DUE especificamente aplicável nesse domínio. Ora, a par do RGPD foi adotada igualmente, a *Diretiva (UE) 2016/680* do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (a mesma data de adoção do RGPD), *relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais* ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-

Quadro 2008/977/JAI do Conselho – e que constitui, a par do direito nacional, o referente de direito derivado da União[13] adequado ao enquadramento, nessa perspetiva, de questões como a suscitada nos presentes autos.

3.4.1. Com efeito, a Diretiva (UE) 2016/680 estabelece um específico regime de harmonização na matéria em causa (em paralelo com o RGPD, mas com algumas especificidades), o qual a mesma considera conforme ao DUE e necessário à luz do artigo 52.º, 1 da CDFUE (cf. considerando 104) – tendo a mesma sido já transposta para a ordem jurídica portuguesa pela *Lei n.º 59/2019, de 8 de Agosto* (que *aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infração penais ou de execução de sanção penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016* – cfr. o respetivo artigo 1.º).

É este o regime harmonizado de DUE – e já transposto para a ordem jurídica interna, pela Lei n.º 59/2019, de 8 de agosto – que constitui o referente a levar em conta quando se trata de enquadrar o tratamento de dados (apreensão incluída) *directamente* pelas autoridades nacionais competentes (autoridades públicas) em matéria de exercício da ação penal, por um lado; e que incida sobre dados pessoais que se encontram na própria esfera do visado por aquela ação (e fora da esfera dos prestadores de serviços de comunicações eletrónicas e do quadro de imposição de obrigações a estes) – i.e., a apreensão (autorizada, ordenada ou validada, consoante o caso, pela autoridade judiciária competente), no âmbito da "[…] *pesquisa informática ou de outro acesso legítimo a um sistema informático, de mensagens de correio eletrónico ou de natureza semelhante* […]", que "[…] *forem encontradas, armazenadas nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro* […] *que sejam necessárias à produção de prova, tendo em vista a descoberta da verdade*" (n.º 1 do artigo 17.º da disposição ora em causa).

Com efeito, nos termos do artigo 3.º, n.º 7, da Diretiva (UE) 2016/680, transposta pela já referida Lei n.º 59/2019 (cfr. alínea *i*) do n.º 1 do seu artigo 3.º), deve entender-se por "*Autoridade competente*": "[…] *a) [u]ma autoridade pública competente para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública; ou b) [q]ualquer outro organismo ou entidade designados pelo direito de um Estado-Membro para exercer a autoridade pública e os poderes públicos para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.*".

O regime de DUE derivado contém, em especial: princípios aplicáveis ao tratamento de dados (artigo 3.º) e licitude de tratamento (artigo 8.º, tendo em conta os fins do artigo 1.º, n.º1); tratamento de categorias especiais de dados (artigo 10.º); *limitações aos direitos dos titulares de dados* (artigo 13.º, n.º 3, alínea *b*)); e *limitações ao direito de acesso aos dados* (artigo 15.º, n.º 1, alínea *b*)) – todos *replicados* na Lei n.º 59/2019 (cfr. os respetivos artigos 4.º, 5.º, 6.º 16.º, n.º 1, alínea *b*) – e se os dados recolhidos forem tratados para fins diversos dos previstos no artigo 1.º, n.º 1, da Diretiva aplica-se, então, o RGPD (artigo 9.º, n.º 1, da Diretiva e artigo 8.º, n.º 1, da Lei n.º 59/2019).

Em suma, o *paradigma europeu* aplicável à questão em causa nos presentes autos – apreensão de dados pessoais diretamente por autoridade pública no exercício da ação penal junto do equipamento informático do visado – é outro, que não o decorrente da Diretiva 2002/58/CE e do RGPD: é o da licitude e da necessidade de tratamento dos dados em causa pelas autoridades públicas nacionais (diretamente) e o da consagração e admissibilidade de limites aos direitos dos titulares dos dados, incluindo quanto ao acesso aos mesmos e sua apreensão, para os específicos fins em causa.

