SEPARATA RPDC N.º 1 (2021)

REVISTA PORTUGUESA DE DIREITO CONSTITUCIONAL

PORTUGUESE REVIEW OF CONSTITUTIONAL LAW

AATRIC

A apreensão de correio electrónico após o Acórdão do Tribunal Constitucional n.º 687/2021: *do* juiz das liberdades *ao* juiz purificador investigador?*

Rui Cardoso

Procurador da República; *Docente no Centro de Estudos Judiciários*
rui-cardoso@outlook.pt

Resumo: No Acórdão n.º 687/2021, o Tribunal Constitucional pronunciou-se pela primeira vez sobre o regime de apreensão do correio electrónico. Embora sendo em sede de fiscalização preventiva, as posições que assumiu – que extravasam o regime de apreensão de correio electrónico e implicam directamente com todo o regime de pesquisa e apreensão de dados informáticos – e as consequências que poderão ter para a interpretação da lei vigente e para qualquer alteração que a esse regime venha a ser feita exigem análise, reflexão e comentário imediatos, o que neste artigo se tenta fazer. De entre os vários possíveis regimes legais para a delimitação recíproca da competência de Ministério Público e juiz de instrução na pesquisa e apreensão de dados informáticos, alguns devem ser afastados por desconformidade constitucional: ou por não preverem qualquer intervenção do juiz de instrução, ou por preverem demasiada intervenção do mesmo, ofendendo a estrutura acusatória do processo, o exercício da acção penal pelo Ministério Público e até a função do juiz de instrução no sistema de garantias de defesa. Quer o regime vigente, interpretado no sentido de que a intervenção do juiz de instrução é apenas para decidir da utilização

* Por opção do Autor, o presente texto segue a ortografia anterior ao Acordo Ortográfico em vigor desde 2009.

probatória dos dados, quer um outro (dependente de alteração legislativa), em que seja dele a autorização para a pesquisa e apreensão (sem qualquer intervenção posterior) são conformes à Constituição.

Abstract: In the Ruling no. 687/2021, the Constitutional Court addressed for the first time the legal regime of seizure of electronic correspondence. Although the Ruling was delivered in a context of preventive constitutionality control, the positions upheld therein – which go beyond the seizure of electronic correspondence and touch directly upon the whole regime of search and seizure of informatic data –, and the consequences that they may have upon the interpretation of the law as it currently stands and as it may come to be amended, require immediate analysis and commentary. From the several possible legal solutions of reciprocal delimitation of competences between the Public Prosecution and the judge of instruction in the search and seizure of informatic data, some must be set aside due to disconformity with the Constitution: whether because they do not involve any intervention whatsoever or because they involve excessive intervention by the judge, thus hampering upon the accusatorial structure of the criminal procedure, the exercise of penal action by the Public Prosecution and even the function of the judge of instruction in the system of defence guarantees. Both the legal regime currently in place, if interpreted in the sense that the intervention of the judge is limited to deciding on the use of the data as evidence, and any other legal regime that may come to be enacted whereby the judge is competent for authorizing the search and seizure of the data (with no further intervention on his/her part) comply with the Constitution.

Palavras-chave: prova digital; pesquisa e apreensão de dados informáticos; correio electrónico; reserva de juiz; acusatório; proporcionalidade; inviolabilidade da correspondência e das comunicações; protecção dos dados pessoais no âmbito da utilização da informática; reserva de intimidade da vida privada; protecção da vítima.

Keywords: digital evidence; search and seizure of informatic data; e-mail; mandatory intervention by a judge; accusatorial principle; proportionality; inviolability of correspondence and communications; data protection in the digital sphere; privacy; victim protection.

I – Introdução

1. O Acórdão n.º 687/2021

O Tribunal Constitucional (TC), em plenário (mas com metade dos membros por se tratar de período de férias), apreciou um requerimento de fiscalização abstracta preventiva da constitucionalidade do Presidente da República (PR) que tinha por objecto as normas do artigo 5.º do Decreto n.º 167/XIV, da Assembleia da República (AR), na parte em que alterava o artigo 17.º da Lei n.º 109/2009 (conhecida como Lei do Cibercrime – LCC), respeitante à apreensão de correio electrónico.

Por unanimidade (mas com duas declarações de voto), através do Acórdão n.º 687/2021[1] (doravante, apenas "Acórdão"), relatado pela Conselheira Mariana Canotilho, o TC pronunciou-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» (CRP).

As normas em causa eram as seguintes:

> «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

[1] Disponível, como todos os demais acórdãos deste tribunal citados, em www.tribunalconstitucional.pt.

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.»

Apreciando o requerido, o Acórdão coloca as seguintes questões:
«- 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)?»

A ambas responde negativamente, concluindo 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)» (ponto 46).

Na sequência do Acórdão, o PR vetou o Decreto e depois a AR dele retirou a alteração do artigo 17.º da LCC.

2. Razão de ordem

É a primeira vez que o TC efectivamente se pronuncia sobre o regime de apreensão do correio electrónico, e, embora sendo em sede de fiscalização preventiva, as posições que agora assume – que extravasam o regime de apreensão de correio electrónico e implicam directamente com todo o regime de pesquisa e apreensão de dados informáticos – e as consequências que poderão ter para a interpretação da lei vigente (já aplicada a muitos processos pendentes e aplicável a processos pendentes e futuros) e para qualquer alteração que a esse regime venha a ser feita exigem análise, reflexão e comentário imediatos.

É isso que me impõe voltar a este tema,[2] cada vez mais relevante no processo penal, sempre presente, dos crimes mais simples e menos graves aos mais complexos e mais graves.

Assim, no comentário ao Acórdão (II), depois de uma apreciação genérica do mesmo (II.1), analisarei a possível inconstitucionalidade por violação do princípio da proporcionalidade e de direitos fundamentais (II.2) e por violação de reserva de juiz e das garantias de defesa (II.3). Neste ponto, o único em que, em meu entender, poderia ser encontrada alguma inconstitucionalidade, começarei por apresentar os vários possíveis regimes legais de apreensão de dados informáticos, conjugando pesquisa e apreensão, intervenção prévia e intervenção posterior do JIC, a competência deste e a do Ministério Público (MP) (II.3.1), passando depois a tentar fornecer alguns esclarecimentos técnicos sobre o correio electrónico e semelhante (II.3.2.) e a execução da pesquisa e da apreensão indispensáveis à apreciação desses regimes (II.3.3); continuarei fazendo a análise desses possíveis

[2] Sobre o qual escrevi "Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei n.º 109/2009, de 15.IX", *Revista do Ministério Público*, 153, Janeiro-Março (2018), pp. 167-214, que em vários pontos seguirei de perto.

regimes (II.3.4), formulando uma conclusão (II.3.5). Encerrarei a análise do Acórdão com o comentário à declarada inconstitucionalidade das normas não apreciadas (II.4). Terminarei o artigo com algumas considerações sobre as consequências que poderão advir deste Acórdão para a interpretação do regime actual (como foi este aplicado a processos pendentes e se deverá haver alguma alteração na sua futura interpretação) e sobre eventuais alterações legislativas (III).

II – Comentário ao Acórdão

1. Apreciação genérica

a) Na fundamentação do Acórdão, o TC evidencia imprecisão ou mesmo alguns equívocos sobre o regime vigente de prova digital, em especial sobre a apreensão de dados informáticos e, mais ainda, sobre a realidade a que se aplica tal regime, o que condiciona o juízo que acaba por emitir.

b) Desde logo, carecem de fundamento as dúvidas expressas no ponto 32 do Acórdão sobre o âmbito de aplicação da apreensão de correio electrónico. A LCC contém um verdadeiro regime geral de prova digital, sendo as disposições processuais previstas nos seus artigos 12.º a 17.º aplicáveis, em abstracto, a qualquer tipo de crime. Efectivamente, por força do disposto no n.º 1 do artigo 11.º, aplicam-se elas (incluindo, pois, as respeitantes a correio electrónico, artigo 17.º), a processos relativos a crimes (a) previstos nessa lei, (b) cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, ou seja, repete-se, em abstracto, *a todos os tipos de crime*, pois em qualquer deles pode ser necessário recolher prova em suporte electrónico e quase todos eles podem ser cometidos por meio de um sistema informático. Nestes termos, no regime hoje vigente, *as mensagens de correio electrónico ou similares são utilizáveis como meio de prova de qualquer crime*. Nesse aspecto não havia qualquer alteração pelo Decreto apreciado, contrariamente ao afirmado no Acórdão.

c) O Acórdão revela incompreensão sobre o regime vigente de apreensão de dados informáticos e a divisão de competências nele feita entre MP e JIC (no inquérito). No artigo 16.º não se prevê sempre a intervenção prévia do JIC (como afirmado no ponto 38 do Acórdão): só excepcionalmente tal sucede (e não é no caso do n.º 3).

A apreensão de dados informáticos[3] está prevista nos artigos 16.º e 17.º da LCC. Contém o regime geral (nos n.ºs 1 e 2 do artigo 16.º) e quatro regimes especiais. São estes: i) para dados pessoais ou íntimos (16.º, n.º 3); ii) para sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária, sistemas informáticos utilizados para o exercício da profissão de jornalista (16.º, n.º 5); iii) para sistemas informáticos contendo segredo profissional ou de funcionário e de segredo de Estado (16.º, n.º 6); iv) para as mensagens de correio electrónico ou registos de comunicações de natureza semelhante (artigo 17.º).

Como regime-regra, a apreensão deve ser feita por ordem ou autorização da autoridade judiciária competente (que, no inquérito, será o MP) – n.º 1. Apenas excepcionalmente podem os OPC's efectuar apreensões – n.º 2. Neste caso, as apreensões são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas – n.º 4.

Estabelece o n.º 3 que, «[c]aso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto». Aplica-se apenas a dados ou documentos informáticos *já apreendidos*, cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, mas não quaisquer dados pessoais ou íntimos: apenas aqueles que possam pôr em causa a privacidade do respectivo titular ou de terceiro. Tratando-se de dados íntimos, por regra estará sempre em causa a privacidade do titular ou terceiro; tratando-se de dados pessoais, apenas quando estes sejam sensíveis, como diários, dados de saúde, de práticas religiosas, *etc*. (excluindo outros dados pessoais como nome, morada, números de cartões de identificação, número de telefone, e-mail, e quaisquer dados que sejam do conhecimento público, *v. g*., em redes sociais).[4] Durante o inquérito, o MP deverá apresentar estes dados, apesar de já apreendidos, ao JIC em suporte autónomo com requerimento fundamentado sobre a

[3] Não se deve confundir apreensão de dados informáticos, a que se aplica o disposto nos artigos 16.º e 17.º da LCC, com apreensão de objectos que são sistemas informáticos (computadores, discos, telemóveis, *etc*.), a que se aplica o regime das buscas, revistas e apreensões previsto no CPP. A mera apreensão destes enquanto coisas não permite a utilização probatória dos dados neles contidos.

