



TRIBUNAL CONSTITUCIONAL

COTA:

---- Em 29 de outubro de 2024 consigno que vou juntar requerimento, com documento, do Ex.mo Juiz Conselheiro José Eduardo Figueiredo Dias, com douto despacho do Presidente desta 2^a Secção à margem exarado. -----

O Oficial de Justiça,

802
R

TRIBUNAL CONSTITUCIONAL

Processo n.º 1104/2022

Pleno

Exmo. Senhor Conselheiro Vice-Presidente do Tribunal Constitucional

Compulsada a declaração de voto por mim apostada ao Acórdão n.º 533/2024, constato que a mesma padece de inexatidões que importa retificar.

Assim sendo, requer-se a Vossa Excelência a junção aos autos da declaração de voto retificada que segue em anexo ao presente e que substituirá, para todos os efeitos legais e processuais, a declaração de voto retificada.

Lisboa, 29 de outubro de 2024

(José Eduardo Figueiredo Dias)

Proceda imediatamente à rectificação assinada pelo Senhor Conselheiro
José Eduardo Figueiredo Dias.

Notifique:

Conclua os autos ao Senhor Conselheiro António José Araújo
Amaral para que determine se, perante esta circunstância processual,
é apropriado que as partes gozem de novo prazo para apresentarem
se justifica que as partes gozem de novo prazo para apresentarem
os argumentos ou produzirem as abstracções e que falem d'íntio, nos
termos da lei.

Lisboa, 29 de outubro de 2024.

V.S.F.F.-r



TRIBUNAL CONSTITUCIONAL

CÓPIA DO DESPACHO PROFERIDO EM 29.X.24

À MARGEM EXARADO NO REQUERIMENTO APRESENTADO PELO SENHOR
CONSELHEIRO JOSÉ EDUARDO FIGUEIREDO DIAS (Proc. 1104/22)

3^a Secção

Relator: Vice-Presidente **GONÇALO ALMEIDA RIBEIRO**

*«Proceda imediatamente à retificação requerida pelo Senhor
Conselheiro José Eduardo Figueiredo Dias.*

*Conclua aos autos ao Senhor Conselheiro António José Ascensão
Ramos, para que determine se, perante esta vicissitude processual, se justifica que as
partes gozem de novo prazo para apresentarem os requerimentos ou produzirem as
alegações a que têm direito, nos termos da lei.*

Lisboa, 29 de outubro de 2024

a) Gonçalo de Almeida Ribeiro»

ESTÁ CONFORME

Lisboa, 30 de outubro de 2024

O Oficial de Justica,



803
21

TRIBUNAL CONSTITUCIONAL

Processo n.º 1104/2022
Pleno

DECLARAÇÃO DE VOTO – RETIFICAÇÃO

Por manifesto lapso, pelo qual me penitencio, a declaração de voto por mim apostada ao Acórdão n.º 533/2024, de 04 de julho, corresponde a um simples documento de trabalho e não à respetiva versão final, contendo inexatidões que importa retificar.

Assim sendo, onde se lê:

«Vencido, por entender que a **norma do artigo 18.º, n.º 1, alínea c)**, da Lei n.º 19/2012, de 8 de maio, que aprovou o Regime Jurídico da Concorrência (na redação original, anterior à conferida pela Lei n.º 17/2022, de 17 de agosto), **no sentido indicado nos autos, é inconstitucional**, pelas seguintes razões:

a) É **inconstitucional**, por violação do disposto nos **artigos 32.º, n.º 4, e 34.º, n.ºs 1 e 4**, este conjugado com o **artigo 18.º, n.º 2**, todos da Constituição, pelas razões constantes do Acórdão n.º 91/2023, de 16 de março – em particular, nos seus **pontos 25. e 26.**;

b) E é também **inconstitucional**, por violação do **artigo 34.º, n.º 4, da Constituição**, pelas razões expressas pelo **Conselheiro Afonso Patrão**, em declaração de voto apostada ao mesmo Acórdão n.º 91/2023.»

deverá ler-se:

«Vencido, por entender que a **norma do artigo 18.º, n.º 1, alínea c)**, da Lei n.º 19/2012, de 8 de maio, que aprovou o Regime Jurídico da Concorrência (na redação original, anterior à conferida pela Lei n.º 17/2022, de 17 de agosto), **no sentido indicado nos autos, é inconstitucional**, por violação do **artigo 34.º, n.º 4, da Constituição**, pelas razões expressas



804
a

TRIBUNAL CONSTITUCIONAL

pelo **Conselheiro Afonso Patrão**, em declaração de voto apostado ao mesmo Acórdão n.º 91/2023.».

Retifique nos locais próprios, incluindo todas as bases de dados onde se encontra publicitado o presente acórdão e no sítio do Tribunal Constitucional na *Internet*.

A handwritten signature in black ink, appearing to read "José Eduardo Figueiredo Dias".

José Eduardo Figueiredo Dias



805

TRIBUNAL CONSTITUCIONAL

CONCLUSÃO

Nº 1 ----- Em 29 de outubro de 2024, ao Ex.mo Cons. Relator.-----

2 O Oficial de Justica,

3

4 -cls-

5 Tendo em conta o artigo 8º
6 da lei de voto preventivo para eleições
7 presenciais (Lei n.º 10-A/2019) e tendo a
8 pessoa eleitoral com os seguintes a
9 declarar já consultado, não que os
10 partidos políticos no seu âmbito, prete-
11 gem nenhuma figura judicial, ou detêm
12 de os mesmos só desempenhará a sua
13 autorização apresentada)

a

13 J.J., 30/10/2024

14

J. J. & F.



TRIBUNAL CONSTITUCIONAL

CÓPIA DO DESPACHO PROFERIDO EM 30.10.24

NOS AUTOS DE RECURSO N° 1104/24

2^a Secção

Relator: Conselheiro ANTÓNIO JOSÉ ASCENSÃO RAMOS

«Tendo em conta a retificação da declaração de voto apresentada pelo Senhor Conselheiro José Eduardo Figueiredo Dias e podendo a mesma colidir com os requerimentos e alegações já apresentados, notifique as partes para querendo, no prazo legal, apresentarem novos requerimentos/alegações ou dizerem se as mesmas são desnecessárias face às já anteriormente apresentadas.

Lisboa, 30/10/2024

a) António José Ascensão Ramos»

ESTÁ CONFORME

Lisboa, 31 de outubro de 2024

O Oficial de Justiça,

Rua de O Século, 111, 1249-117 Lisboa – Telef. 213 233 600/700 Fax 213 233 610

Home Page: <http://www.tribunalconstitucional.pt>

E-Mail: processos@tribconstitucional.pt

315
R

TRIBUNAL CONSTITUCIONAL
ACÓRDÃO N.º 533/2024*

Processo n.º 1104/22

2.º Secção

Relator: Conselheiro António José da Ascensão Ramos

*

Acordam na 2.º Secção do Tribunal Constitucional

I. Relatório

1. Somafel – Engenharia e Obras Rodoviárias, SA (doravante, Somafel, SA) interpôs recurso para o Tribunal Constitucional ao abrigo do artigo 70.º, n.º 1, alínea b) da Lei n.º 28/82 de 15 de novembro (LTC) do acórdão do Tribunal da Relação de Lisboa de 26 de outubro de 2022, pedindo a fiscalização das seguintes normas com os seguintes fundamentos:

- Artigo 18.º, n.º 1, alínea c), da Lei n.º 19/2012, de 8 de maio, que aprovou o Regime Jurídico da Concorrência (na redação original, anterior à conferida pela Lei n.º 17/2022, de 17 de agosto – doravante RJdC), quando interpretado no sentido de que “é possível, em processo de contraordenação da concorrência, examinar, recolher e apreender mensagens de correio eletrónico”, com fundamento em “violação da reserva absoluta ao processo penal da admissibilidade da ingerência, por autoridade pública, na correspondência, telecomunicações e demais meios de comunicação e, consequentemente, da garantia jusfundamental de inviolabilidade das mesmas” decorrente do disposto no artigo 34.º, n.º 4 da Constituição da República Portuguesa, também “em conjugação com o princípio da proporcionalidade decorrente do artigo 18.º n.º 2º do diploma;
- Artigo 18.º, n.º 1, alínea c), do RJdC quando interpretado no sentido de admitir a “possibilidade de exame, recolha e/ou apreensão de mensagens de correio eletrónico «abertas» ou «fechadas»”, com fundamento em violação dos “direitos à inviolabilidade da correspondência e das comunicações (...) e à proteção dos dados pessoais no âmbito da utilização da informática (...) enquanto regras específicas do direito à reserva de intimidade da vida privada” decorrente do disposto nos artigos 34.º, n.ºs 1 e 4, 35.º, n.ºs 1 e 4 e 26.º, n.º 1, todos da Constituição da República Portuguesa, em articulação com o princípio da proporcionalidade (artigo 18.º, n.º 2, da Constituição da República Portuguesa);

* Retificada Declaração de Voto do Cons. José Eduardo Figueiredo Dias (fls.454)

conforme fls. 802-805.