Por assim ser, e diversamente do afirmado no final do ponto 20 do acórdão (e também no início do seu ponto 24), não pode relevar diretamente para o caso dos autos a consideração dos aí referidos "[…] *acervo legal e jurisprudencial da União Europeia acerca de temáticas paralelas*" e "[…] *'standards' de tutela*

jusfundamental no que respeita ao tratamento de dados pessoais e de dados relativos às comunicações, no âmbito da utilização da informática […]" (acervo jurisprudencial do Tribunal de Justiça que o Acórdão explicita, em particular, no seus pontos 23 e 25).

3.5. Este enquadramento específico de DUE implica, por um lado: *i)* a relevância acrescida do Direito nacional, especialmente, neste ca[14]do Direito constitucional nacional, desde logo quando este preveja níveis protetivos mais densos, sem prejuízo dos fins impostos pela harmonização decorrente da Diretiva (UE) 2016/680; *ii)* a convocação dos específicos parâmetros de constitucionalidade pertinentes para a análise da norma, que se situam, primeiramente, no quadro próprio do exercício da ação penal e, em concreto, das garantias do processo penal especialmente consagradas pela CRP no seu artigo 32.º, concretamente no seu n.º 4 em matéria de reserva do juiz. É pois, este, o parâmetro constitucional de referência com o qual deve ser fundamentalmente confrontada a norma sindicada.

4. É esta, enfim, a visão particular dos subscritores do presente voto, quanto a alguns pontos tratados no Acórdão. Não obstante as divergências antes explicitadas, estamos fundamentalmente perante argumentos que concorrem, na centralidade dos parâmetros constitucionais convocados, com o decidido pelo Tribunal na apreciação da redação do artigo 17.º da Lei n.º 109/2009, de 15 de setembro pretendida introduzir através do artigo 5.º do Decreto n.º 167/XIV.

J.A. Teles Pereira – Maria José Rangel de Mesquita

[1] Por *posição* (*opinião*) *concorrente* pretendem os subscritores desta declaração significar o entendimento corrente da expressão *voto concorrente*, na dinâmica decisória de um tribunal de recurso: uma concordância na decisão e mesmo na fundamentação que apresenta, todavia, certos pontos argumentativos separados da posição expressa pela maioria, que se podem somar (em alguns trechos poderiam mesmo substituir-se) a essa posição, mas que não deixam de a reafirmar embora com certo grau de autonomia argumentativa (cfr. as entradas "*concur*" e "*concurring opinion*", *in Black's Law Dictionary*, 6.ª ed., West Publishing Co., St Paul Minnesota, 1990, p. 291).

[2] "*O direito processual penal faz parte integrante da denominada 'ciência total do direito penal', onde se integra o direito penal em sentido amplo, a criminologia e a política criminal. É no direito penal em sentido amplo que, a par do direito penal (substantivo) e do direito da execução de penas e de medidas de segurança (direito penal executivo), se localiza o direito processual penal (direito adjetivo).*" (Maria João Antunes, *Direito Processual Penal*, Coimbra, 2017, p. 7).

[3] Isso mesmo consta do ponto 15 do Acórdão n.º 403/2015 (*Metadados I*):

"[…]

Já quanto aos dados de base (v.g. número de telefone, endereço eletrónico, contrato de ligação à rede) e aos dados de localização de equipamento, quando não dão suporte a uma concreta comunicação, não são objeto de proteção do direito ao sigilo das comunicações (cfr. Acórdão n.º 486/2009). De facto, se o objeto de proteção é uma comunicação individual, então os dados que não pressuponham uma concreta comunicação, que não façam parte do processo de comunicação, ainda que protegidos pela reserva da vida privada – artigo 26.º da CRP – não estão cobertos pela tutela do sigilo das comunicações.

[…]".