[4] Para Tiago Caiado Milheiro, "Comentário ao artigo 189.º", in *Comentário Judiciário ao Código de Processo Penal*, António Gama *et al*, Coimbra: Almedina, 3.ª ed., 2021, p. 861, «o legislador não pretendeu que todos os documentos eletrónicos sejam objeto de apreciação por parte de um juiz. Mas apenas os documentos que impliquem uma especial ponderação de valores em virtude de uma forte intrusão de privacidade como sejam os diários».

sua relevância para a prova dos factos em investigação.[5] O JIC apreciará o requerido pelo MP e decidirá sobre a sua junção ou devolução [em caso de apreensão pela forma prevista no n.º 7, alínea a)] ou destruição [em caso de apreensão pela forma prevista no n.º 7, alínea b)]. Da redacção deste n.º 3 resulta claro que, mesmo tratando-se de dados íntimos ou sensíveis, *o legislador apenas previu a intervenção do juiz no momento posterior à pesquisa e ao conhecimento e apreensão dos mesmos por parte do MP.*[6]

As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e da actividade médica estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no artigo 180.º do CPP; para o exercício da actividade bancária, estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no artigo 181.º do CPP; para o exercício da profissão de jornalista, estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista (artigo 11.º da Lei 64/2007) – n.º 5. O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do CPP é aplicável com as necessárias adaptações – n.º 6. Por força dessas remissões, exige-se intervenção prévia do JIC.

d) O Acórdão evidencia claramente o entendimento de que a apreensão de correio electrónico deve seguir o regime da apreensão de correio físico. Esse entendimento está patente na leitura de que o actual artigo 17.º faz uma remissão em bloco para o disposto no artigo 179.º do CPP, que seria substituída, na versão aqui em crise, por uma previsão de aplicação subsidiária e com as necessárias adaptações do disposto naquela norma do CPP – ponto 15, §4. Ora, a *aplicação correspondente* do regime do artigo 179.º do CPP deve hoje ser exactamente essa: de *aplicação subsidiária e com as necessárias adaptações*. Só se pode aplicar esse regime naquilo que não estiver especialmente previsto na LCC: a remissão para o CPP não pode sobrepor-se ao regime especial de prova electrónica previsto na LCC.[7] Assim, exemplificando:

[5] Apesar da especial ofensa a direitos fundamentais em causa, o n.º 3 deste artigo 16.º não apresenta qualquer real critério adicional de relevância probatória ("interesses do caso concreto"?... não acontecerá isso com qualquer meio de prova em qualquer processo?), mas a CRP sempre exigirá reforçadas necessidade, adequação e proporcionalidade.

[6] Não é, pois, correcta a afirmação no Acórdão de que o artigo 16.º estabeleça a exigência de intervenção primária do JIC, bem como a necessidade de este ser o primeiro a tomar conhecimento do conteúdo dos dados apreendidos (ponto 38).

[7] O elemento histórico aponta no mesmo sentido. A mera leitura da Exposição de Motivos da Proposta de Lei n.º 289/X/4.ª, que esteve na origem da LCC, evidencia que o Governo, reconhecendo a «desadequação da ordem jurídica nacional às novas realidades a implementar», não pretendeu fazer uma mera extensão do regime das buscas e apreensões previsto no CPP à prova digital, antes assumindo

- no CPP, o âmbito objectivo é o de correspondência em trânsito ou ainda não aberta; na LCC, todas as mensagens de correio electrónico ou semelhantes, não havendo verdadeiramente regime aberto-lido *vs* fechado-não lido;[8]
- no CPP, a apreensão de correspondência só é meio de obtenção de prova admissível para crimes puníveis com pena de prisão superior, no seu máximo, a 3 anos; na LCC, não há catálogo, como visto;
- finalmente, no CPP é o juiz que, num primeiro momento, determina a apreensão de cartas, encomendas, valores, telegramas ou qualquer outra correspondência, e, depois, que determina a junção ao processo da que considerar relevante para a prova; na LCC, a intervenção do juiz só está prevista para o segundo momento (o da apreensão para utilização probatória).

Neste aspecto, o novo regime não continha, pois, qualquer alteração no que respeita à relação entre o artigo 17.º da LCC e o artigo 179.º do CPP.

e) Ponto central do Acórdão, com o qual não tenho divergências significativas, é o da identificação dos direitos fundamentais que podem

a vontade de proceder a uma adaptação desse regime, superando-o quando necessário: «a forma como a busca e a apreensão estão descritas no CPP exigiam alguma adequação a estas novas realidades». O legislador propôs-se adaptar estes regimes, não aplicá-los integral e acriticamente.

[8] Aspecto em que concordo com o Acórdão. Como expus antes ("A apreensão de correio electrónico…", *ob. cit.*, pp. 186-188), creio que não existe fundamento jurídico ou técnico para fazer qualquer distinção entre correio electrónico recolhido e não recolhido, aberto e não aberto, lido e não lido.
Afigura-se-me então que não é prestável a definição de correio electrónico que consta da Lei n.º 41/2004 – invocada no Acórdão –, que, no seu artigo 2.º, alínea b), o define 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*» (realces meus). Para além de se dever incluir o correio electrónico em redes privadas (tecnicamente muito diferente daquele transmitido por redes públicas, mas, para o utilizador, materialmente idêntico, e por isso com o mesmo perigo de ofensa a direitos fundamentais e com a mesma necessidade de protecção), há que notar que, com os novos protocolos de e-mail (*IMAP, Exchange*), mensagem entregue é mensagem recolhida, pois no momento em que entra no servidor de recepção este entrega-a nos programas-cliente (programas que correm no computador do utilizador) de correio electrónico do destinatário (como é do conhecimento empírico de qualquer pessoa que tenha hoje um *smartphone* com um programa de correio electrónico).
O protocolo *SMTP* (*Simple Mail Transfer Protocol*) é usado quando o e-mail é enviado de um cliente de e-mail para um servidor de e-mail ou quando o e-mail é enviado de um servidor de e-mail para outro. Permite apenas enviar e-mails. Para receber é necessário um protocolo *POP3* (*Post Office Protocol*). O *POP3* permite que um cliente descarregue o e-mail de um servidor de e-mail para um programa cliente. Despois de descarregado, o e-mail é apagado do servidor. *IMAP* significa *Internet Message Access Protocol*. Tal como o POP3, é um protocolo que um cliente de e-mail pode usar para fazer *download* de e-mails de um servidor de e-mail, mas, ao contrário deste, permite que os utilizadores mantenham os seus e-mails no servidor e os descarreguem para diferentes programas clientes em diferentes sistemas (*PC's, tablets, smartphones, etc.*). A *Microsoft* usa um protocolo seu, o *Exchange ActiveSync*, muito similar ao *IMAP*. Hoje, todos os grandes fornecedores de e-mail (*Gmail, Outlook, Yahoo, Apple Mail, Hotmail* e, em Portugal, o *Sapo*) usam protolocos *IMAP* ou *Exchange*, estando o *POP3* ultrapassado ("morto", para muitos).

ser afectados pela pesquisa, apreensão e utilização probatória de dados informáticos, *v. g.*, de correio electrónico,[9] direitos fundamentais esses que, por isso mesmo, exigem um especial regime de garantia e protecção. Qual seja esse regime foi o analisado pelo TC, fundamentou a pronúncia de inconstitucionalidade e exige agora comentário.

2. Proporcionalidade e violação de direitos fundamentais

No Acórdão, o Tribunal começa por afirmar que «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 protecção 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» (ponto 41, 4§), para, porém, depois concluir no sentido de que «[…] 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» (ponto 44, 1§).[10] Esse pensamento fica mais claro adiante, quando conclui 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

[9] Cf. Rui Cardoso, "Apreensão de correio electrónico…", *ob. cit.*, pp. 175-179. Também Paulo Sousa Mendes, "A privacidade digital posta à prova no processo penal", *Revista do Ministério Público*, 165, Janeiro-Março (2021), pp. 109-143 (*passim*), e Alexandre Au-Yong Oliveira, "Prelúdios a uma revisitação da Lei do Cibercrime no âmbito da prova digital", in Paulo Pinto de Albuquerque / Rui Cardoso / Sónia Moura (org.), *Corrupção em Portugal – Avaliação legislativa e propostas de reforma*, Lisboa: Universidade Católica Editora, 2021, pp. 529 e ss., que refere ainda o direito à confidencialidade, integridade e disponibilidade de sistemas informáticos (p. 532).

[10] Neste ponto segue o parecer da Comissão Nacional de Protecção de Dados, que cita: «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».

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)» (ponto 46).

Ou seja, para o TC, as exigências de *excepcionalidade* [?], *necessidade* e *proporcionalidade* a que deve obedecer este meio de prova (dados informáticos de mensagens de correio electrónico) só estarão satisfeitas se for um juiz a permitir a sua produção e utilização. Esta é uma ideia verdadeiramente inovadora e, salvo melhor opinião, altamente problemática.

Inovadora face à doutrina e jurisprudência mais importantes, incluindo a do próprio TC,[11] que nunca haviam chegado a tal conclusão. Segundo Gomes Canotilho e Vital Moreira,[12] «o princípio da proporcionalidade (também chamado *princípio da proibição do excesso*) desdobra-se em três subprincípios: (a) *princípio da adequação* (também chamado por *princípio da idoneidade*), isto é, as medidas restritivas legalmente previstas devem revelar-se como meio adequado para a prossecução dos fins visados pela lei (salvaguarda de outros direitos ou bens constitucionalmente protegidos); (b) *princípio da exigibilidade* (também chamado *princípio da necessidade* ou da *indispensabilidade*), ou seja, as medidas restritivas previstas na lei devem revelar-se necessárias (tornaram-se exigíveis), porque os fins visados pela lei não podiam ser obtidos por outros meios menos onerosos para os direitos, liberdades e garantias); (c) *princípio da proporcionalidade em sentido restrito*, que significa que os meios legais restritivos e os fins obtidos devem situar-se numa "justa medida" impedindo-se a adopção de medidas legais restritivas desproporcionadas, excessivas, em relação aos fins obtidos».[13] Autores estes que afirmam expressamente a sujeição das *intervenções restritivas,* sejam normativas ou concretas – «actos ou actuações das autoridades públicas, restritivamente incidentes, de modo concreto e imediato, sobre um direito, liberdade e garantia ou direito de natureza análoga» – *v. g.*, decisões judiciais,

[11] Recentemente, sobre o princípio da proporcionalidade na justiça constitucional, cf. Ana Raquel Gonçalves Moniz, "Juízo(s) de proporcionalidade e justiça constitucional", *Revista da Ordem dos Advogados*, 80, n.º 1-2, Janeiro-Junho (2020), pp. 41-71 (também publicado *online*: http://www.doi.org/10.47907/clq2021_2a2).

[12] *Constituição da República Portuguesa Anotada. Vol. I*, 4.ª ed., Coimbra: Coimbra Editora, 2007, pp. 392-393.

[13] Jorge Miranda / Jorge Pereira da Silva, ("Comentário ao artigo 18.º", in Jorge Miranda / Rui Medeiros (org.), *Constituição Portuguesa Anotada. Vol. I*, Lisboa: Universidade Católica Editora, 2.ª ed. revista, 2017, pp. 274 e ss., adoptam classificação e desdobramento similares. Com algumas diferenças, Jorge Reis Novais, *Os princípios constitucionais estruturantes da República Portuguesa*, Coimbra: Coimbra Editora, 2004, pp. 161-194.

ao princípio da proibição do excesso, integrado pelos já referidos três testes: adequação, necessidade e proporcionalidade em sentido estrito.[14-15]

Concretizando estes princípios no que respeita às medidas de aquisição de prova no processo penal, Paulo Pinto de Albuquerque[16] refere que «a idoneidade da medida reporta-se à aptidão objectiva (potencialidade) da medida para alcançar o fim visado»; «a necessidade da medida reporta-se à comparação dos efeitos nocivos da medida, devendo optar-se pela medida menos lesiva»; «a proporcionalidade em sentido estrito da medida reporta-se à adequação material da medida ao fim visado e aos danos causados, o que inclui a ponderação da gravidade do crime indicado, o grau de suspeita dos indícios, a sanção previsível, as consequências da medida, incluindo o tempo de duração da medida».