320
28

TRIBUNAL CONSTITUCIONAL

- Artigo 18.º, n.º 1, alínea c), do RjdC, quanto interpretado no sentido de “admitir o exame, recolha e apreensão de mensagens de correio eletrónico em processo de contraordenação da concorrência sem despacho judicial prévio” com fundamento em “violação dos princípios do Estado de direito democrático e da reserva de juiz para a ponderação da efetuação de direitos fundamentais em direito sancionatório, em particular, do direito à inviolabilidade e ao sigilo da correspondência, contidos nos artigos 2.º, 18.º n.º 2, 32.º n.º 4 e 34.º n.ºs 1 e 4 dd” Constituição da República Portuguesa;

[REDAÇÃO] interpôs também recurso ao abrigo da alínea b), do n.º 1, do artigo 70.º, da LTC, do acórdão do Tribunal da Relação de Lisboa de 26 de outubro de 2022, pedindo a fiscalização das seguintes normas com os seguintes fundamentos:

- Artigo 18.º, n.º 1, alínea c), do RjdC, quando interpretado no sentido de admitir a “possibilidade de exame, recolha e/ou apreensão de mensagens de correio eletrónico «abertas» ou «lidas»”, com fundamento em violação “dos direitos à inviolabilidade da correspondência e das comunicações, consagrados no artigo 34.º, n.ºs 1 e 4, da Constituição da República Portuguesa, e à proteção dos dados pessoais no âmbito da utilização da informática, nos termos do artigo 35.º, n.ºs 1 e 4, da CRP, enquanto infrações específicas do direito à reserva de intimidade da vida privada, consagrado no artigo 26.º, n.º 1, da CRP, bem como do princípio da proporcionalidade tal como previsto no artigo 18.º, n.º 2 da CRP”;
- Artigo 18.º, n.º 1, alínea c), do RjdC, quando interpretado no sentido de que “é possível, em processo de contraordenação da concorrência, examinar, recolher e apreender mensagens de correio eletrónico”, com fundamento em “violação da reserva absoluta ao processo penal da admissibilidade da ingerência, por autoridade pública, na correspondência, telecomunicações e demais meios de comunicação e, consequentemente, da garantia fundamental de inviolabilidade das mesmas, tal como previstas e consagradas no disposto no artigo 34.º, n.º 4 da CRP”;
- Artigo 18.º, n.º 1, alínea c), do RjdC, quando interpretado no sentido de “admitir o exame, recolha e apreensão de mensagens de correio eletrónico em processo de contraordenação da concorrência, sem despacho judicial prévio”, com fundamento em violação dos “princípios do Estado de Direito democrático e da reserva de juiz para a ponderação da efetuação de direitos fundamentais em direito sancionatório, em particular, do direito à inviolabilidade e ao sigilo da correspondência, contidos nos artigos 2.º, 18.º, n.º 2, 32.º n.º 4 e 34.º n.ºs 1 e 4”, todos da Constituição da República Portuguesa;



TRIBUNAL CONSTITUCIONAL

2. Somafel, SA foi condenada pela Autoridade da Concorrência (AdC) pela prática de duas contraordenações, p. p. pelo artigo 101.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) e artigo 68.º, n.º 1, alínea a) e 9.º, n.º 1, ambos do RjdC, na coima única, apurada em címulos jurídicos, de € 925.000,00 e na sanção acessória de publicação de um extrato da decisão em jornal de expansão nacional, a seu encargo.

Paulo Alfredo Carvalho Serradas foi condenado pela AdC pela prática de duas contraordenações, p. p. pelo artigo 101.º, n.º 1, do TFUE e artigos 73.º, n.ºs 1 e 6, e 68.º, n.º 1, alínea a), ambos do RjdC, na coima única, apurada em címulos jurídicos, de € 11.800,00.

Desta decisão, ambos os arguidos interpuseram recurso judicial para o Tribunal do Juízo central de Concorrência, Regulação e Supervisão da comarca de Lisboa.

3. O recurso de Somafel, SA foi julgado parcialmente procedente, resultando condenada pela prática de uma contraordenação, p. p. pelo artigo 101.º, n.º 1, do TFUE, e artigos 9.º, n.º 1, alínea a), e 68.º, n.º 1, alínea a), ambos do RjdC e uma contraordenação, p. p. pelo artigo 101.º, n.º 1, do TFUE, e artigos 9.º, n.º 1, alíneas a) e b), e 68.º, n.º 1, alínea a), ambos do RjdC, na coima única, apurada em címulos jurídicos, de € 640.000,00 e na sanção acessória de publicação de um extrato da decisão em jornal de expansão nacional, a seu encargo.

O recurso de [REDACTED] foi também julgado parcialmente procedente, resultando condenado pelas contraordenações constantes da decisão administrativa na coima única, apurada em címulos jurídicos, de € 6.800,00.

Ainda inconformados, ambos os arguidos interpuseram recurso da sentença para o Tribunal da Relação de Lisboa que, pelo acórdão ora recorrido, lhes negou provimento.

Os recursos interpostos para o Tribunal Constitucional, supra relatados, foram admitidos e os autos recebidos neste Tribunal.

4. Depois de notificada para o efeito, a recorrente Somafel, SA apresentou alegações concluindo do seguinte modo:

"1. O presente recurso vem interposto quanto ao Acórdão do Tribunal da Relação de Lisboa, de 26.10.2022, que veio negar provimento ao recurso interposto pela Somafel da Sentença do TCRS, de entre o mais, na parte em que a



TRIBUNAL CONSTITUCIONAL

372
8.

Recorrente arguiu a nulidade da prova correspondente ao correio eletrónico apreendido e que serve de alicerce à decisão final condenatória da AdC e, bem assim, àquela sentença, bem como quanto às questões de constitucionalidade suscitadas e agora trazidas à apreciação deste Tribunal Constitucional.

2. No Acórdão Recorrido, o Tribunal da Relação de Lisboa interpretou e aplicou, como ratio decidendi, as seguintes normas, cuja apreciação da respectiva conformidade à Constituição a Recorrente vem pelo presente submeter à apreciação de V. Exas.:

(i) a norma que se extrai do disposto no artigo 18.º, n.º 1, alínea c) da LdC, quando interpretada no sentido de que é possível, em processo de contraordenação da concorrência, examinar, recolher e apreender mensagens de correio eletrónico, por violação da reserva absoluta ao processo penal da admissibilidade da ingerência, por autoridade pública, na correspondência, telecomunicações e demais meios de comunicação e, consequentemente, da garantia insfundamental de inviolabilidade das mesmas, tal como previstas e consagradas no disposto no artigo 34.º, n.º 4 da CRP, em conjugação com o princípio da proporcionalidade (efr. 18.º, n.º 2 da CRP) ("Primeira Questão de Constitucionalidade");

(ii) a norma constante do artigo 18.º, n.º 1, alínea c) da LdC, quando interpretada no sentido de que o mesmo prevê a possibilidade de exame, recolha e/ou apreensão de mensagens de correio eletrónico "abertas" ou "lidas" porquanto tais mensagens de correio eletrónico consubstanciam meros documentos, por violação dos direitos à inviolabilidade da correspondência e das comunicações (consagrado no artigo 34.º, n.ºs 1 e 4, da CRP), e à proteção dos dados pessoais no âmbito da utilização da informática (nos termos do artigo 35.º, n.ºs 1 e 4, da CRP), enquanto regras específicas do direito à reserva de intimidade da vida privada, (consagrado no artigo 26.º, n.º 1, da Constituição), bem como do princípio da proporcionalidade tal como previsto no artigo 18.º, n.º 2 da CRP ("Segunda Questão de Constitucionalidade"));

(iii) a norma contida no artigo 18.º, n.º 1, alínea c) da LdC, no sentido de admitir o exame, recolha e apreensão de mensagens de correio eletrónico em processo de contraordenação da concorrência, sem despacho judicial prévio, por violação dos princípios do Estado de direito democrático e da reserva de juiz para a ponderação da afetação de direitos fundamentais em direito sancionatório, em particular, do direito à inviolabilidade e ao sigilo da correspondência, contidos nos artigos 2.º, 18.º, n.º 2, 32.º n.º 4 e 34.º n.ºs 1 e 4 da CRP ("Terceira Questão de Constitucionalidade").