E, mais expressivamente, no Acórdão n.º 464/2019 (*Metadados II*), o Tribunal, na alínea b) do dispositivo, não declarou "[…] *a inconstitucionalidade da norma constante do artigo 3.º, da Lei Orgânica n.º 4/2017, de 25 de agosto, na parte em que admite o acesso dos oficiais de informações* [*do SIS e do SIED*]*, no âmbito das respetivas atribuições, relativamente a dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação, para efeitos de produção de informações necessárias à prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada* […]".

[4] João de Castro Mendes, *Limites Objectivos do Caso Julgado em Processo Civil*, Lisboa, 1968, p. 203.

[5] "*O artigo 17.º da Lei n.º 109/2009* […] *aplica-se à apreensão de mensagens de correio eletrónico ou registos de comunicações de natureza semelhante (como SMS, SEM, MMS, conversações no Messenger, mensagens de voz relativas a comunicações via Whatsapp, Viber, Skype, Facebook, etc.) que se encontrem armazenados no sistema informático que tenha sido acedido pelas autoridades e não à sua interceção em tempo real* […]" (Duarte Rodrigues Nunes, *Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime*, Coimbra, 2018, p. 140).

[6] "[…]

50. Assim, e uma vez que um acesso geral a todos os dados conservados, independentemente de qualquer ligação, no mínimo indireta, com o objetivo prosseguido, não pode ser considerado limitado ao estritamente necessário, a regulamentação nacional em causa deve basear-se em critérios objetivos para definir as circunstâncias e as condições em que o acesso aos dados em causa deve ser concedido às autoridades nacionais competentes. A este respeito, tal acesso só poderá, em princípio, ser concedido, em relação com o objetivo de luta contra a criminalidade, aos dados de pessoas que se suspeita estarem a planear, irem cometer ou terem cometido uma infração grave ou, ainda, estarem envolvidas de uma maneira ou de outra nessa infração. Todavia, em situações especiais, como aquelas em que os interesses vitais da segurança nacional, da defesa ou da segurança pública sejam ameaçados por atividades terroristas, o acesso aos dados de outras pessoas poderia igualmente ser concedido quando existam elementos objetivos que permitam considerar que esses dados poderiam, num caso concreto, contribuir efetivamente para a luta contra essas atividades (v., neste sentido, Acórdãos de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.° 119, e de 6 de outubro de 2020, La Quadrature du Net e o., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, n.° 188).

51. A fim de garantir, na prática, o pleno respeito destes requisitos, é essencial que o acesso das autoridades nacionais competentes aos dados conservados esteja, em princípio, sujeito a uma fiscalização prévia efetuada por um órgão jurisdicional ou por uma entidade administrativa

independente e que a decisão desse órgão jurisdicional ou dessa entidade seja tomada na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de perseguição penal. […]" (sublinhado acrescentado).

[7] "*No que respeita ao conteúdo essencial do direito fundamental ao respeito da vida privada e dos outros direitos consagrados no artigo 7.º da Carta, deve observar-se que, embora a conservação dos dados imposta pela Diretiva 2006/24* [invalidada pelo Acórdão *Digital Rights*] *constitua uma ingerência particularmente grave nesses direitos, não é suscetível de afetar o referido conteúdo, tendo em conta que, como resulta do seu artigo 1.º, n.º 2, esta directiva não permite tomar conhecimento do conteúdo das comunicações eletrónicas, enquanto tal.*" (quanto à definição dos dados conservados pelos operadores, no quadro da Diretiva 2006/24, cfr. o ponto 26 do mesmo Acórdão – "[…] *designadamente, os dados necessários para encontrar e identificar a fonte e o destino de uma comunicação, para determinar a data, a hora, a duração e o tipo de uma comunicação, o equipamento de comunicação dos utilizadores, bem como para localizar o equipamento de comunicação móvel, dados entre os quais figuram, designadamente, o nome e o endereço do assinante ou do utilizador registado, o número de telefone de origem e o número do destinatário e também um endereço IP para os serviços Internet*").

[8] "*U.S. Postal Service Logging All Mail for Law Enforcement*, disponível, em 25 de agosto de 2021, no sítio do jornal em: https://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html.