No processo penal, estes princípios e seus subprincípios não se confundem, em momento algum, com a categoria da entidade que decide a medida. São dela separados, autónomos, impondo-se na mesma exacta dimensão a todos: sejam juízes, sejam procuradores. No plano legislativo, a determinação da adequação/idoneidade, necessidade e proporcionalidade da medida probatória em causa é feita *ex ante*, em abstracto, entre a mesma e a sua idoneidade para obter a prova que se pretende, ponderando a possibilidade de afectar direitos fundamentais e colocando estes em confronto com a gravidade dos crimes para cuja prova pode ser utilizada e os bens jurídicos por eles protegidos; no plano adjectivo, na sua aplicação processual, tal determinação é feita apenas de acordo com as circunstâncias factuais do caso concreto, no concreto momento da decisão. Em nenhum momento, pois, levando em consideração a identidade de quem no processo o decide.

Ora, as normas em apreciação não respeitavam ao âmbito de aplicação desta medida de investigação: nem subjectivo (pessoas que por ela podem ser visadas), nem objectivo (tipo de crimes para cuja prova é, em abstracto,

[14] *Op. cit.*, p. 388.

[15] Assim também Raul Soares da Veiga, "O Juiz de Instrução e a Tutela de Direitos Fundamentais", in Maria de Fernanda Palma (coord.), *Jornadas de Direito Processual Penal e Direitos Fundamentais*, Coimbra: Almedina, 2004, p. 186: «Este imperativo de que as restrições a direitos fundamentais sejam limitadas por critérios de necessidade e de proporcionalidade, orientados pela importância do ataque a direitos fundamentais que é imputada ao arguido, emerge directamente do art. 18.º, n.º 2, da Constituição e tanto se dirige ao legislador, no plano das ponderações abstractas de valores que subjazem à feitura das leis processuais penais, como aos aplicadores destas leis, no plano das ponderações concretas que subjazem aos actos das autoridades judiciárias (e portanto necessariamente também às que subjazem aos actos das entidades policiais)».

[16] *Comentário do Código de Processo Penal*, Lisboa: Universidade Católica Editora, 4.ª ed., 2011, p. 475. Cf. ainda, com profunda análise do tema, Maria de Fátima Mata-Mouros, *Juiz das Liberdades: desconstrução de um mito do processo penal*, Coimbra: Almedina, 2011, pp. 252-264.

admissível). Tão pouco às exigências de proporcionalidade (em sentido lato) que em cada caso deveriam ser respeitadas.[17] Nesses aspectos, em nada alterava, pois, a lei vigente. O que estava em causa era apenas a intervenção do JIC.

Por isso mesmo, a posição do TC é altamente problemática. Por passar a fazer depender a proporcionalidade de um concreto meio de obtenção de prova da entidade que o decide. Será menor a restrição de direitos fundamentais do cidadão caso a decisão seja de um juiz? Para o cidadão visado, qual será a diferença? Sentirá menos restringidos os seus direitos fundamentais? Aquilo que é desnecessário, inadequado ou desproporcional passará a ser necessário, adequado e proporcional se for ordenado por juiz? Com que fundamento? Pelo seu "toque independente"? Não se estará assim a metamorfosear o JIC de *juiz das liberdades* em *juiz purificador*, que com o seu toque tornará admissível o que não o era?

Altamente problemática ainda por considerar que só um juiz pode satisfazer tais exigências, pondo dramaticamente em causa uma multiplicidade de importantes institutos do processo penal e, por isso, a própria estrutura acusatória do mesmo (artigo 32.º, n.º 5, da CRP). O princípio que decorre do n.º 2 do artigo 18.º da CRP impõe-se também ao MP – e até aos OPC's – em todas as suas actuações onde possa estar em causa a restrição de direitos fundamentais, e onde muitas vezes efectivamente está em medida significativa. Recorde-se, p. ex., a detenção fora de flagrante delito e a manutenção ou libertação do detido em flagrante delito (em que uma pessoa pode ficar totalmente privada da liberdade até 48 horas), as buscas (mesmo as domiciliárias, nos casos em que excepcionalmente a CRP e o CPP o permitem), as revistas, as apreensões, *etc*. Não sendo constitucionalmente sustentável dispensar o MP de obediência a tal princípio,[18] e, paradoxalmente, se não se lhe reconhecer a competência para em concreto o aplicar – e fazê-lo na mesma exacta medida que o juiz –, nada mais restará do que reservar todos esses actos ao JIC. Com isso ficará inviabilizada a direcção do inquérito pelo MP, tendo esta de ser assumida pelo juiz. Juiz que assim passará a *juiz purificador investigador*.

As mesmas exactas razões devem afastar o nexo relacional entre a violação de reserva de juiz e a violação dos direitos fundamentais identificados:

[17] O critério de necessidade probatória mantinha-se exactamente o mesmo: *grande interesse para a descoberta da verdade ou para a prova*.

[18] «[…] dada a passividade característica dos tribunais, a sua vinculação a direitos, liberdade e garantias tem de ser articulada com a vinculação do Ministério Público, que, enquanto garante da legalidade democrática e titular da acção penal, assume um papel de superlativa relevância na tutela preventiva e repressiva dos cidadãos […]» – Jorge Miranda / Jorge Pereira da Silva, *ob. cit.*, p. 244.

esta existirá ou não independentemente de ser juiz ou procurador a decidir o acto.

Concluo, pois, no sentido de que a exigência de proporcionalidade (em sentido lato) e a potencial ofensa aos direitos fundamentais (inviolabilidade da correspondência e das comunicações, protecção dos dados pessoais no âmbito da utilização da informática, reserva de intimidade da vida privada), nada têm que ver com a entidade que decide o recurso ao meio de obtenção de prova / a utilização do meio de prova; não se confundem, enfim, com a reserva de juiz prevista no n.º 4 do artigo 32.º.

É então apenas neste ponto que pode residir a inconstitucionalidade das normas apreciadas.[19] O que passo a analisar.

3. Reserva de juiz e garantias de defesa

3.1. Regimes legais possíveis

a) Sendo indiscutível, como vimos, a potencial restrição de direitos fundamentais que pode haver com a apreensão de mensagens de correio electrónico e semelhantes, é igualmente inquestionável que, por força do disposto no n.º 4 do artigo 32.º da CRP, deve nela haver intervenção do JIC. Igualmente se afigura correcto o entendimento de que, estando em causa possíveis ingerências graves em direitos fundamentais, a intervenção reservada ao juiz no inquérito deverá, *tanto quanto possível*, consistir numa *intervenção prévia*, devendo ser vista como excepcional a intervenção do juiz que surge apenas após o início da execução da medida.[20] No entanto, há que não esquecer que, como repetidamente tem afirmado o TC, uma vez que a reserva de juiz comprime a reserva do MP na direcção do inquérito, *ela só se justifica na medida do necessário para a protecção efectiva dos direitos, liberdades e garantias dos cidadãos* – cf., p. ex., Acs. 387/2019, 474/2012, 412/2011 e 234/2011. O próprio Acórdão em comentário, citando o Acórdão 121/2021, expressa a necessidade de ser respeitada a estrutura acusatória do processo, a direcção do inquérito pelo MP e a função do JIC no inquérito como juiz das liberdades e não como juiz investigador (ponto 31).

[19] A declaração de voto dos Conselheiros José António Teles Pereira e Maria José Rangel de Mesquita no Acórdão parece ir no mesmo sentido, concluindo que «[…] 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».

[20] Cf. Maria de Fátima Mata-Mouros, *ob. cit.*, p. 185.

Cabe então determinar qual deve ser a intervenção do JIC: quando, de que forma e com que finalidade, conjugando pesquisa e apreensão, intervenção prévia e intervenção posterior, a sua competência e a do MP. São cinco, em traços largos, as possibilidades que se colocam:[21]

1. Depois de pesquisa e apreensão cautelar (sem análise do seu conteúdo) pelos OPC's/MP, o MP apresenta-as ao juiz, que é o primeiro a delas tomar conhecimento e determina a apreensão das que considere relevantes;
2. Depois de pesquisa e apreensão cautelar pelos OPC's/MP, o MP, analisando-as, apresenta-as ao juiz com proposta fundamentada da sua relevância individual; o juiz toma delas conhecimento e aprecia o requerimento do MP (apreendendo ou não);
3. A requerimento do MP, o juiz autoriza a pesquisa de mensagens de correio electrónico; realizada esta pelos OPC's/MP, o MP, sem as analisar, apreende-as cautelarmente e apresenta-as ao juiz, que é o primeiro a delas tomar conhecimento e determina a apreensão das que considere relevantes;
4. A requerimento do MP, o juiz autoriza a pesquisa de mensagens de correio electrónico; realizada esta pelos OPC's/MP, o MP apreende-as cautelarmente, analisa-as e apresenta-as ao juiz com proposta fundamentada da sua relevância individual; o juiz toma delas conhecimento e aprecia o requerimento do MP (apreendendo ou não);
5. A requerimento do MP, o juiz autoriza a pesquisa e apreensão de mensagens de correio electrónico; esta é realizada pelos OPC's/MP; o MP analisa e apreende as que considera relevantes.

Apreciando a posição assumida pelo TC, mas tendo também em vista a subsistente necessidade de revisão da LCC,[22] há que determinar se todas estas soluções são conformes à CRP e, face às que o sejam, qual será a mais adequada à aquisição da prova.

Um importante aspecto deve ser sublinhado e ponderado. Apesar de o Acórdão se pronunciar apenas sobre a apreensão do correio electrónico, a potencialidade ofensiva a direitos fundamentais existe, em maior ou menor medida, com todas as apreensões de dados informáticos. Há sempre a possibilidade de, na apreensão de dados em sistemas informáticos de uso pessoal (*PC's, tablets, smartphones, wearables, etc.*), existir conhecimento de dados pessoais íntimos ou sensíveis e violação do direito à reserva de intimidade da

[21] Não se incluindo aqui os regimes especiais respeitantes a segredos profissionais protegidos, já referidos, em que há sempre intervenção prévia do JIC.

[22] Com um pormenorizado e fundamentado roteiro das necessidades de revisão do nosso regime de prova digital, cf. Alexandre Au-Yong Oliveira, "Prelúdios...", *ob. cit.*

vida privada. Como vimos, para esses casos a LCC apenas prevê a intervenção do juiz depois de os dados estarem já apreendidos e com a finalidade de decidir sobre a sua utilização probatória (a "junção"). Para além disso, a apreensão de correio electrónico anda necessariamente ligada à apreensão de outros dados informáticos.[23] A posição que se adopte pode, pois, exigir o seu alargamento a outras dimensões do regime de pesquisa e apreensão de dados informáticos.

b) O Acórdão evidencia o entendimento de que a apreensão de correio electrónico deve seguir o regime da apreensão de correio físico. Coloca grande ênfase em ter de ser o juiz o primeiro a tomar conhecimento do conteúdo das mensagens de correio electrónico apreendidas (ponto 11, 1§; ponto 38, 2§) e no afastamento que a norma apreciada traria face ao regime de apreensão de correspondência previsto no artigo 179.º do CPP, em cujo n.º 3 está expresso que o «juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida».

Porém, essas duas formas de comunicação à distância não são equiparáveis e, se fosse feita tal equiparação em termos exactos, o regime de apreensão de correio electrónico ficaria quase sem aplicação, pois, por regra, a apreensão só acontece quando o processo de comunicação está já terminado, com as mensagens entregues ao destinatário, circunstância que, no mundo corpóreo, as deixa fora do campo de aplicação do artigo 179.º do CPP. Por outro lado, a CRP, embora não distinguindo as diferentes formas de correspondência, não exige que a protecção seja feita de forma exactamente igual.

Antes de prosseguir na análise, há, pois, que atentar com maior detalhe nas diferenças entre essas duas formas de "correspondência" e nas operações técnicas envolvidas na apreensão da electrónica.

3.2. A apreensão do correio electrónico e do correio corpóreo: entre a realidade e alguns mitos

a) Não se deve olhar para o correio electrónico como se olha para o correio físico e tentar apreender e analisar aquele como se apreende e analisa este.