3. A apreciação das questões de constitucionalidade elencadas requer, essencialmente, a resposta autónoma, à luz da Constituição e da lei, a cada uma das seguintes interrogações práticas:

(i) é conforme à CRP examinar, recolher e apreender mensagens de correio eletrónico no âmbito de diligências de busca e apreensão levadas a cabo em processo de contraordenação de direito da concorrência?

(ii) é conforme à CRP examinar, recolher e apreender mensagens de correio eletrónico se "abertas" ou "lidas" no âmbito de diligências de busca e apreensão levadas a cabo em processo de contraordenação de direito da concorrência?

(iii) é conforme à CRP examinar, recolher e apreender mensagens de correio eletrónico no âmbito de diligências de busca e apreensão levadas a cabo em processo de contraordenação de direito da concorrência, sem despacho judicial prévio, bastando para tanto um despacho do Ministério Público?

4. A Somafel invoca a inconstitucionalidade das normas em crise, porquanto considera que as mesmas comprometem, de forma irremediável, o princípio do Estado de Direito Democrático, assente no respeito pelos direitos fundamentais dos privados (artigo 2.º da CRP), o princípio da vinculatividade e aplicação direta dos direitos fundamentais (artigo 18.º, n.ºs 1 e 2 da CRP), o princípio da reserva de juiz para a ponderação da afetação de direitos fundamentais em direito sancionatório (artigo 32.º, n.º 4), a garantia da inviolabilidade e sigilo da correspondência e a proibição de ingerência de autoridades públicas na mesma (artigo 34.º n.ºs 1 e 4) e o princípio da subordinação da atuação da Administração à Lei e à Constituição (artigo 266.º da CRP), consubstanciando, nessa medida, e pelas razões melhor explicitadas nas nestas alegações supra, Normas materialmente inconstitucionais.

Quanto à Primeira Questão de Constitucionalidade

5. O correio eletrónico é, na actualidade, um dos meios de comunicação por exceléncia e, por isso, reclama adeuada proteção constitucional.

6. O correio eletrónico integra o conceito de correspondência (ou pelo menos de outro meio de comunicação) constitucionalmente previsto, e, como tal, o meio de comunicação, o conteúdo da comunicação (i.e. as mensagens de correio eletrónico) e os dados associados à comunicação (nomeadamente os dados de tráfego) beneficiam de proteção



TRIBUNAL CONSTITUCIONAL

523
L

constitucional nos termos do artigo 34.º, n.º 1 da CRP e do artigo 8.º da CEDH, incluindo o direito à inviolabilidade do sigilo das mensagens de correio eletrónico - conteúdo e tráfego (e informações correspondentes) -, independentemente de se tratar de mensagens cujos remetentes e/ou destinatários sejam, conjunta ou separadamente, indivíduos e/ou pessoas coletivas, neste caso enviadas e recebidas através dos seus colaboradores.

7. Conforme resulta da jurisprudência do TEDH, o correio eletrónico trocado em contexto empresarial ou profissional encontra-se abrangido pelo âmbito de tutela do artigo 8.º da CEDH, inexistindo qualquer razão atendível que justifique retirar o correio eletrónico trocado nesse âmbito do alcance da proteção conferida pelo artigo 34.º da CRP.

8. A Constituição prevê uma tutela especial para a inviolabilidade do sigilo da correspondência, apenas permitindo, no n.º 4 do artigo 34.º da CRP, a ingerência das autoridades públicas na correspondência e nas telecomunicações nos casos previstos na lei e apenas em matéria de processo criminal.

9. Por ingerência deve entender-se toda a agressão ao direito fundamental da inviolabilidade do sigilo da correspondência, consubstanciada na intervenção ou acesso ao objeto protegido pela inviolabilidade do sigilo.

10. O exame, a recolha e a apreensão de mensagens de correio eletrónico configuram uma ingerência nos termos e para efeitos do disposto no artigo 34.º, n.º 4 da CRP, por permitirem o acesso ao conteúdo de mensagens de correio que estão protegidas pelo direito à inviolabilidade do sigilo da correspondência ou de outros meios de comunicação, constituindo ingerências graves - porque irremediáveis - na inviolabilidade do sigilo do correio eletrónico, e, como tal, devem ser, em regra, proibidas nos termos do artigo 34.º, n.º 4 da CRP, apenas podendo ser admitidos no âmbito do processo penal.

11. A contrário, está absolutamente vedado às autoridades públicas, entre as quais qualquer autoridade administrativa, seja qual for a sua natureza, a ingerência na correspondência e nas telecomunicações, mormente em processo de contraordenação ou em quaisquer outros processos sancionatórios de natureza não penal, como é o caso do processo de contraordenação em matéria de direito da concorrência.

12. Não se justifica admitir em processo de contraordenação a compressão do direito à inviolabilidade e ao sigilo da correspondência porque o valor em confronto tem "menor ressonância ética". Estando em causa a proteção do mesmo direito fundamental - o direito à inviolabilidade e ao sigilo da correspondência -, a importância relativamente menor do ilícito contraordenacional e dos valores sociais que protege menos ainda pode justificar qualquer limitação àquele direito.

13. O texto fundamental comina a prova obtida, de entre o mais, em violação do disposto no seu artigo 34.º, n.º 4 da CRP, com o mais severo vício existente na ordem jurídica nacional, encerrando, dessa forma, a consagração de uma nulidade de fonte constitucional (cf. artigo 32.º, n.º 8 da CRP), diretamente aplicável e vinculativa para as entidades públicas e privadas, por via do disposto no artigo 18.º n.º 1 da CRP.

14. A restrição à inviolabilidade do sigilo da correspondência em sede de investigação de eventual violação de normas de direito da concorrência com base no disposto no artigo 18.º, n.º 1, alínea c) da LdC, ou sequer com base no disposto em qualquer outra norma daquele diploma (mesmo que interpretada em conjugação com a primeira), não cumpre as restantes exigências constitucionais decorrentes do artigo 18.º da CRP, porque não tem apoio numa lei restritiva válida, nos termos e para os efeitos do disposto no artigo 18.º da CRP, por decorrer de uma violação da reserva de lei restritiva em sentido material.

15. A LdC não prevê, de forma expressa e inequívoca, em nenhuma das suas disposições, a possibilidade de exame, recolha, apreensão e utilização como prova de correio eletrónico ou, em rigor, de qualquer outro tipo de correspondência. Em rigor, a LdC não contém sequer, em nenhuma das suas numerosas disposições, as expressões correspondência, correio eletrónico, telecomunicações ou meios de comunicação.

16. A LdC, de resto, sofreu recentemente alterações legislativas (inclusivamente, com alterações do teor do seu artigo 18.º, n.º 1), na sequência do processo de transposição da Diretiva ECN+ para o ordenamento nacional, tendo esta questão sido discutida - com participação da própria AdC - e o legislador ordinário decidiu, intencionalmente e com base em parecer da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, não prever a possibilidade de ingerência pela AdC no correio eletrónico dos visados em processos de contraordenação por si tramitados ao abrigo daquele diploma.

17. A Diretiva ECN+ não obriga o Estado Português a atribuir legalmente poderes à AdC para examinar e apreender correspondência eletrónica, seja qual for o seu estado, sendo que os considerandos da Diretiva ECN+,



324

TRIBUNAL CONSTITUCIONAL

desprovidos de valor jurídico obrigatório, não podem, numa perspetiva de pretensa interpretação conforme ao Direito da União, sobrepor-se à Constituição Portuguesa e ao princípio do Estado de Direito Democrática, tal como decorre do artigo 8.º, n.º 4 da CRP. Com efeito, inexistem argumentos de direito da União ou de direito nacional que justifiquem e permitam a apreensão de correio eletrónico em processos de contraordenação de direito da concorrência.