[9] Este exemplo concreto é utilizado por Amitai Etzioni (*Privacy in a Cyber Age*, Palgrave Macmillan, New York, 2015, pp. 132/133) para ilustrar o carácter incomensuravelmente insidioso, na sua potencialidade danosa de usos desviados, do acesso a sistemas que tratam, na sua vertente mais abrangente (a do próprio conteúdo, diversamente das simples circunstâncias envolventes), informação digitalizada: "[…] *a digitalização da informação, o uso generalizado da internet e de computadores, e a introdução de sistemas de inteligência artificial para analisar vastas quantidades de dados incrementaram a medida, o volume, o escopo e os tipos de usos secundários em tantos graus de magnitude que é difícil encontrar uma expressão apropriada para capturar a importância desta transformação. A questão essencial não é tanto o facto de a informação poder ser agora processada a uma fração do custo e a velocidades incomparavelmente maiores do que quando era feita a partir do papel, o que é certamente o caso, mas sim o facto de os modos de análise que fazem derivar nova informação pessoal de dados pessoais previamente recolhidos serem hoje comuns, mas eram inconcebíveis quando a maior parte da informação pessoal assentava em suporte de papel. Por outras palavras, prevenir a intrusão excessiva implicava menor recurso à Quinta Emenda quando a maior parte da informação pessoal assentava em papel, porque com frequência era simplesmente impossível armazenar e analisar grandes quantidades de informação pessoal – mas são necessárias proteções acrescidas agora que tais capacidades cresceram significativamente*" (*ibidem*, pp. 1/2).

[10] *Permanent Record*, Macmillan, Londres, 2019, p. 1. E o texto que estamos a citar segue com a seguinte explicação para esse fenómeno: "[*d*]*epois do 11 de setembro a CI ficou esmagada pela culpa de não ter conseguido defender a América, por ter deixado que o ataque mais devastador e destrutivo* […] *desde Pearl Harbor acontecesse no seu tempo* [a expressão exata é "*on its watch*"]" (*ibidem*, pp. 1/2).

[11] Designadamente, cfr. a entrevista, de janeiro de 2014, do General Michael Hayden, Director da NSA em 11 de setembro, ao site *Frontline*: https://www.pbs.org/wbgh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-michael-hayden.

Remetemos aqui para o que se refere, a propósito da chamada *Verizon Order* do FISA Court, na nota 43 do voto do primeiro subscritor da presente declaração no Acórdão n.º 464/2019.

[12] "[*S*]*egundo a qual, sem prejuízo das disposições adotadas em aplicação das Diretivas 95/46 e 2002/58, deveriam ser respeitados certos princípios de proteção e de segurança dos dados pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, princípios de acordo com os quais os Estados-Membros devem assegurar a adoção de medidas técnicas e organizacionais adequadas contra a destruição acidental ou ilícita, a perda ou a alteração acidental dos dados*".

[13] Cfr. Marcus Klamert, anotação D ao artigo 16.º do TFUE, *in* Manuel Kellerbauer, Marcus Klamert, Jonathan Tomkin (eds.), *The EU Treaties and The Charter of Fundamental Rights, A Commentary*, Oxford University Press, Oxford, 2019, pp. 409/410.

[14] "*A Diretiva 2016/680 estabelece mínimos de harmonização, permitindo aos Estados membros a adoção de padrões mais elevados (artigo 1(2) da Diretiva* […]. *Os Estados membros são instados a estabelecer limites de tempo para o apagamento de dados pessoais ou para uma revisão periódica da necessidade de permanência do armazenamento destes. E são também instados a estabelecer tratamentos diferenciados, e outras partes*

no processo, como entre os dados pessoais de suspeitos do cometimento de crimes, de condenados, de vítimas ou de possíveis vítimas e terceiros envolvidos, como sucede com testemunhas" (Marcus Klamert, anotação indicada na nota 10, *supra*, pp. 409/410; cfr. artigos 5.º e 6.º da Diretiva 2016/680).