Desde logo, há que não esquecer que o regime se aplica não só ao correio electrónico como também aos «registos de comunicações de natureza semelhante»,[24] muito distantes, pelas suas características técnicas, do correio

[23] Pense-se, p. ex., na necessidade de apreender os *logs* de um sistema para poder determinar quem era o utilizador na máquina aquando do envio de um e-mail.

[24] Não apenas os "registos de mensagens", mas as próprias mensagens, nelas se incluindo quer as feitas através de um mero serviço telefónico (*SMS, EMS, MMS*), quer as feitas através de *IP Adress* por *IM – Instant Messenger* (programas de mensagens instantâneas, *e. g.*, *Facebook Messenger, Skype, WhatsApp, Signal, Viber, Snapchat, Telegram*), cada vez mais importantes e frequentes (o número de utilizadores do *Facebook Messenger* é de perto de 3 mil milhões e do *WhatsApp* de 2 mil milhões), e ainda as feitas em *chats* ou *chatrooms*. Com maior desenvolvimento, cf. Rui Cardoso, "Apreensão de correio electrónico…", *ob. cit.*, pp. 181-183.

físico. Nestes, o processo de comunicação estará sempre terminado no momento da apreensão.

Depois, as mensagens de correio electrónico podem estar simultaneamente em vários sistemas do remetente (que fica com a mensagem que envia) e do(s) destinatários(s), o que não pode suceder com a correspondência corpórea (ou está em trânsito ou está já entregue ao único destinatário, e num único local). Por outro lado, antes de ser expedida a carta ou encomenda não há correspondência: há um objecto (*e. g.*, folhas de papel) dentro de um invólucro (*e. g.*, um envelope). Às mensagens de correio electrónico enviadas e aos rascunhos não poderia nunca aplicar-se o regime de apreensão de correspondência – também por isso a remissão para o regime do CPP é inadequada.

O processo de apreensão de dados informáticos é algo tecnicamente complexo e exigente. Para ser tecnicamente admissível, deve cumprir as melhores práticas internacionais, *v. g.*, os requisitos de *autenticidade* (as provas devem estabelecer factos de uma forma que não possa ser contestada e seja representativa do seu estado original), *completude* (a análise ou qualquer opinião baseada nas provas deve contar toda a história e não ser adaptada para corresponder a uma perspectiva mais favorável ou desejada), *confiabilidade* (não deve haver nada sobre a maneira pela qual as provas foram recolhidas e posteriormente tratadas que possa lançar dúvidas sobre sua autenticidade ou veracidade), *credibilidade* (as provas devem ser persuasivas quanto aos factos que representam e os decisores no processo judicial devem poder confiar nelas como verdadeiras) e *proporcionalidade* [os métodos utilizados para reunir as provas devem ser justos e proporcionais aos interesses da justiça: o dano (ou seja, o nível de intrusão ou coerção) causado aos direitos de qualquer parte não deve superar o seu valor como prova].[25]

Antes do momento da formal apreensão – que, verdadeiramente, deve ser apenas (e não é pouco) uma *decisão de permissão de utilização processual dos dados para efeitos de prova* – há todo um processo técnico de procura, identificação, preservação e recolha dos dados, tudo devidamente documentado.

[25] Cf. *Electronic Evidence Guide – A Basic Guide for Police Officers, Prosecutors and Judges*, Cybercrime Division – Directorate General of Human Rights and Rule of Law (Council of Europe), v. 2.1, 2020, p. 13.

Processo esse que, embora não regulado na lei, é já objecto de vários *standards* mínimos de garantia, bem consolidados internacionalmente.[26] Aquilo que a LCC chama hoje de *apreensão* é apenas um momento no final nesse processo.

b) Não tem contacto com a realidade a ideia de que em todos os sistemas informáticos e em todos os suportes será possível apresentar as mensagens ao JIC sem delas tomar conhecimento primeiro, em maior ou menor medida. Concretizo, exemplificando:

- Qualquer pessoa identifica, por características físicas externas, o correio físico: envelope/embalagem (com vários tamanhos possíveis) fechado/a contendo algo (*v. g.*, escritos) que é entregue a entidade que presta o serviço de o entregar a outra pessoa. O mesmo não sucede com o correio electrónico: trata-se sempre de dados informáticos [escritos numa de várias linguagens binárias, mas sempre com "1" (uns) e "0" (zeros)], a que só se pode aceder através de uma *interface* (sistema informático executando um ou mais programas)[27] e onde nem sempre são facilmente identificáveis.
- Há que procurar por programas cliente de correio electrónico, que podem conter mensagens. Porém, essas mensagens desses programas podem estar já arquivadas em ficheiros de diversos formatos (*pst*, *ost*, *mbox*, *etc*., cujas terminações podem até ter sido manualmente alteradas pelo utilizador),[28] não sendo visíveis nos programas. Depois, as mensagens de correio electrónico ou semelhantes podem ser guardadas, individualmente ou em grupo, podendo o utilizador fazê-lo em diferentes tipos de ficheiro e com os nomes que quiser.[29]

[26] Para além do *Electronic Evidence Guide... cit.*, cf. a *Norma ISO/IEC FDIS 27037:2012* - *Directrizes para identificação, recolha, apreensão e preservação de prova digital* (Termo de Adopção em Portugal n.º 1252/2016, 2016-10-12). Cf., ainda, p. ex.: da European Network of Forensic Science Institutes (ENFSI), *Best Practice Manual for the Forensic Examination of Digital Technology*, 2015 (acessível em https://enfsi.eu/documents/best-practice-manuals/); do National Institute of Justice (USA), *Forensic Examination of Digital Evidence*: *A Guide for Law Enforcement*, 2004 (acessível em https://nij.ojp.gov/library/publications/forensic-examination-digital-evidence-guide-law-enforcement), e *Digital Evidence in the Courtroom*: *A Guide for Law Enforcement and Prosecutors*, 2007 (acessível em https://nij.ojp.gov/library/publications/digital-evidence-courtroom-guide-law-enforcement-and-prosecutors); do Scientific Working Group on Digital Evidence (SWGDE), os vários específicos (acessíveis em https://www.swgde.org/documents/published). Todos os endereços *online* foram acedidos em Novembro de 2021.

[27] A mensagem de correio electrónico, «por natureza, não é fechada, não é envelopável, não é unívoca quanto ao número de destinatários e não circula em ambiente seguro [...]. E, sobretudo, é, no seu estado natural imaterial»: Rogério Bravo, "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", *Polícia e Justiça*, III Série, 7, Janeiro-Junho (2006), p. 214.

[28] Os ficheiros de arquivo de correio electrónico do programa *Outlook* têm a terminação *pst*, mas, depois de gravado, o utilizador pode alterar tal terminação, não permitindo a outros conhecer – sem abrir – que esse ficheiro respeita a arquivo de correio electrónico.

[29] Poderá gravá-los como páginas *web* (*e. g., html*), ficheiros de texto (*e. g., docx, doc, txt, tiff, rtf*), de arquivo de imagem (*pdf*), como imagem (*e. g., jpeg*), *etc*.

Nesses casos, só com a abertura de cada um desses ficheiros será possível saber se contêm ou não mensagens de correio electrónico ou semelhantes.[30-31]

- As mensagens de correio electrónico ou semelhantes podem até ter sido apagadas ou escondidas. São cada vez mais e a todos facilmente acessíveis diversas ferramentas *antiforensics,*[32] desde a encriptação à esteganografia.[33] Nesses casos, serão necessárias ferramentas informáticas específicas para as detectar e recuperar, tarefa em que, necessariamente, haverá conhecimento do seu conteúdo, em maior ou menor medida.
- Em alguns aparelhos móveis, como *Apple iPhones*, a extracção de mensagens de e-mail não pode ser feita directamente do programa de e-mail original instalado, tendo o examinador de manualmente as procurar e gravar de outras fontes no aparelho.[34]
- O acesso ao correio electrónico poderá ter sido feito apenas em *webmail* e, no momento da pesquisa, a única forma de acesso às mensagens (de forma

[30] Como alerta Peter Sommer, *Digital Evidence, Digital Investigations and E-Disclosure*: *A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers*, IAAC, 4.ª ed., 2013, p. 83, acessível em https://www.researchgate.net/publication/341509816_Digital_Evidence_Digital_Investigations_and_E-Disclosure_A_Guide_to_Forensic_Readiness_for_Organisations_Security_Advisers_and_Lawyers, «[t]he emails themselves are stored in files associated with the email application – a forensic technician needs to have a knowledge of which files are important and where they are located. Attachments to emails may be stored elsewhere, in another directory on the disk. In the simpler older products, often the email files can be read directly using a text editor, but in more modern products such as Outlook, Outlook Express, and Thunderbird the emails are held inside a structured database and can be read only from within the email program or a specialist utility.»

[31] Não se nos afigura admissível considerar que o artigo 17.º só se aplica às mensagens que se encontram no respectivo programa utilizado para as transmitir: isso seria reduzir o âmbito da sua tutela sem qualquer apoio na letra da lei e sem qualquer fundamento material para tal. Seria o mesmo que considerar que, para o correio corpóreo, apenas se aplica o regime do artigo 179.º à correspondência em trânsito ou ainda na caixa de correio do destinatário, não a partir do momento em que deste local fosse retirada.

[32] Técnicas destinadas a impedir a recolha de prova digital por parte das autoridades ou a condicionar a sua validade probatória. Cf., p. ex., Scott Berinato, "The Rise of Anti-Forensics", *CSO Online*, 2007, acessível em https://www.csoonline.com/article/2122329/the-rise-of-anti-forensics.html.

[33] Esta permite esconder a prova relevante em imagens (fixas ou dinâmicas) ou outros tipos de ficheiros enviados por e-mail (como de som ou textos). Sobre a recente utilização da esteganografia no terrorismo, cf. Kaustubh Choudhary, "Image Steganography and Global Terrorism", *IOSR Journal of Computer Engineering*, DOI:10.9790/0661-0123448, 2012, acessível em https://www.researchgate.net/publication/265185373_Image_Steganography_and_Global_Terrorism, Stephanie R. Betancourt, *Steganography*: *A New Age of Terrorism*, acessível em https://www.giac.org/paper/gsec/3494/steganography-age-terrorism/102620, e William Eyre / Marcus Rogers, *Steganography and Terrorist Communications*: *Current Information and Trends - Tools, Analysis and Future Directions in Steganalysis in Context with Terrorists and Other Criminals*, acessível em https://commons.erau.edu/cgi/viewcontent.cgi?article=1013&context=adfsl.

[34] Cf. *Digital Forensics – A Basic Guide for the Management and Procedures of a Digital Forensics Laboratory*, Cybercrime Division – Directorate General of Human Rights and Rule of Law (Council of Europe), 2017, p. 53.

integral ou parcelar) será através da recuperação de páginas *html* em pastas temporárias. Só com a sua abertura e análise individual será possível saber se são ou não mensagens de correio electrónico ou semelhantes.

- Depois, a própria letra da lei prevê a possibilidade de o "encontrar" os dados ocorrer durante uma perícia: esta, por definição, consiste na percepção e análise dos dados – ou seja, obriga a tomar conhecimento do seu conteúdo. Não raras vezes, a perícia deve ser feita no momento da pesquisa inicial, com o sistema ligado, durante a busca a um espaço físico, sob pena de se perderem os dados relevantes.

- Finalmente, no que respeita aos *IM*, em alguns casos as mensagens são apagadas automaticamente após algum (curto) tempo depois do envio (*e. g.*, *Snapchat*), o que obriga a que, a serem apreendidas, tenham de o ser no momento da pesquisa. Também nestes casos será impossível não tomar conhecimento, ainda que em pequena medida, dessa conversa. Quanto aos *chats online*, em caso de pesquisa de um sistema informático em que esteja aberta uma conversa reservada (situação vulgar na *Darkweb* em processos de pornografia infantil), a mesma terá de ser apreendida antes de ser desligado o sistema, sob pena de se perder irrecuperavelmente. Igualmente neste caso será impossível não tomar conhecimento, ainda que em pequena medida, dessa conversa.