18. A interpretação normativa do disposto no artigo 18.º, n.º 1, alínea c) da LdC (mesma que conjugadamente com o disposto no artigo 20.º, n.ºs 1 e 2 do mesmo diploma) no sentido de que aquela disposição permite à AdC, em processo de contraordenação da concorrência, examinar, recolher e apreender mensagens de correio eletrónico no âmbito de diligências de busca e apreensão é materialmente inconstitucional, não só por violação da reserva absoluta ao processo penal da admissibilidade da ingerência, por autoridade pública, na correspondência, telecomunicações e demais meios de comunicação e, consequentemente, da garantia jusfundamental de inviolabilidade das mesmas, tal como previstas e consagradas no disposto no artigo 34.º, n.º 4 da CRP, mas também dos princípios subjacente à restrição de direitos, liberdades e garantias (cfr. artigo 18.º da CRP).

Quanto à Segunda Questão de Constitucionalidade

19. Como vimos, é absolutamente seguro que a garantia constitucional do sigilo e da inviolabilidade da correspondência e demais meios de comunicação abrange não só o meio de comunicação e os dados associados à comunicação, nomeadamente os dados de tráfego, como também, e, para o que ora releva, sobretudo, o conteúdo da comunicação.

20. A distinção entre correio eletrónico não aberto/não lido e correio eletrónico aberto/lido, que sustenta a norma em crise, não encontra qualquer apoio no texto constitucional ou na letra da lei.

21. A não diferenciação entre correio eletrónico não aberto/não lido e correio eletrónico aberto/lido justifica-se, desde logo, pelas dificuldades técnicas associadas à determinação no domínio digital do que foi efetivamente aberto/lido pelos intervenientes no processo comunicativo, tendo o legislador ordinário, no quadro processual penal, reconhecido o anacronismo e a inadequação daquela diferenciação e optado por atribuir à mensagem de correio eletrónico uma tutela unitária, indiferente à sua abertura/leitura pelo destinatário.

22. As dificuldades técnicas e demais problemas que a diferenciação entre correio eletrónico não aberto/não lido e correio eletrónico aberto/lido comporta verificam-se, nos mesmos termos em que se verificam no domínio processual penal, no âmbito dos processos de contraordenação juscronenciais e respetiva investigação.

23. Com efeito, por identidade de razão, deve aquela distinção ser rejeitada também neste âmbito, entendendo-se que o correio eletrónico configura sempre correspondência e nunca um mero documento eletrónico, com as inerentes consequências de regime, desde logo a sua sujeição integral e permanente ao âmbito de proteção do artigo 34.º da CRP.

24. Por outro lado, e conforme já destacado a respeito da Primeira Questão de Constitucionalidade, também neste conspecto cumpre concluir que a interpretação normativa aqui em causa não cumpre as exigências constitucionais decorrentes do artigo 18.º da CRP, porque não tem apoio numa lei restritiva válida, nos termos e para os efeitos do disposto no artigo 18.º da CRP, por decorrer de uma violação da reserva de lei restritiva em sentido material.

25. As restrições a direitos, liberdades e garantias consagradas na lei só devem poder ser nela consagradas, com respeito pela Constituição, se, para além do mais, o forem em termos claros e apreensíveis para o cidadão comum que é deles titular.

26. Quando, para além do mais, sejam as restrições a direitos, liberdades e garantias extraídas da lei ordinária em moldes cujo teor e alcance fique na disponibilidade exclusiva da comunidade jurídica, exigindo do respetivo titular o conhecimento de complexas e pouco intuitivas posições doutrinárias e/ou jurisprudenciais por forma a conseguir apreender tais restrições, devem as normas donde são extraídas tais restrições ser rejeitadas e condenadas à inconstitucionalidade material. É o caso da norma sob escrutínio.

27. A norma extraída do artigo 18.º, n.º 1, alínea c) da LdC e aplicada no Acto da Recorrido como ratio decidendi em interpretação desproporcional e violadora daquelas exigências decorrentes da reserva de lei inscrita no artigo 18.º, n.º 2 da CRP, forçosa se assume a conclusão de aquela norma, interpretada no sentido de que o mesmo prevê a possibilidade de exame, recolha e/ou apreensão de mensagens de correio eletrónico "abertas" ou "lidas" porquanto tais mensagens de correio eletrónico consubstanciam meros documentos, é materialmente inconstitucional, não só por violação dos direitos à inviolabilidade da correspondência e das comunicações (consagrado no artigo 34.º, n.ºs 1 e 4, da CRP), e à proteção dos dados pessoais no âmbito da utilização da informática (nos termos do artigo 35.º, n.ºs 1 e 4, da CRP), enquanto regras específicas do direito à reserva de intimidade da vida privada, (consagrado no artigo

325
T

TRIBUNAL CONSTITUCIONAL

26.º, n.º 1, da Constituição), mas também por atropelo ao disposto naquele artigo 18.º, n.º 2 da Constituição. Quanto à Terceira Questão de Constitucionalidade

28. A proteção constitucional conferida ao sigilo da correspondência prevista no artigo 34.º n.º 4 da CRP impõe que a afetação desse direito, liberdade e garantia, mediante a realização de exame, recolha e apreensão de mensagens protegidas seja feita num quadro legal e normativo (o do processo penal) que assegure adequada proteção contra intrusões abusivas, no âmbito do qual, o exame, recolha e apreensão de correio eletrónico, na medida em que atentam contra a inviolabilidade da correspondência, dependem de uma ponderação prévia que, constitucionalmente, constitui matéria reservada ao juiz.

29. A reserva de juiz radica, em primeira linha, no princípio do Estado de Direito democrático, previsto no artigo 2.º da CRP, sendo imposta em matérias que possam afetar direitos fundamentais precisamente para assegurar os princípios da separação e interdependência de poderes, que corporizam um Estado de Direito.

30. O legislador constitucional previu expressamente, no artigo 32.º, n.º 4 da CRP, o princípio da reserva de juiz para quando estão em causa matérias que se prendem diretamente com direitos fundamentais no âmbito do processo criminal, como decorrência dos princípios acima referidos e *lato sensu* do princípio enformador do Estado de Direito.

31. É uma garantia constitucional funcionalmente orientada à proteção de direitos, liberdades e garantias, imposta pelo princípio do Estado de Direito democrático para permitir que, num processo crime, se possam afetar direitos fundamentais em prol da Justiça e do interesse punitivo do Estado, sem que essa restrição seja intolerável - independentemente da existência de um arguido num processo crime.

32. O Tribunal Constitucional tem estendido a proteção da norma contida no n.º 4 do artigo 32.º da CRP - e da reserva de juiz ali contida - a todas as situações do processo crime em que esteja em causa, cumulativamente, (i) uma medida que consubstancie uma ingerência em direitos fundamentais; (ii) que seja grave; e (iii) que seja executada sem possibilidade de estabelecer o contraditório do visado.

33. A apreensão de correio eletrónico consubstancia sempre (i) uma ingerência na proteção do sigilo da correspondência, (ii) que é grave (porque uma vez lido por outrem, o sigilo do conteúdo da mensagem fica irremediablemente comprometido), (iii) não sendo precedida de contraditório do visado pela diligência (todos os que possam ter os seus direitos fundamentais afetados pela mesma que não coincidem sempre nem exatamente com o arguido e/ou suspeito do crime), pelo que no âmbito de um processo crime, o disposto no artigo 32.º n.º 4 da CRP e o princípio do Estado de Direito democrático impõem que o exame, a recolha e a apreensão de correio eletrónico - do arguido ou de terceiro por afetarem o direito fundamental da inviolabilidade e do sigilo da correspondência (artigo 34.º n.º 1 e 4 da CRP) constituam matéria da reserva de juiz.

34. Em coerência, tendo presente que, no quadro do processo penal, a Constituição impõe, no seu artigo 32.º n.º 4 da CRP, e como decorrência do princípio do Estado de Direito democrático, a reserva de juiz para a adoção de qualquer medida grave, restritiva do sigilo da correspondência tomada sem contraditório do visado - como o é o exame, recolha e apreensão de correio eletrónico - também essa exigência se aplicará noutro quadro processual que não o penal caso haja necessidade de afastar a inviolabilidade da correspondência.

35. O direito fundamental violado com a medida lesiva (apreensão de correio eletrônico) não perde valor (nem podem perder proteção) em função da natureza de processo que esteja em causa.

36. Não pode ler-se na lei constitucional uma reserva da competência do juiz para autorizar a afetação de direitos fundamentais exclusivamente no processo penal; essa competência é independente da natureza do processo, nascendo, como se disse, de um outro princípio mais amplo e que não olha à distinção entre a natureza de processos: o princípio do Estado de Direito democrático.

37. Não é suficiente exigir-se a este propósito e para a mesma restrição, em processo de contraordenação, (mero) despacho do Ministério Público. O recorte constitucional e legal da organização, estatuto e garantias do Ministério Público não iguala a independência e a imparcialidade, estatutárias e funcionais, de um juiz, pelo que as exigências do Estado de Direito democrático, da imparcialidade e independência, e da separação e interdependência de poderes não se mostram suficientemente cumpridas mediante uma autorização da diligência em causa (e da compressão do direito fundamental à inviolabilidade da correspondência) mediante despacho do Ministério Público.

38. Acresce que o Ministério Público pode inclusivamente assumir as vestes de acusador, numa fase posterior do processo de contraordenação, pelo que não poderá pretender-se que o seu interesse na recolha da (melhor) prova seja,

326
L.

TRIBUNAL CONSTITUCIONAL

sempre, neutro.

39. Não havendo norma expressa quanto à apreensão de correspondência eletrónica, mas sujeitando-se a realização de diligências intrusivas de recolha de prova a autorização da autoridade judiciária competente, terá de interpretar-se a referida norma conforme à Constituição no sentido de que, sempre que a medida de recolha de prova constituir uma restrição de direito, liberdade e garantia, grave, realizada sem contraditório prévio do visado, a mesma fica sujeita a reserva de juiz, dependendo de despacho judicial.

40. Conclui-se que o desenho legislativo da investigação em processo contraordenacional é compatível e materialmente equivalente à fase de inquérito em processo penal, e segundo a interpretação do artigo 32.º n.º 4 da CRP que tem sido acolhida - de forma unânime - por este Tribunal Constitucional, terá de se concluir que a medida de exame, recolha e apreensão de correio eletrónico - porque consubstancia uma ingerência grave no sigilo da correspondência do visado pela mesma - carece de despacho judicial prévio, sob pena de ser considerada intolerável num Estado de Direito democrático.

41. Consequentemente, a interpretação da norma contida nos artigos 18.º n.º 1 alínea c), n.º 2, 20.º n.º 1 e 21.º da LdC, no sentido de admitir o exame, recolha e apreensão de mensagens de correio eletrónico em processo de contraordenação da concorrência, sem despacho judicial prévio, é materialmente inconstitucional, por violação dos princípios do Estado de direito democrático e da reserva de juiz para a ponderação da afectação de direitos fundamentais em direito sancionatório, em particular, do direito à inviolabilidade e ao sigilo da correspondência, contidos nos artigos 2.º, 32.º n.º 4 e 34.º n.ºs 1 e 4 da CRP.

Nestes termos e nos moldes de Direito, requer-se a V. Exas. se dignem julgar o presente recurso de constitucionalidade, com os fundamentos invocados, procedente com as devidas e legais consequências, julgando inconstitucionais:

a) a norma que se extrai do disposto no artigo 18.º, n.º 1, alínea c) da LdC, quando interpretada no sentido de que é possível, em processo de contraordenação da concorrência, examinar, recolher e apreender mensagens de correio eletrónico, por violação da reserva absoluta ao processo penal da admissibilidade da ingerência, por autoridade pública, na correspondência, telecomunicações e demais meios de comunicação e, consequentemente, da garantia jufundamental de inviolabilidade das mesmas, tal como previstas e consagradas no disposto no artigo 34.º, n.º 4 da CRP, em conjugação com o princípio da proporcionalidade (cf. 18.º, n.º 2 da CRP);

b) a norma constante do artigo 18.º, n.º 1, alínea c) da LdC, quando interpretada no sentido de que o mesmo prevê a possibilidade de exame, recolha e/ou apreensão de mensagens de correio eletrónico "abertas" ou "lidas" enquanto tais mensagens de correio eletrónico consumstançam meros documentos, por violação dos direitos à inviolabilidade da correspondência e das comunicações (consagrado no artigo 34.º, n.ºs 1 e 4, da CRP), e à proteção dos dados pessoais no âmbito da utilização da informática (nos termos do artigo 35.º, n.ºs 1 e 4, da CRP), enquanto infrações específicas do direito à reserva de intimidade da vida privada, (consagrado no artigo 26.º, n.º 1, da Constituição), bem como do princípio da proporcionalidade tal como previsto no artigo 18.º, n.º 2 da CRP; e

(c) a norma contida no artigo 18.º, n.º 1, alínea c) da LdC, no sentido de admitir o exame, recolha e apreensão de mensagens de correio eletrónico em processo de contraordenação da concorrência, sem despacho judicial prévio, por violação dos princípios do Estado de direito democrático e da reserva de juiz para a ponderação da afectação de direitos fundamentais em direito sancionatório, em particular, do direito à inviolabilidade e ao sigilo da correspondência, contidos nos artigos 2.º, 18.º, n.º 2, 32.º n.º 4 e 34.º n.ºs 1 e 4 da CRP.

Mais se requer que, consequentemente, seja ordenada a baixa dos autos ao Tribunal da Relação de Lisboa a fim de que este reformar a decisão em conformidade com o julgamento sobre a questão da inconstitucionalidade.

Assim fazendo Justiça!



TRIBUNAL CONSTITUCIONAL

O recorrente [REDACTED] de sua parte, apresentou alegação enunciando as seguintes conclusões:

- "1. A interpretação da norma contida no artigo 18.º, n.º 1, alínea c) do RJC, sustentada no Acórdão recorrido, no sentido de que o mesmo prevê a possibilidade de exame, recolha e/ou apreensão de mensagens de correio eletrónico "abertas" ou "lidas" é materialmente inconstitucional, por violação dos direitos à inviolabilidade da correspondência e das comunicações, consagrados no artigo 34.º, n.ºs 1 e 4, da Constituição da República Portuguesa (adiante "CRP"), e à proteção dos dados pessoais no âmbito da utilização da informática, nos termos do artigo 35.º, n.ºs 1 e 4, da CRP, enquanto regras específicas do direito à reserva de intimidade da vida privada, consagrado no artigo 26.º, n.º 1, da CRP, bem como do princípio da proporcionalidade tal como previsto no artigo 18.º, n.º 2 da CRP.*
- 2. Conforme resulta da recente da recente jurisprudência deste Tribunal Constitucional (cfr. Acórdão do Tribunal Constitucional n.º 687/2021, publicado em 30.08.2021), o âmbito da proteção constitucional do sigilo da correspondência eletrónica decorrente do artigo 34.º n.º 1 da Constituição da República Portuguesa (CRP) (i) abrange o seu conteúdo, (ii) os dados associados à comunicação, e (iii) não distingue se a comunicação em causa foi ou não aberta ou lida pelo seu destinatário, rejeitando-se, dessa forma, os fundamentos em que assenta o Acórdão recorrido.*
- 3. Sublinha-se ainda que, o exposto na referida jurisprudência tanto vale no âmbito da Lei do Cibercrime, como valerá para qualquer outra lei ordinária da qual se pretenda retirar a possibilidade de apreensão de correspondência [em particular, para efeitos de interpretação do RJC, nomeadamente do seu artigo 18.º, n.º 1, alínea c), do qual o Acórdão recorrido pretende retirar permissão para a apreensão das mensagens de correio eletrónico].*
- 4. Também a interpretação da norma contida no artigo 18.º n.º 1 alínea c) do RJC, sustentada no acórdão recorrido, no sentido de que é possível, em processo de contraordenação da concorrência, examinar, recolher e apreender mensagens de correio eletrónico é materialmente inconstitucional, por violação da reserva absoluta ao processo penal da admissibilidade da ingerência, por autoridade pública, na correspondência, telecomunicações e demais meios de comunicação e, consequentemente, da garantia fundamental de inviolabilidade das mesmas, tal como previstas e consagradas no disposto no artigo 34.º, n.º 4 da CRP, em conjugação com o princípio da proporcionalidade previsto no artigo 18.º, n.º 2 da CRP.*
- 5. Conforme decorre do disposto no artigo 34.º, n.º 4, parte final, da CRP, "salvo nos casos previstos na lei em matéria de processo penal" é proibida a ingerência das autoridades públicas na correspondência e nas comunicações.*
- 6. Está, pois, absolutamente vedado às autoridades públicas, entre as quais qualquer autoridade administrativa (incluindo a Autoridade da Concorrência), a ingerência na correspondência e nas telecomunicações, em processo de contraordenação ou em quaisquer outros processos sancionatórios de natureza não penal.*
- 7. Por fim, a interpretação da norma contida no referido artigo 18.º, n.º 1, alínea c) do RJC, sustentada no Acórdão recorrido, no sentido de admitir o exame, recolha e apreensão de mensagens de correio eletrónico em processo de contraordenação da concorrência, sem despacho judicial prévio é materialmente inconstitucional, por violação dos princípios do Estado de Direito democrático e da reserva de juiz para a ponderação da aferição de direitos fundamentais em direito sancionatório, em particular, do direito à inviolabilidade e ao sigilo da correspondência, contidos nos artigos 2.º, 18.º, n.º 2, 32.º n.º 4 e 34.º n.ºs 1 e 4, todos da CRP.*
- 8. Com efeito, sendo o desenho legislativo da investigação em processo contraordenacional compatível e materialmente equivalente à fase de inquérito em processo penal, e seguindo a interpretação do artigo 32.º, n.º 4 da CRP que tem sido acolhida pelo Tribunal Constitucional, bem como atendendo ao enquadramento plasmado no referido Acórdão n.º 687/2021 quanto à indispensabilidade da reserva de juiz nesta matéria, terá de se concluir que a medida de exame, recolha e apreensão de correio eletrónico - porque constitui uma ingerência grave no sigilo da correspondência do visado pela mesma - carece de despacho judicial prévio, sob pena de ser considerada intolerável num Estado de Direito democrático.*