Em todas estas situações, exigir o prévio conhecimento pelo juiz significaria, na prática, impedir a apreensão desses dados, o que, para além de constituir uma interpretação contra a Convenção sobre Cibercrime do Conselho da Europa[35] e o âmbito de apreensão de dados que Portugal, como Estado-Parte, deve assegurar na sua legislação,[36] levaria em muitos casos ao *incumprimento pelo Estado do seu dever de protecção dos direitos fundamentais* – da vida, liberdade, e segurança das pessoas, *etc*. –, e para tanto, em medida proporcional, de prevenir e investigar o crime e de perseguir e sancionar quem o comete.[37] Ao Estado também cabe garantir os direitos e liberdades fundamentais das vítimas, não apenas dos suspeitos ou arguidos.[38]

[35] A LCC adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa (STE 185), doravante CCiber, adoptada em Budapeste em 23 de Novembro de 2001, aprovada pela AR através da Resolução n.º 88/2009, de 15 de Setembro, e ratificada pelo Decreto do PR n.º 91/2009, da mesma data.

[36] Cf. artigos 14.º, n.º 1, e 19.º, n.ºs 1 e 3, da CCiber.

[37] Salientando este aspecto, com uma perspectiva crítica sobre o Acórdão, cf. Vital Moreira, *Causa Nossa*, in https://causa-nossa.blogspot.com/2021/09/nao-conordo-21-contra-corrente.html.

[38] Sobre o direito à protecção do Estado contra a vitimização primária ou repetida na jurisprudência do Tribunal Europeu dos Direitos Humanos (TEDH), que múltiplas vezes censurou os Estados pela sua inércia ou omissão na protecção do cidadão, cf. Paulo Pinto de Albuquerque, *ob. cit.*, pp. 210-211, e os acórdãos aí citados. Importante ainda o Acórdão K.U. c. Finlândia (Queixa n.º 2872/02), de 02.12.2008,

Exigir que seja o juiz, como se estivesse com uma faca a abrir uns poucos envelopes fechados, a abrir e analisar milhares de mensagens (ou milhões…), que não estão fechadas nem são "fecháveis", é, pois, querer criar Direito que nunca poderá aplicar-se à realidade que deve regular e que desde o primeiro momento renuncia a proteger as vítimas do crime.

3.3. A pesquisa e apreensão através da utilização de palavras-chave

Igualmente desenquadrado da realidade é pensar que, depois de tecnicamente identificadas e cautelarmente apreendidas as mensagens de correio electrónico e semelhantes, as relevantes podem sempre ser encontradas através da aplicação de termos de pesquisa ou palavras-chave. Isso apenas é possível em processos simples, onde se procura umas poucas mensagens cuja existência até já se conhece (p. ex., enviadas pelo suspeito/arguido ao ofendido com uma injúria, ou ameaça/coacção ou até extorsão). Não já em criminalidade complexa, organizada, económico-financeira, empresarial, em que, por regra, as mensagens – aos muitos milhares – são parte de extensos e complexos processos de comunicação, ao longo de períodos latos, com muitos intervenientes, com utilização de diferentes meios de comunicação, desde a presencial (eventualmente registada através de uma escuta ambiental), ao telefone, passando por diferentes programas de *IM* (*WhatsApp, Signal, etc.*) e por diferentes contas de correio electrónico, que exigem por isso análise global, integrada, de contexto, algo a que uma pesquisa por termos nunca será adequada.[39] Nestes casos, os termos de pesquisa devem ser apenas um primeiro (e geralmente pequeno) passo na triagem e identificação da prova relevante.

É um mito pensar que um examinador forense digital pode realizar uma análise forense adequada e completa apenas usando pesquisas de palavras-chave. Em verdade, não é possível criar, antes da análise, uma lista abrangente de palavras-chave relevantes que identificarão todas as provas digitais relevantes.[40]

onde, na fundamentação da sua decisão, o TEDH referiu que «[…] a previsão de um crime tem efeito dissuasor limitado se não existir meio de identificar o agente e chamá-lo à justiça» (§46) e que «[…] pese embora a liberdade de expressão e a confidencialidade das telecomunicações sejam considerações relevantes (primárias) e os utilizadores de telecomunicações e de serviços de internet devam ter garantias de que a sua própria privacidade e liberdade de expressão será respeitada, *tais garantias não são absolutas e devem por vezes ceder em face de outros imperativos legítimos, tais como a prevenção de crimes e a protecção dos direitos e liberdades dos outros* [tarefa esta de concordância prática que cabe ao legislador assegurar]» (§49, itálico meu).

[39] A necessária completude dos dados exigirá a apreensão de todas as mensagens de uma "conversa", não apenas daquela que seja considerada a *smoking gun*, sob pena de vedar ao arguido a possibilidade de contestar a interpretação que é feita de qualquer comunicação sua.

[40] Sobre esse e outros mitos, cf. SWGDE, *Collection of Digital and Multimedia Evidence – Myths vs Facts*, acessível em https://www.swgde.org/documents/published.

Deve estar bem delimitado o objecto da pesquisa (o que se pretende apurar, face ao objecto do processo, para que se possa aferir da sua necessidade, adequação e proporcionalidade),[41] mas não a forma técnica de o alcançar. A técnica da análise não é algo acessível ao juiz, nem é da sua competência. Exactamente como sucede com uma autorização de busca domiciliária: deve estar devidamente fundamentada, incluindo a identificação, de forma mais ou menos precisa (consoante as circunstâncias do caso), dos animais, coisas ou objectos relacionados com um crime ou que possam servir de prova que se pretende apreender, mas o mandado não deve conter instruções técnicas de como a busca deve ser executada.[42]

Esta ideia está bem evidenciada no *Manual de Busca e Apreensão de Computadores e Recolha de Prova Digital em Investigações Criminais*, do Departamento de Justiça dos Estados Unidos da América. Aí se afirma:

> «Limitations on search methodologies have the potential to seriously impair the government's ability to uncover electronic evidence. "[A] search can be as much an art as a science," United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005), and the forensic process can require detective work, including intuition and on-the-spot judgment in deciding, based on what the examiner has just seen, what is the best step to take next. One particularly burdensome restriction that could be placed on a forensic investigator is the requirement that the investigator limit the search to files containing particular keywords. *Forensic analysis may include keyword searches, but a properly performed forensic analysis will rarely end there*, because keyword searches will fail to find many kinds of files that fall within the scope of a warrant» [exemplificando com tipos de ficheiros onde não é possível pesquisar com *keywords* – em geral, todos os de imagem, que pode ser o que sucede com um documento em formato *jpg* anexo a um e-mail sem qualquer tipo de texto]. […]
>
> In addition, *keyword searches can also be thwarted through the use of code words or even unintentional misspellings. Law and investment firms—not to mention individuals involved in criminal activity—often use code words to identify entities, individuals, and specific business arrangements in documents and communications*; sometimes the significance of such terms will not be apparent until after a careful file-by-file review has commenced. […]
>
> While it might be helpful for the affidavit to contain background information that might justify particular steps taken during the search—such as describing the ease with which evidence can be concealed in a computer, explaining the need to search off-site, or justifying the seizure of commingled records—*neither the search warrant application nor the affidavit need contain special restrictions on how agents search for the things described in the warrant*».[43]

A procura e apreensão de dados informáticos apenas por palavras-chave é hoje, pois, técnica ultrapassada.

3.4. Análise dos regimes legais possíveis

a) Das cinco possibilidades supra expostas, duas há que devem ser afastadas liminarmente e pelos mesmos motivos: a 1. e a 3. Nelas, para além de se continuar a acreditar nos mitos de que é possível levar as mensagens ao conhecimento do JIC sem, pelo menos parcialmente, tomar conhecimento do seu conteúdo, e de que este conseguirá tomar efectivo conhecimento de todas elas, será o JIC quem verdadeiramente fará a selecção das relevantes e, assim, será *juiz investigador*, violando a estrutura acusatória do processo. Fá-lo-á mal – pois não tem meios nem conhecimentos técnicos para tal – e em vão – pois, não podendo impedir o (concomitante ou posterior) conhecimento das mensagens por parte do MP, *v. g.*, para efeitos de recurso dessa decisão, não haverá nesse "primeiro conhecimento" do JIC qualquer real garantia.[44-45]

Há ainda que não esquecer que, tal como sucede com todos os demais meios de prova, a identificação do que é ou não probatoriamente relevante não ocorre apenas num momento, mas a todo o tempo até ao encerramento do inquérito, e pode ocorrer mesmo depois deste. À luz de cada nova prova obtida, dos novos factos apurados, dos seus possíveis enquadramentos jurídico-penais, a produção de prova e a sua apreciação estão em constante mutação. Aquilo que num momento pode parecer irrelevante pode mais tarde vir a ser a prova decisiva. O legislador há muito o compreendeu no que respeita às escutas telefónicas, permitindo que, até à acusação, o MP identifique e utilize quaisquer comunicações, ainda que até esse momento não tenham sido consideradas relevantes pelo JIC. O mesmo deve suceder com a apreensão de dados informáticos, designadamente de correio electrónico. Não pode transformar-se o JIC num *super investigador judicial* a quem frequentemente se recorre para que faça novas pesquisas nas mensagens de correio electrónico à luz dos desenvolvimentos da investigação.

[41] A pesquisa deve visar «obter dados informáticos específicos e determinados» – artigo 16.º, n.º 1, da LCC. Porém, não se deve partir da exigência dessa finalidade – que deve ser previamente bem identificada no processo, com a maior precisão possível – para a conclusão de que *apenas podem ser vistos dados específicos e determinados*. Tal como sucede com uma busca física, para se encontrar o que se pretende há que procurar detalhadamente. Pense-se que, numa empresa, se procura todos os documentos respeitantes a determinado processo de contratação com o Estado: nos escritórios, poderá ser necessário abrir e verificar todas as pastas de documentos existentes; o mesmo pode ser necessário numa pesquisa informática.

[42] Sobre estas, cf. José Braz, *Ciência, Tecnologia e Investigação Criminal*, Coimbra: Almedina, 2015, pp. 144 e ss.

b) Três possibilidades restam então: ou a intervenção do JIC ocorre apenas para, analisando a selecção de mensagens já feita pelo MP, determinar quais poderão ser utilizadas como prova (a 2.), ou o mesmo tem intervenção prévia, autorizando a pesquisa. Nesse caso, ou a sua intervenção se esgota nesse momento (5.) ou ainda é chamado a decidir a concreta apreensão de cada mensagem, apreciando a selecção feita pelo MP (4.).

Dir-se-á que um sistema com dupla intervenção do JIC (prévia e posterior), decalcado do artigo 179.º do CPP, é o mais garantístico. Porém, por tratar de forma igual o que é diferente, levaria a uma significativa incoerência do sistema: criaria um regime substancialmente diferente do da apreensão de correio físico, onde, depois de aberta a correspondência pelo destinatário, o seu conteúdo é apenas documento/objecto, livremente apreensível pelo MP e OPC's (não dispensando, claro, um concreto juízo de necessidade, adequação e proporcionalidade caso possa existir ofensa a direitos fundamentais) e não teria qualquer justificação de existência para os dados que não são de correio electrónico.