Termos em que, com as devidas consequências legais, se requer a V. Exas. se dignem julgar inconstitucional:

- (i) a norma contida no artigo 18.º, n.º 1, alínea c) do RJC, interpretada no sentido de que o mesmo prevê a possibilidade de exame, recolha e/ou apreensão de mensagens de correio eletrónico "abertas" ou "lidas";*



TRIBUNAL CONSTITUCIONAL

527
8.

(ii) a norma contida no artigo 18.º, n.º 1, alínea c) do RJC, interpretada no sentido de que é possível, em processo de contraordenação da concorrência, examinar, recolher e apreender mensagens de correio eletrónico; (iii) a norma contida no referido artigo 18.º, n.º 1, alínea c) do RJC, interpretada no sentido de admitir o exame, recolha e apreensão de mensagens de correio eletrónico em processo de contraordenação da concorrência, sem despacho judicial prévio.”

O Ministério Público respondeu à alegação, apresentando as seguintes conclusões:

“1. Os recorrentes sustentam o seu juízo da constitucionalidade da interpretação normativa extraída do arco normativo constituído pelos artigos 18.º a 21.º do Regime Jurídico da Concorrência no sentido de que em processo por prática restritiva da concorrência é permitida a busca e apreensão de mensagens de correio eletrónico, na ideia de que a apreensão de “e-mails” que já haviam sido abertos ou lidos, documentos que circularam por uma pluralidade de destinatários e que se encontravam acessíveis a um conjunto de utilizadores profissionais para além dos seus destinatários, representaria uma ingerência das autoridades na correspondência ou em telecomunicações, violando, consequentemente, o disposto o princípio da inviolabilidade da correspondência, enquanto regra do princípio da proteção da intimidade da vida privada.

2. Ora, a visualização, e mesmo a apreensão, de conteúdos documentais que, num dado momento histórico, possam ter sido transmitidos por correio eletrónico, mas que no momento relevante da sua aquisição processual, já após terem sido abertos ou lidos e acedidos por distintos destinatários profissionais que não os seus destinatários, não podem ser considerados em trânsito.

3. Na verdade, se tais documentos já não se encontram num processo dinâmico de comunicação ou de transmissão de informação entre um emissor e um receptor e, distintamente, se revelam reais documentos consolidados porque estabilizados após as suas abertura, leitura e divulgação, então não se pode considerar que exista correspondência ou telecomunicação nas quais as autoridades – Autoridade da Concorrência ou Ministério Público – possam exercer qualquer ingerência.

4. Sobre este tema, embora na sua dimensão criminal e processual criminal, pronunciou-se Paulo Dá Mesquita, a páginas 111 e 112, da sua obra “Processo penal, prova e sistema judiciário”, Coimbra Editora, 2010, nos seguintes termos:

“No art. 17.º [da Lei n.º 109/2009, de 15 de Setembro], apesar da redação pouco clara, a remissão para as regras do processo penal sobre a apreensão de correspondência parece implicar que a mesma reconduz o intérprete à teologia do regime processual sobre a apreensão de correspondência, pelo que não são objecto da sua tutela especial, nomeadamente, mensagens de correio eletrónico e já acedidas pelo destinatário. Apreensão de correio eletrónico e registos de comunicações de natureza semelhante, que convoca, além do regime geral do art. 179.º, a medida cautelar e de polícia dos n.ºs 2 e 3 do art. 252.º do CPP”.

5. Sobre a mesma temática, sustentam Germano Marques da Silva e Fernando Sá, a páginas 771 e 772 da Constituição Portuguesa Anotada (Coord. Jorge Miranda e Rui Medeiros), Vol. I, Coimbra Editora, 2010, que: “Através do sigilo da correspondência, a Constituição pretende proteger o tráfego de informação privada que circula, em suporte corpóreo, entre pessoas determinadas. O objecto de protecção é o conteúdo da correspondência individual, entre um remetente e um destinatário, não obtendo protecção constitucional, através do artigo 34.º, por exemplo, uma carta escrita que manifestamente não foi ou será enviada.

Parece fundamental que a correspondência circule de forma fechada, porque só dessa forma se pode concretizar a dimensão constitucional de protecção da esfera privada, da qual o sigilo da correspondência é tributário”.

6. Mais à frente, a páginas 773, os mesmos autores afirmam que:

“A esta luz, é possível afirmar que meios como o fax, o e-mail, telefone e videoteléfono partilham, em regra, da garantia constitucional do sigilo. Haverá muitos meios, especialmente aqueles que têm como suporte a internet, cuja forma como são utilizados determinará se as informações que através deles circulam se integram no âmbito do sigilo, visto que admitem uma utilização mista, individual e dirigida a destinatários determinados, ou dirigida a uma



TRIBUNAL CONSTITUCIONAL

329
X

pluralidade de destinatários com maior ou menor grau de indeterminação. Assim, muitas das comunicações realizadas através das chamadas redes sociais não têm tutela constitucional porque não oferecem as condições de inviolabilidade necessárias para tal, ou em virtude de serem facilmente acessíveis a uma panóplia de utilizadores que não apenas os destinatários dessa informação".

7. Assim sendo, afigura-se-nos que a eventual apreensão de meros documentos armazenados em equipamentos ou sistemas informáticos, bem como a norma que a autorize, não se revelam violadoras do disposto no nº4, do artigo 34.º, da Constituição da República Portuguesa.

8. Na realidade, se a apreensão dos documentos abertos e divulgados armazenados em equipamentos ou sistemas informáticos não representa uma interferência das autoridades na correspondência, nas telecomunicações ou noutra meio de comunicação, então, conforme apurámos, a proteção do disposto no artigo 34.º, n.º 4, da Constituição, não a tem por objeto e, consequentemente, não se lhe aplica.

9. Por assim ser, também a salvaguardada exceção à proibição de toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, consubstanciada na possibilidade de previsão de casos constantes de lei em matéria processual criminal, se revela inaplicável, por desadequada, à situação vertente.

10. De igual forma, não constituindo os atos autorizativos da apreensão dos documentos armazenados em equipamentos ou sistemas informáticos, matéria da reserva jurisdicional, nada impede que os mesmos sejam autorizados por decisão da autoridade judiciária que não um juiz, ou seja, por decisão do Ministério Público, não havendo, assim, igualmente, qualquer violação do art.32º nº4 da Constituição.

11. Acresce que, no caso, a diligência dirigia-se às instalações de pessoas coletivas, logo, a equipamentos e sistemas informáticos áquelle pertencentes.

12. Ora, diuidas temos que as normas constitucionais que visam proteger a reserva da vida privada tenham o mesmo alcance de aplicação quando nos deparamos com sistemas informáticos instalados em computadores de pessoa coletiva.

13. Não se pode, genericamente, falar numa equiparação entre pessoas coletivas e pessoas singulares no que aos direitos fundamentais diz respeito.

Como se pode ler em comentário ao art.12º nº2 da CRP, Jorge Miranda : «Os direitos fundamentais e, em geral, todos os direitos são, primordialmente, direitos das pessoas singulares. No entanto, há também direitos institucionais e o nº2 acrescenta que as pessoas coletivas gozam dos direitos e estão sujeitas aos deveres compatíveis com a sua natureza.

Não se trata de uma equiparação, porque não pode confundir-se o caráter final da personalidade jurídica do homem e o caráter instrumental da personalidade jurídica coletiva (Vieira de Andrade, os direitos fundamentais, pág.119, chegando a considerar os direitos fundamentais das pessoas coletivas direitos por analogia e atípicos).

Trata-se, antes, de uma limitação: as pessoas coletivas só têm os direitos compatíveis com a sua natureza, ao passo que as pessoas singulares têm todos os direitos, salvo os especificamente concedidos apenas a pessoas coletivas ou a instituições (v.g., o direito de antena). E, como nota o Tribunal Constitucional, tem que reconhecer-se que, ainda quando certo direito fundamental seja compatível com essa natureza e, portanto, suscetível de titularidade colectiva» (hoc sensu) daí não se segue que a sua aplicabilidade nesse domínio se vá operar exatamente nos mesmos termos e com a mesma amplitude com que decorre relativamente às pessoas singulares (Acs. N.ºs 198/85, 539/97, 569/98, 174 e 518/00. *(sublinhados nossos)*).

14. Nesta linha, ainda que se admita que as pessoas coletivas gozam, nomeadamente, do direito ao sigilo do conteúdo da correspondência, a verdade é que, tal como salientado pelo Venerando Tribunal da Relação, também a especial natureza dos bens jurídicos que se tutelam na LcD gozam de tutela constitucional, designadamente, na alínea f) do artigo 81º da Constituição, no qual se estabelece como incumbência prioritária do Estado assegurar o funcionamento eficiente dos mercados, de modo a garantir a equilibrada concorrência entre as empresas, a contrariar as formas de organização monopolistas e a reprimir os abusos de posição dominante e outras práticas lesivas do interesse geral.

15. Pelo que se pode afirmar que o primeiro, interesse privado da pessoa coletiva, deverá ceder perante o segundo, claramente de interesse público.

330
8

TRIBUNAL CONSTITUCIONAL

16. Por fim, mas não menos relevante, ainda que se admitisse que, pese embora se tratasse de computadores profissionais, poderão estar em questão mensagens de conteúdo privado dos trabalhadores, a verdade é que não vem invocado que tivessem sido apreendidos documentos informáticos cujo conteúdo seja suscetível de revelar dados pessoais ou íntimos, que possam por em causa a privacidade do respetivo titular, caso em que teriam de ser apresentados ao JIC que ponderaria da sua junção aos autos.

17. Aliás, como salientam Germano Marques da Silva e Fernando Sá, alguma doutrina entende que, por exemplo, o email profissional, quando suscetível de ser conhecido ou manipulado pela entidade empregadora, não comunga da garantia constitucional do sigilo (Thomas Gross, *Die Schutzwirkung des Brief – Post – und Fernmeldegeheimnisses nach der Privatisierung der Post*, in JZ, 1999, pág.327).

18. Por força do acabado de explanar, e reiterando o já afirmado, entendemos que deverá o Tribunal Constitucional julgar não constitucional a interpretação dos artigos 18º, nº1, alíneas c) e d) e 20º nº1 do Regime Jurídico da Concorrência no sentido de admitir a apreensão de mensagens de correio eletrónico pela Autoridade da Concorrência, mediante autorização do Ministério Público, e sem intervenção de um juiz, negando, assim, provimento ao presente recurso.

Em face do explanado, negando provimento ao recurso, fará o Tribunal Constitucional a costumada JUSTIÇA”

A AdC, finalmente, respondeu à alegação concluindo nos seguintes termos:

“A. No âmbito do processo de contraordenação que correu termos na AdC sobre a ref.º interna PRC/2016/6, a AdC realizou as diligências de busca, exame e apreensão nas instalações da Somafel - entre outras empresas visadas - nos dias 12 a 14, 17 a 21 e 24.07.2017 (fls. 739 a 77 do processo na sua fase administrativa), no âmbito das quais foram apreendidos os elementos identificados nos respetivos autos, a fls. 770 a 777, onde se incluíram mensagens de correio eletrónico marcadas como lidas pelo seu destinatário.

B. As referidas diligências foram nos termos do n.º 2 do artigo 18.º e do artigo 21.º da Lei da Concorrência, autorizadas pelo Ministério Público (cf. fls. 140 a 162 e 247 a 249 do processo na fase organicamente administrativa).

C. Em sede de recurso de impugnação judicial da Decisão final da AdC, os ora Recorrentes (Paulo Serradas e Somafel) suscitaram, quer junto do TCRS, quer junto do TRL, a título de questão prévia, a nulidade da prova referente às mensagens de correio eletrónico apreendidas, tendo ambas as instâncias julgado improcedente o referido vício, confirmado a possibilidade da apreensão de correio eletrónico à luz do regime jurídico da concorrência e afastado a existência das inconstitucionalidades para tanto invocadas por ambos os Recorrentes.

D. A condenação dos dois foi também confirmada pelos dois Tribunais, ainda que com redução da sanção aplicada.

E. Nesta sede, pretendem os Recorrentes submeter à apreciação deste Tribunal as seguintes questões (embora Paulo Serradas as apresente por ordem distinta):

(i) Pretensa inconstitucionalidade da norma contida alínea c) do n.º 1 do artigo 18.º da Lei da Concorrência, quando interpretada no sentido de que é possível, em processo de contraordenação da concorrência, examinar recolher e apreender mensagens de correio eletrónico;

(ii) Pretensa inconstitucionalidade da norma contida na alínea c) do n.º 1 do artigo 18.º da Lei da Concorrência, quando interpretada no sentido de que o mesmo prevê a possibilidade de exame, recolha e/ou apreensão de mensagens de correio eletrónico "abertas" ou "lidas" em processo contraordenacional da concorrência;

(iii) Pretensa inconstitucionalidade da norma contida alínea c) do n.º 1 do artigo 18.º da Lei da Concorrência, quando interpretada no sentido de admitir o exame, recolha e apreensão de mensagens de correio eletrónico em processo de contraordenação da concorrência, sem despacho judicial prévio.

F. O caminho percorrido pelos Recorrentes na sua alegação arrima-se numa petição de princípio: a apreensão de mensagens de correio eletrónico, mesmo referente a pessoas coletivas - e quer estas se encontrem sinalizadas como lidas ou não lidas - é um exclusivo do processo penal não extensível ao processo contraordenacional,

331
R

TRIBUNAL CONSTITUCIONAL

razão pela qual uma interpretação da norma constante dos artigos 18.º a 21.º da Lei da Concorrência no sentido da admissibilidade da apreensão de mensagens de correio eletrónico é inconstitucional.

G. Adicionalmente, também na sua ótica, não estando no domínio penal, não será admissível que o direito comprima o direito à inviolabilidade do sigilo da correspondência ao arrepio da exigência de despacho judicial prévio prevista no domínio penal.

H. Desde já se adianta, contudo, que não se antevê que possa assistir razão aos Recorrentes nas inconstitucionalidades que arguem. As duas primeiras questões colocadas à apreciação deste Tribunal impõem resposta conexa, entendendo a AdC que a resposta dada à primeira questão consumirá a segunda. A terceira questão colocada à apreciação do Tribunal merece resposta autónoma.