Para além isso, e com maior relevo, tal solução seria em absoluto incoerente com o regime vigente da intercepção – artigo 188.º do CPP e artigo 18.º da LCC. Salientando-se que os dados em causa serão exactamente os mesmos (nos artigos 188.º e 18.º em trânsito, no artigo 17.º já armazenados), no caso mais gravoso (intercepção, em que há sempre intrusão nas telecomunicações em curso) o juiz só teria intervenção prévia, no caso menos gravoso (apreensão) o juiz não só autorizaria a medida como depois também a selecção das mensagens a utilizar como prova. Qual o fundamento para tal diferença? Note-se que, no regime das intercepções, as intervenções do JIC posteriores à autorização são apenas para controlo do processo de realização das intercepções e para permanente verificação da manutenção dos pressupostos legais e factuais que fundamentaram a medida, não sobre a selecção daquelas relevantes para prova. Para além disso, como visto, a selecção das mensagens pelo JIC contém sempre sério risco de o fazer assumir o papel de *juiz investigador*.

No mesmo sentido, não deverá esquecer-se a Directiva (UE) 2019/1 do Parlamento Europeu e do Conselho que visa atribuir às autoridades da concorrência dos Estados-Membros competência para aplicarem a lei de forma mais eficaz e garantir o bom funcionamento do mercado interno, que prevê que essas autoridades devem ter a competência para, após autorização prévia de uma autoridade judicial, examinarem todas as formas de correspondência, incluindo mensagens electrónicas, independentemente de parecerem não

ter sido lidas ou de terem sido apagadas, inclusive no domicílio privado dos dirigentes, de membros dos órgãos de administração e de outros membros do pessoal das empresas ou das associações de empresas.[46] Não haverá, pois, necessidade de "visualização prévia" pelo juiz, nem deste dependerá a decisão de utilização probatória das concretas mensagens. Exigir isso em processo penal será, pois, incoerente e desproporcional.

c) Restarão então as soluções 2 – com o juiz a intervir apenas posteriormente, decidindo da utilização probatória – e 5 – com intervenção apenas inicial, autorizando a pesquisa e apreensão. Ambas, em meu entender, constitucionalmente conformes, ambas com vantagens e com desvantagens na compatibilização entre a defesa dos bens jurídicos ofendidos pelo crime e os direitos fundamentais do visado.

Contrariamente ao que parece resultar do Acórdão, afigura-se-me que mesmo o sistema em que a intervenção do JIC só ocorre para, analisando a selecção de mensagens já feita pelo MP, determinar quais poderão ser utilizadas como prova (2.) é não só conforme à Constituição como é aquele previsto na lei vigente.[47] Como supra assumido, é inquestionável que deve haver intervenção do JIC. Porém, esta não necessita de ser prévia, sendo a posterior ainda adequada à sua função garantística. As concretas especificidades da apreensão de dados informáticos em geral e de correio electrónico em especial, supra expostas – *v. g.*, a dificuldade em determinar previamente onde irão ser encontrados dados de correio electrónico ou até dados sensíveis ou íntimos, a dificuldade em separar a pesquisa que vise obter dados de correio electrónico das pesquisas que tenham outra finalidade –, justificam que neste caso a intervenção seja apenas posterior.

Note-se que esta intervenção posterior não é para validação de ofensa a direitos fundamentais *já terminada*, como sucede com a validação das buscas domiciliárias ou a da detenção. Aqui, houve já uma primeira ofensa (mero conhecimento pelos OPC's e MP), mas, creio, a maior virá com a utilização probatória das mensagens e o seu conhecimento pelos demais sujeitos processuais e, para além deles, o público e a comunicação social. *A intervenção*

[46] Cf. Considerando 32 e artigos 6.º, n.º 1, alínea b), e n.º 3, e 7.º, n.ºs 1 e 2. Para transposição dessa Directiva está nesta data pendente a Proposta de Lei 99/XIV/2.ª, que visa alterar a Lei n.º 19/2012, de 8.V. As normas relevantes para o correio electrónico estão no artigo 18.º, n.º 1, alínea b), e n.º 2, desta lei.

[47] Essa a posição assumida em "Apreensão de correio electrónico…", cit.. No mesmo sentido, Pedro Verdelho, *ob. cit.*, pp. 744-745, Tiago Caiado Milheiro, *ob. e loc. cit.*, e Duarte Alberto Rodrigues Nunes, *ob. cit.*, pp. 101 e ss. e 153 e ss. Contra, Rita Castanheira Neves, *As ingerências nas comunicações electrónicas no processo penal*, Coimbra: Coimbra Editora, 2011, pp. 274-275, e Santos Cabral, *Código de Processo Penal Comentado*, AAVV, Coimbra: Almedina, 3.ª ed., 2021, p. 712.

do JIC é posterior ao início da lesão, mas ainda anterior às maiores que se lhe sucederão.

Atente-se ainda que se houver intervenção prévia do JIC haverá depois menor controlo sobre o que é visto por todos os sujeitos processuais e por estes utilizado como prova (como nas intercepções) do que haverá quando a sua intervenção é posterior e é sempre sua a decisão de utilização probatória.

Repito que com o mero conhecimento pelos sujeitos processuais há já ofensa aos direitos fundamentais em causa. Dir-se-á então que a intervenção prévia do JIC é indispensável a impedir que tal ocorra sem justificação. Porém, não se podendo conhecer nesse momento com a menor precisão que dados poderão estar em causa (qual, na verdade, a dimensão da ofensa aos direitos fundamentais que poderá ocorrer), o JIC carecerá de elementos para a concreta ponderação necessária ao juízo de proporcionalidade[48] e, com isso, mais dificilmente terá fundamentos para indeferir a pretensão do MP, sob pena de, indeferindo, impedir à partida a apreensão de todos os dados informáticos, mesmo aqueles com pouca ou nenhuma ofensa à privacidade do visado. Numa perspectiva global, a intervenção prévia oferece, pois, menor garantia.

Há ainda que não esquecer o que pode suceder no mundo corpóreo: nunca se sabe quando é que, numa busca que não é da competência do JIC, se encontram, p. ex., fotos íntimas ou um diário que podem ter relevância probatória. Nessas situações, haverá que fazer intervir o JIC e será dele a decisão, apreciando os fundamentos invocados pelo MP. Esse o sistema garantístico previsto na LCC, no artigo 16.º, n.º 3. O regime similar ao desta norma é, pois, o adequado. Nunca se sabe onde poderão estar os dados informáticos com maior potencialidade de violar a privacidade.

Contraponho ainda que, como vimos, o MP deve decidir de acordo com os mesmos critérios que o JIC, *v. g.*, o juízo de proporcionalidade deve ser o mesmo. Não pode afirmar-se que, não havendo intervenção prévia do JIC, não há qualquer garantia judiciária. Não pode desvalorizar-se a função do MP no inquérito e o seu estatuto constitucional e legal que a enquadra: os princípios constitucionais e legais que nessas tarefas regem a actuação de juízes e procuradores são exactamente os mesmos. Vejamos.

d) Realço a leitura parcial das características do MP e dos seus magistrados em confronto com as dos juízes feita no Acórdão, que conduz

[48] A ponderação de necessidade, adequação e proporcionalidade será sempre feita apenas para a medida (a pesquisa) e não para a concreta mensagem/objecto informático. Aquela será necessariamente mais vaga e indeterminada, com um juízo de previsão mais abstracto; esta será sempre concreta, sem qualquer abstracção. Um juízo de necessidade, adequação e proporcionalidade sobre uma mensagem concreta é muito mais rigoroso do que um sobre uma pesquisa.

à afirmação da existência de um «impressivo e distinto retrato do juiz e do Ministério Público que resulta do texto constitucional e das disposições legais aplicáveis». De facto, nele se lê que:

> «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 […]).
>
> 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).»

O que o Acórdão não refere, como devia, é *a que garantia constitucional da inamovibilidade é exactamente igual para juízes e magistrados do MP* (artigos 216.º, n.º 1, e 219.º, n.º 4); que estes últimos devem actuar sempre com *independência* em relação a interesses de qualquer espécie e às suas convicções políticas, religiosas ou filosóficas, abstendo-se de obter vantagens indevidas, directa ou indirectamente, patrimoniais ou outras, para si ou para terceiro, das funções que exercem (artigo 104.º, n.º 1, do Estatuto do Ministério Público [EMP]) – deveres de *imparcialidade* e de *isenção*; que devem igualmente desempenhar as suas funções *tendo exclusivamente em vista a realização da justiça, a prossecução do interesse público e a defesa dos direitos dos cidadãos* (n.º 2 deste artigo); que devem exercer as suas funções no respeito pela Constituição, pela lei e pelas ordens e instruções legítimas dos

superiores hierárquicos;[49] e que também lhes cabe a defesa do princípio da igualdade dos cidadãos perante a lei [o que resulta do artigo 66.º, alínea h)].

Ainda que, no concreto regime legal hoje vigente, as proclamadas *irresponsabilidade dos juízes e responsabilidade dos procuradores se traduzem exactamente na mesma responsabilidade criminal, civil e disciplinar*. A responsabilidade dos procuradores consiste em responderem, nos termos da lei, pelo cumprimento dos seus deveres e pela observância das directivas, ordens e instruções que receberem (artigo 97.º, n.º 2, do EMP). A observância das directivas, ordens e instruções que receberem é decorrência do seu estatuto de autonomia: é porque podem autodeterminar a sua actuação que são responsáveis por ela e pelas consequências daí resultantes.[50] Porém, também os juízes respondem, nos termos da lei, pelo cumprimento dos seus deveres.

Assim, em verdade, tal como sucede com os juízes, os magistrados do MP só podem ser responsabilizados pelas suas decisões nos termos previstos na lei em termos criminais, civis ou disciplinares. A lei penal é, naturalmente, igual para todos; o regime da responsabilidade civil é o mesmo (artigo 5.º, n.ºs 3 e 4, do Estatuto dos Magistrados Judiciais [EMJ], artigo 98.º do EMP e artigo 14.º do Regime da responsabilidade civil extracontratual do Estado e demais entidades públicas); em termos disciplinares, embora a definição de infracção disciplinar não seja exactamente igual,[51] nem num caso nem noutro é fundada *no sentido da decisão*. O órgão com competência disciplinar é idêntico: o respectivo Conselho Superior.

e) A reserva de juiz não pode ser desligada das garantias de defesa que o n.º 1 do artigo 32.º da CRP obriga a defender. Também ela é uma garantia de defesa.[52] O que está em causa com a apreensão de dados informáticos é também a potencial violação das garantias de defesa. O TC pronuncia-se pela

[49] Ordens e instruções estas que igualmente devem respeitar a Constituição e a lei, sob pena de deverem ser recusadas – artigos 103.º, n.º 1, e 100.º, n.º 3, do EMP.

[50] Cf. Luís Sousa da Fábrica, *A Autonomia do Ministério Público no Novo Estatuto*, Lisboa: Sindicato dos Magistrados do Ministério Público, 2020, p. 78.

[51] «[O]s atos, ainda que meramente culposos, praticados pelos magistrados do MP com violação dos princípios e deveres consagrados no presente Estatuto e os demais atos por si praticados que, pela sua natureza e repercussão, se mostrem incompatíveis com a responsabilidade e a dignidade indispensáveis ao exercício das suas funções» no artigo 205.º do EMP e «os atos, ainda que meramente culposos, praticados pelos magistrados judiciais com violação dos princípios e deveres consagrados no presente Estatuto e os demais atos por si praticados que, pela sua natureza e repercussão, se mostrem incompatíveis com os requisitos de independência, imparcialidade e dignidade indispensáveis ao exercício das suas funções» no artigo 82.º do EMJ.

[52] «Garantia fundamental de defesa» a consideram Gomes Canotilho / Vital Moreira, *ob. cit.*, p. 520.

violação das garantias constitucionais de defesa invocando apenas o n.º 4 do artigo 32.º, mas não vemos como possa deixar de convocar também o n.º 1 do mesmo artigo.

Essa apreciação global a fazer da reserva de juiz no quadro das garantias de defesa impõe um particular cuidado na valorização a fazer do factor "independência" e do factor "terceiro imparcial", coexistentes no JIC durante o inquérito. Este último é importante, mas não absoluto ou inultrapassável. É que se o considerarmos inultrapassável ou não dispensável teremos de concluir pela inaplicabilidade constitucional na fase de instrução de todas as medidas de investigação que possam contender gravemente com direitos fundamentais e com isso colocar em crise essa fase do processo penal e todo o nosso sistema processual penal.

Não estariam essas garantias violadas na fase de instrução quando é o juiz a decidir sobre o exercício da acção penal, quando é ele que, sem obrigatoriedade de qualquer contraditório, simultaneamente tem o impulso e a decisão sobre os meios de obtenção de prova a utilizar, e é sua a decisão sobre a sujeição do arguido a julgamento? As garantias de defesa não valem também para a fase de instrução?

Em caso de instrução a requerimento do assistente, não estará o JIC a dirigir uma actividade de recolha de prova em tudo similar à do inquérito (saber se houve ou não crime, quem o cometeu e recolher prova tendo em vista a decisão instrutória)? A possibilidade/necessidade de apreensão de dados informáticos, incluindo os de correio electrónico, existe quer no inquérito, quer na instrução. Numa e noutra fase, a sua finalidade é a mesma: ser utilizada para a descoberta da verdade quanto aos crimes objecto do processo.

A posição de neutralidade do juiz na instrução não é diferente da do MP no inquérito. Ambos estão sujeitos ao mesmo dever de objectividade, de obediência à lei, de (iniciativa para a) descoberta da verdade e de realização do direito – artigos 9.º, n.º 1, e 53.º, n.º 1, do CPP, artigos 3.º e 4 do EMJ.

A independência dos juízes e a autonomia do MP são apenas garantes da actuação de uns e outros nesses termos. Na sua dimensão externa (face a quaisquer entidades externas aos órgãos do MP, *v. g.*, os tribunais e outros órgãos do Estado), a autonomia do MP é uma verdadeira independência, pois está legalmente assegurado que os seus magistrados não sejam submetidos, no exercício das suas funções, a influências ilegítimas ou a quaisquer pressões de origem exterior.[53]

[53] Recorde-se a *Rec(2000)19* do Comité de Ministros do Conselho da Europa, bem como a *Declaração de Bordéus sobre o papel dos Juízes e dos Procuradores numa sociedade democrática*, de 02.07.2009, documento

Se, no inquérito, o JIC tem a posição de terceiro face a quem pretende o acesso aos dados, por não estar envolvido na condução do processo, podendo assim ter uma posição de neutralidade relativamente aos interesses conflituantes no processo penal (no apuramento dos factos e efectivação da responsabilidade criminal *versus* do arguido de a isso se eximir), na instrução tal não sucede. Embora esta fase não deva ser um *novo inquérito*, um *complemento* ou *suplemento*, a «comprovação judicial da decisão de deduzir acusação ou de arquivar o inquérito» está funcionalmente dirigida a objectivo idêntico ao do inquérito: submeter ou não o arguido a julgamento[54] – artigos 262.º, n.º 1, e 286.º, n.º 1, do CPP. É só do JIC a responsabilidade de direcção do processo, sendo ele que «investiga autonomamente o caso» (artigo 288.º, n.º 4), ele que determina todos os actos de instrução a levar a cabo (artigo 289.º, n.º 1), actos que podem ser de natureza policial, praticados pelos OPC's (artigo 290.º, n.º 2), visando o apuramento da verdade (artigo 291.º, n.º 1), limitado apenas pelo objecto do processo definido na acusação ou no requerimento de abertura de instrução do assistente. Não está, pois, numa posição de terceiro imparcial[55] face ao caso: tem acção e tem jurisdição, tem impulso e tem decisão.[56] Está directamente comprometido com esses actos.[57] Não lhe cabe proferir a decisão final no processo,[58] mas submetê-lo, caso recolha indícios suficientes, ao órgão jurisdicional competente para tal – o tribunal de julgamento.

Onde ficaria então a garantia judiciária de defesa que se exigiria no inquérito? Será menor a necessidade de controlo sobre a restrição a direitos

conjunto do Conselho Consultivo dos Juízes Europeus e do Conselho Consultivo dos Procuradores Europeus.

[54] O artigo 262.º, n.º 1, refere «em ordem à decisão sobre a acusação», não, como o artigo 286.º, n.º 1, «em ordem a submeter ou não a causa a julgamento». Porém, a decisão sobre a acusação é verdadeiramente uma decisão sobre submeter ou não alguém a julgamento, pois a acusação exige a existência de indícios suficientes e estes, por sua vez, obrigam a juízo sobre a «possibilidade razoável de ao arguido vir a ser aplicada, por força deles, em julgamento, uma pena ou uma medida de segurança» – artigo 283.º, n.º 2, do CPP. A mesma definição de indícios suficientes que é critério para a decisão instrutória – artigo 308.º, n.ºs 1 e 2, do mesmo Código.

[55] Terceiro tão pouco será o tribunal de recurso, pois tal decisão é irrecorrível – artigo 291.º, n.º 2.

[56] Como refere Paulo Dá Mesquita (*Direcção do Inquérito Penal e Garantia Judiciária*, Coimbra: Coimbra Editora, 2003, p. 331), «[n]a fase de instrução o juiz de instrução assume uma posição polifuncional que, embora vinculada tematicamente, não se confunde com a intervenção de um juiz que vai apenas apreciar a actividade indagatória do Ministério Público, pois tem o poder de protagonizar uma actividade inquisitória de recolha suplementar de prova tendo em atenção as pretensões e contributos constitutivos de outros sujeitos processuais».

[57] António Henriques Gaspar, "As exigências da investigação no processo penal durante a fase de inquérito", in AAVV, *Que futuro para o direito processual penal? Simpósio de homenagem a Jorge de Figueiredo Dias por ocasião dos 20 anos do Código de Processo Penal Português*, Coimbra: Coimbra Editora, 2009, p. 97.

[58] É certo que toma a decisão instrutória no processo com total independência, mas o mesmo sucede com o MP na decisão de encerramento do inquérito.

fundamentais do cidadão caso a ordem venha de um juiz? Por que motivo? Essa restrição não será a mesma, venha a decisão de um procurador ou de um juiz? Qual a diferença entre *investigar para acusar* e *investigar para pronunciar*, entre *investigação originária* do MP e *investigação posterior* do JIC? Na independência do juiz *versus* a autonomia do MP não estará certamente, pois uns e outros têm a mesma garantia contra interferências externas.

Deve, pois, concluir-se que, *se as garantias de defesa podem prescindir da intervenção de um terceiro imparcial na fase da instrução, então no inquérito também o carácter relativo dessa garantia deve ser considerado na repartição de competências entre MP e JIC e, quanto a este, na definição do momento em que deve ocorrer a sua intervenção*, pois a autonomia do primeiro e a independência do segundo são, para esse fim, similares na garantia conferida.

Quem considerar que há violação das garantias de defesa se for o MP a ordenar a pesquisa, a tomar conhecimento dos dados e só depois existir intervenção do JIC para decidir da sua utilizabilidade (haverá intervenção de duas entidades com estatuto e deveres similares, estando uma em posição de terceiro face à condução do processo), então, por maioria de razão, deve chegar à mesma conclusão na instrução (em que só haverá intervenção de uma entidade e não estará na posição de terceiro imparcial).

f) O Acórdão invoca ainda que as intervenções no domínio de direitos fundamentais não são passíveis de integral reparação, quando abusivas, e que o que o MP ou os OPC's viram, indevidamente, não pode deixar de ser visto, mesmo que a informação não seja depois junta aos autos (ponto 34).

É verdade que o visto não pode deixar de ser visto. Mas isso também sucede se o vício for da decisão do JIC. Não pode ser apagado da memória, mas pode ser apagado do processo se for decidida pelo JIC a não utilização dessa prova (como sucede hoje com qualquer proibição de valoração de prova,[59] como um diário – só para a utilização probatória do diário se exige a intervenção do JIC e isso não impede o MP de dele tomar conhecimento, pois só assim pode fundamentar a sua relevância para a prova[60] – ou até

[59] Para além, claro, da destruição ou devolução dos dados.

[60] Cf. o Ac. do TC 607/2003, onde se lê: «Ou seja, a lícita apreensão de um diário não faz, sem mais, que, à luz das inarredáveis dimensões constitutivas do Estado de direito supra mencionadas, se haja de admitir a relevância probatória, no todo ou em parte, do seu conteúdo específico: de fora de tal valoração ficam, em homenagem à autonomia ética da pessoa humana, todas as "descrições" que apenas relevam de um estrito plano interior, ineliminavelmente agrilhoado à consciência do seu autor, sendo assim de reter, relativamente a estas, *praevalet quod principale est*, que a intervenção formalmente justificada na intimidade não a transforma, *ipso facto*, em "não abusiva" de um ponto de vista axiológico-material. E tal juízo não pode, pois, efectuar-se em abstracto tendo como ponto de partida e como critério de valoração o subjacente à validade da obtenção de um diário, outrossim deve realizar-se crítico-reflexivamente em concreto perante

com as escutas telefónicas, se, depois de autorizadas pelo JIC, vierem a ser consideradas inválidas, *v. g.*, por incumprimento dos prazos de controlo – artigo 188.º, n.ºs 3 e 4).

Reparação integral nunca acontece verdadeiramente. No caso da apreensão, o tempo em que a pessoa fica privada da posse, uso e fruição da coisa não é reparado pela restituição; no caso da detenção fora de flagrante delito, o detido poderá ficar privado de liberdade até 48 horas antes de ser presente a juiz (a eventual indemnização por privação ilegal da liberdade nunca poderá fazer devolver as 48 horas de liberdade perdidas).

Não se me afigura, pois, aspecto central.

3.5. Conclusão

Pelo que fica exposto, concluo que quer o regime vigente, interpretado da forma como o faço (com o JIC a intervir apenas posteriormente, decidindo da utilização probatória), quer um eventual outro (dependente de alteração legislativa), em que seja dele a autorização para a pesquisa e apreensão (sem qualquer intervenção posterior) são conformes à Constituição: respeitam a reserva de juiz e a estrutura acusatória do processo, asseguram as garantias de defesa e protegem adequadamente os direitos fundamentais.

4. A declarada inconstitucionalidade das normas dos n.ºs 3 e 5 do novo artigo 17.º

O TC pronunciou-se pela inconstitucionalidade de todas as normas constantes do "novo" artigo 17.º, incluindo, pois, as ínsitas nos n.ºs 3 e 5.

Apesar de incluídas no requerido pelo PR, tais normas não têm qualquer relação de acessoriedade com os n.ºs 1, 2 e 4, em qualquer das dimensões da declarada inconstitucionalidade, e não foram objecto de qualquer efectiva apreciação por parte do tribunal, nem com a mais leve das superficialidades. Não se compreende assim a sua inclusão no juízo de inconstitucionalidade.

Ainda que as tivesse analisado, estou certo que não lhes encontraria qualquer desconformidade constitucional.

O n.º 3 determinava a aplicação à apreensão de mensagens de correio electrónico e de natureza semelhante do disposto nos n.ºs 5, 6, 7 e 8 do artigo 16.º. Ora esses n.ºs 5 e 6 determinam a aplicação adaptada dos regimes legais de protecção dos segredos da advocacia, das actividades médica, bancária e jornalística, bem como do segredo de Estado e profissional; os n.ºs 7 e 8

o(s) conteúdo(s) que integra(m) um diário particular, aí discernindo, nos termos já referidos, se e em que medida pode estar em causa a dignidade e integridade éticas apenas do arguido».

descrevem a forma de execução material das apreensões, sendo já aplicáveis às de correio electrónico. Ou seja, o novo n.º 3 apenas deixava expresso na letra da lei aquilo que a boa interpretação já permite hoje concluir.

O n.º 5 determinava que 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». Pretendia, pois, suprir uma lacuna existente no regime vigente, que nada diz sobre o que fazer às mensagens que o juiz não apreende por não serem de grande interesse para a descoberta da verdade ou para a prova. A solução pretendida pela AR era a de seguir regime idêntico ao previsto para as escutas telefónicas no n.º 12 do artigo 188.º do CPP. A única censura que me parece merecer tal solução é a de não prever igualmente regime similar ao do n.º 6 desse artigo. Na verdade, os dados informáticos a que se aplica o artigo 17.º são dados armazenados que poderiam ter sido interceptados, em tempo real, através dos meios de obtenção de prova previstos nos artigos 187.º e 188.º do CPP (*SMS, EMS* e *MMS*) ou no artigo 18.º da LCC (*e. g.*, mensagens de correio electrónico e *instant messages*). Assim, quanto ao regime da destruição/devolução, sendo o artigo 17.º omisso e não oferecendo o artigo 179.º do CPP resposta satisfatória, parece-me que já hoje se deve aplicar o regime do artigo 188.º, n.ºs 6 e 12, deste código, *ex vi* do artigo 28.º da LCC.[61] Sendo os dados da mesma natureza, deve o regime de conservação ser o mesmo.[62-63]

[61] Ou seja, e fazendo as necessárias adaptações, o juiz, sem prejuízo do regime dos conhecimentos fortuitos, deve determinar a destruição imediata das mensagens de correio electrónico ou semelhantes que, sendo manifestamente estranhos ao processo, (i) abranjam matérias cobertas pelo segredo profissional, de funcionário ou de Estado, ou (ii) cuja divulgação possa afectar gravemente direitos, liberdades e garantias. As demais mensagens permanecerão materialmente apreendidas (ou sujeitas a apreensão cautelar ou provisória) à ordem do processo, só devendo ser destruídas após o trânsito em julgado da decisão que puser termo ao processo. Não poderão, pois, ser destruídas na pendência do inquérito.

[62] Com grande relevância sobre esta matéria, cf. o acórdão do TEDH de 04.06.2019 (caso Sigurður Einarsson e Outros c. Islândia – Queixa n.° 39757/15, em que os requerentes se queixaram de que a defesa não tinha tido acesso ao vasto volume de dados recolhidos pela acusação durante a fase de inquérito e que não tinha tido uma palavra a dizer na triagem electrónica desses dados; sustentavam que ninguém tinha revisto a selecção de documentos apresentados ao tribunal e que lhes tinha sido negada a possibilidade de efectuar uma pesquisa utilizando o sistema electrónico aplicado, o "*Clearwell*", um sistema de *eDiscovery*). O tribunal considerou que seria adequado que tivesse sido dada à defesa a possibilidade de realizar uma busca por provas potencialmente ilibatórias e que qualquer recusa em autorizar a defesa a fazer novas buscas nos documentos "marcados" levantaria um problema à luz do artigo 6.º §3 (b), relativamente à disponibilização dos meios adequados para a preparação da defesa.

[63] Por recente acórdão de 31.10.2019 (P. 122/13.8TELSB-BB.L1-9, Maria do Carmo Ferreira), o TRL decidiu no sentido de que «III - As provas, para além de estarem devidamente reguladas na Lei, serão sindicadas quanto à sua validade e pertinência, em sede de julgamento, ou seja, a oportunidade da sindicância sobre a prova é feita, em sede final, na fase do julgamento, quer quanto à validade da sua reprodução, quer

O juízo de inconstitucionalidade feito a estas duas normas no Acórdão não deve, pois, alterar a interpretação que hoje deve ser feita nesses aspectos.

III – Considerações finais

A prova digital é central no processo penal actual. Na primeira vez que se pronunciou sobre o regime vigente, e embora as normas apreciadas não fossem particularmente felizes,[64] o TC evidenciou imprecisão e alguns equívocos sobre o mesmo, em especial sobre a apreensão de dados informáticos e, mais ainda, sobre a realidade a que se aplica tal regime, o que condicionou o juízo que emitiu. Juízo e fundamentos invocados que extravasam o regime de apreensão de correio electrónico e implicam directamente com todo o regime de pesquisa e apreensão de dados informáticos.

Não se pode continuar a olhar para o correio electrónico como se olha para o correio físico e tentar apreender e analisar aquele como se apreende e analisa este. Não se pode reconhecer que a digitalização do mundo facilita a prática de quase todos os crimes e depois, pelo arcaísmo do *Direito* que se pretende criar, recusar o acesso à prova que essa mesma digitalização gera. Não se pode esquecer que ao Estado também cabe garantir os direitos e liberdades fundamentais das vítimas, não apenas dos suspeitos ou arguidos.

Não se pode viver num mundo altamente digitalizado e olhar para as comunicações electrónicas com um abre-cartas na mão. Fazê-lo é querer continuar a olhar para o projéctil com uma lupa, rejeitando o microscópio; é querer apenas saber qual o tipo de sangue presente num vestígio hemático e rejeitar a determinação de um perfil de ADN; enfim, é querer fazer investigação

quanto à sua utilidade e legalidade; IV - A eventual destruição das provas, do mesmo modo se tem de relegar para momento posterior às fases da investigação e da instrução, nomeadamente quanto à destruição de documentos que fazem parte do inquérito, concretamente de correio electrónico apreendido, quer se tenha por entendimento que o correio electrónico apreendido se encontra na forma "física" no processado, ou se entenda que se equiparam a correspondência pessoal, com enquadramento, o certo é que só é pertinente a sua destruição após o trânsito em julgado da decisão que puser termo ao processo, não podendo ser ordenada a sua destruição em fase anterior do processo, que esteja ainda em curso», revogando decisão do JIC a ordenar a destruição no final da instrução de vários suportes de correio electrónico constantes de apensos.»

[64] Nos n.os 1, 2 e 4 do novo artigo 17.º. Primeiro, porque utilizava dois critérios diferentes de necessidade probatória consoante a entidade que tivesse ordenado ou valido a apreensão: se o JIC, o critério seria o da mera necessidade para a prova e esta seria imediatamente utilizável; porém, se tivesse sido o MP, seria necessária nova decisão de "utilização probatória" por parte do JIC, esta já sujeita a um critério de "grande interesse para a descoberta da verdade ou para a prova". Incompreensível. Depois, quanto ao n.º 2, por permitir aos OPC's efectuarem as apreensões "quando haja urgência ou perigo na demora", o que se afigura excessivamente amplo e indeterminado. Não já nos casos previstos no artigo 15.º, onde não vejo qualquer problema: ou há consentimento ou são «casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa», que o próprio TC admite como deverem permitir um regime excepcional.

criminal como se estivéssemos no início do sec. XX e não no início do sec. XXI. A maior eficácia na aquisição da (mesma espécie de) prova nunca poderá constituir um problema.

De entre os vários possíveis regimes legais para a delimitação recíproca da competência de MP e JIC na pesquisa e apreensão de dados informáticos, alguns devem ser afastados por desconformidade constitucional: ou por não preverem qualquer intervenção do JIC, ou por preverem demasiada intervenção do mesmo, ofendendo a estrutura acusatória do processo, o exercício da acção penal pelo MP e até a função do JIC no sistema de garantias de defesa.

Quer o regime vigente, interpretado da forma como interpreto (com o JIC a intervir apenas posteriormente, decidindo da utilização probatória), quer um (dependente de alteração legislativa), em que seja dele a autorização para a pesquisa e apreensão (sem qualquer intervenção posterior) são conformes à Constituição: respeitam a reserva de juiz e a estrutura acusatória do processo, asseguram as garantias de defesa e protegem adequadamente os direitos fundamentais.

Em consequência, continuo convicto que não existe qualquer invalidade – por violação da reserva de juiz ou por ofensa a direitos fundamentais – nos processos pendentes em que a decisão de apreensão do correio electrónico foi sempre do JIC, precedida ou não de visualização pelo MP. Não obstante, os magistrados do MP que se sintam inseguros com tal posição sempre poderão passar a solicitar autorização prévia ao JIC para proceder a pesquisa e apreensão dos dados informáticos em todos os sistemas informáticos de uso pessoal, ficando a utilização daqueles sensíveis ou íntimos, ou de correio electrónico ou semelhante, dependente de juízo concreto do JIC em apreciação de requerimento do MP. Fá-lo-ão, porém, com a consciência das incoerências de regime supra identificadas em II.3.4.

Este acórdão veio acentuar a necessidade de tornar mais seguro para o aplicador o regime vigente, neste e noutros aspectos. Uma possível alteração legislativa poderá ser a de, não alterando, em sentido diverso, o paradigma actual, deixar mais claro quais são as funções de MP e do JIC; outra poderá ser a de prever a competência do JIC para autorizar a pesquisa e apreensão dos dados informáticos, pelo menos em todos os sistemas informáticos de uso pessoal.[65]

[65] O que não me parece adequado e sustentado seria dividir a competência entre o MP e o JIC seguindo os critérios de competências do CPP para as buscas, o que não raramente já terá sido feito. Nesses termos, se o sistema informático a pesquisar estivesse num domicílio a competência para ordenar a pesquisa seria do JIC; se estivesse fora dele, do MP. Creio que com esse critério se confunde acesso ao local físico onde está o sistema com acesso aos dados informáticos, fazendo depender a protecção a estes últimos

Esta segunda via, embora contrária ao sentido de evolução que, em meu entender, deveria ser seguido, talvez seja aquela que maior segurança dará aos aplicadores, precavendo-os contra possíveis juízos de inconstitucionalidade. Aproximaria então o regime da apreensão dos dados informáticos do regime vigente para a intercepção dos mesmos dados: depois de prévia autorização pelo JIC, o MP realizaria a pesquisa e tomaria conhecimento do conteúdo dos dados, determinando quais a usar como prova, sem prejuízo de arguido e assistente mais tarde o poderem também fazer. Este é o regime vigente desde 1998 para as intercepções telefónicas e, creio, a sua conformidade constitucional nunca foi fundadamente questionada.

Qualquer que seja o caminho, deverá ficar clara a admissibilidade de pesquisa e apreensão de dados informáticos (incluindo dados sensíveis ou íntimos, ou de correio electrónico e semelhantes) sem autorização prévia de juiz em casos de urgência e necessidade de impedir crimes de onde possam resultar danos graves e/ou irreparáveis a bens jurídicos de diferentes naturezas – pesquisa e apreensão imediatamente depois comunicadas ao JIC e por este apreciadas em ordem à sua validação. Algo que parta do hoje previsto para as buscas domiciliárias (artigos 174.º, n.º 5, e 177.º, n.º 3, do CPP), mas o adapte ao mundo digital. Assim, não esquecendo as situações de consentimento, para além dos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa, outros crimes há (estritamente informáticos, cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico) que as suas consequências, podendo ser diversas mas não menos importantes do que a ofensa à integridade física, serão mais dificilmente reparáveis.[66] Sem olvido de que aquilo que fundamenta a possibilidade de busca domiciliária em acto seguido à detenção em flagrante delito – a necessidade de intervenção urgente e imediata para que a prova não "desapareça" da residência do arguido – também fundamenta a necessidade de imediata pesquisa e apreensão para que os dados informáticos não "desapareçam" dos seus domicílios virtuais.

É urgente essa alteração legislativa.

---

de factores completamente aleatórios e mutáveis (sistemas informáticos com grande potencialidade de conterem dados privados como os *laptops, tablets* ou *smartphones* poderão ser encontrados em casa ou fora dela consoante o momento do dia).

[66] Pense-se, p. ex., na situação em que o agente acede ilegitimamente ao *smartphone* de outra pessoa e passa a transmitir em directo, na *internet*, o som o imagem que o aparelho, sem o conhecimento do seu utilizar, está a captar.