Sobre a pretensa inconstitucionalidade da norma extraída dos artigos 18.º a 21.º da Lei da Concorrência, quando interpretada no sentido da admissibilidade da apreensão de mensagens de correio eletrónico

I. Importa apreciar a compatibilização da alínea c) do n.º 1 do artigo 18.º da Lei da Concorrência com o n.º 4 do artigo 34.º da CRP, desde logo, apurando-se o alcance e o âmbito subjetivo deste preceito da Lei Fundamental, que, acompanhada pelo Professor Doutor Vital Moreira, no parecer que este deu a propósito da transposição da Diretiva ECN+ (disponível para consulta pública), a AdC entende excluir - ou pelo menos exigir uma aplicação adaptada - a tutela da privacidade às pessoas coletivas; o núcleo do artigo 34.º da CRP reconduz-se à intimidade da vida privada, sem aplicação ao contexto da vida empresarial e da informação criada, produzida e veiculada entre empresas.

J. A própria jurisprudência deste Tribunal Constitucional e a doutrina nela citada que acolhem uma diferenciação ou graduação de proteção entre a esfera de intimidade da vida privada e a esfera de privacidade de uma pessoa coletiva. Veja-se, a este respeito, o Acórdão n.º 593/08, de 10.12.2008.

K. A pretensão do legislador subjacente a este preceito terá sido a de consagrar e proteger o direito fundamental à inviolabilidade do domicílio e da correspondência, ou seja, a prima facie, a liberdade de manter uma esfera de privacidade e sigilo livre de interferência e ingerência estatal, quer no que respeita ao domicílio, quer quanto à comunicação. Todavia, o direito à inviolabilidade das comunicações e da reserva da vida privada, previstos no n.º 4 do artigo 34.º e n.º 1 do artigo 26.º da CRP, não abrange as comunicações eletrónicas enviadas e recebidas no âmbito do correio eletrónico profissional de uma empresa ou dos seus representantes.

L. Tratando-se de direitos iminentemente pessoais, não podem, numa base de automaticidade e de uma pretensa desvergência lógica, ser extensíveis às pessoas coletivas, nomeadamente às empresas e às comunicações que são criadas e circuladas noquele contexto empresarial. O próprio n.º 2 do artigo 12.º da CRP estatui que as pessoas coletivas (só) gozam dos direitos compatíveis com a sua natureza.

M. Por outro lado, como sinalizou já este Tribunal Constitucional, ainda quando certo direito fundamental seja compatível com a natureza coletiva da pessoa, isso não significa que a sua aplicabilidade nesse domínio se vá operar exactamente nos mesmos termos e com a mesma amplitude que se verifica quanto às pessoas singulares. Este entendimento foi também já sufragado por outros Tribunais. Nesse sentido, veja-se o Acórdão do Tribunal Central Administrativo Sul, de 11.07.2019, proferido no processo n.º 1590/17.4BEPRT.

N. Ocorrendo a apreensão de mensagens de correio eletrónico em ambiente empresarial, como acontece nos presentes autos, não se verifica qualquer ofensa ao direito à inviolabilidade das comunicações, porquanto estamos no âmbito da esfera jurídica da pessoa coletiva e não das pessoas singulares que colaboram com aquela. Tais mensagens de correio eletrónico - independentemente de se encontrarem marcadas como lidas ou não lidas - não beneficiam, por isso, da tutela constitucional conferida pelo n.º 4 do artigo 34.º da CRP no momento da busca e da apreensão.

O. A par da posição expressamente tomada pelo Constitucionalista Vital Moreira no já referido parecer, a orientação recente do TRL vem propugnando entendimento idêntico. Vejam-se, nesse sentido, o Acórdão aqui recorrido, o Acórdão proferido no processo n.º 28999/18.3T8LSB.L1, em 26.09.2022) e o Acórdão produzido no âmbito do processo n.º 71/18.3YUSTR-M, em 25.02.2022. Semelhante entendimento já também havia sido cogitado pelo TCRS na Sentença proferida no processo n.º 225/15.4YUSTR-W (Juiz Mariana Gomes Machado), em 02.05.2022.

P. A jurisprudência produzida pelo TEDH a propósito do artigo 8.º da CEDH - alguma dela trazida à colação pela Somafel - não preclude o entendimento da exclusão ou, pelo menos de moldagem do escopo do n.º 4 do artigo 34.º relativamente às pessoas coletivas, especificamente no que diz respeito ao enforcement das regras da concorrência. O



TRIBUNAL CONSTITUCIONAL

332
R.

que aquele Tribunal vem entendido é que as pessoas coletivas podem beneficiar da tutela emergente do artigo 8.º, mas que essa tutela pode comportar exceções desde que previstas na lei e justificadas num quadro de um Estado Direito Democrático o que se afigura, precisamente, o caso.

Q. A concorrência é também um bem com assento constitucional e uma das incumbências prioritárias do Estado é, precisamente, "[a]ssegurar o funcionamento eficiente dos mercados, de modo a garantir a equilibrada concorrência entre as empresas, a contrariar as formas de organização monopolistas e a reprimir os abusos de posição dominante e outras práticas lesivas do interesse geral" (cf. alínea f) do artigo 81.º da CRP). Por seu turno, e já no plano infra-constitucional, as previsões específicas da Lei da Concorrência que autorizam a apreensão de correio eletrónico, já supra mencionadas, constituem lei especial relativamente ao RCCO e negam qualquer aplicação subsidiária ou remissão para a Lei do Cibercrime (isto tem entendido, de forma praticamente unânime, o próprio TRL).

R. Também no contexto do Direito da União Europeia, a Diretiva ECN+, que visa dotar as autoridades da concorrência dos Estados-Membros de poderes e competência para aplicarem a lei de forma mais eficaz e garantir o bom funcionamento do mercado interno, oferece um quadro claro sobre os poderes de investigação de correio eletrónico que os Estado-Membros deverão assegurar às respectivas autoridades nacionais da concorrência.

S. Neste sentido, veja-se que a convicção em torno da relevância e instrumentalidade da apreensão de correio eletrónico para a prossecução de infrações à concorrência é tal que, a nível europeu, a Diretiva ECN+ visa precisamente dotar as autoridades da concorrência dos Estados-Membros de poderes e competência para aplicarem a lei de forma mais eficaz as regras da concorrência e garantir o bom funcionamento do mercado interno, num ambiente digital cada vez mais complexo e desafiante. São particularmente reveladores, neste sede os Considerandos 6, 30, 32, 35 e 73, assim como os artigos 6.º e 32.º que, de forma inequívoca, permitem à Comissão Europeia e às autoridades nacionais da concorrência a apreensão de correio eletrónico independentemente este estar sinalizado como lido ou não lido.

T. As temáticas em apreciação devem ser analisadas à luz do primado do Direito da União Europeia - proclamado, entre outros, no conhecido Acórdão Costa c. Ene - cuja primazia perante a ordem constitucional interna apenas cederá, nos termos do n.º 4 do artigo 8 da CRP, em face de ameaça dos aspectos essenciais dos princípios fundamentais do Estado de Direito. A este propósito, veja-se o Acórdão deste Tribunal n.º 422/2020.

U. Importa igualmente observar os princípios da efetividade e da interpretação conforme ao direito da União Europeia, do disposto no n.º 6 do artigo 7.º e o n.º 4 do artigo 8.º da CRP e do primado do direito da União Europeia, a interpretação e correta aplicação das normas de direito da concorrência não podem desvirtuar nem comprometer a eficácia e a uniformidade do direito da concorrência da União Europeia, devendo ser interpretadas e aplicadas de forma coerente e conforme o direito da União. Tal princípio tem sido estabilizadamente reconhecido pelo TJUE. Nesse sentido vejam-se, designadamente, os casos Pfleiderer Courage and Crehan.

V. A visão preconizada pelos Recorrentes a propósito do alcance do n.º 4 do artigo 34.º da CRP representa uma interpretação absolutamente anacrónica dos poderes de investigação conferidos à Autoridade da Concorrência e opõe-se frontalmente ao propósito da Diretiva ECN+, de conferir às diversas autoridades da concorrência de cada Estado-Membro os poderes de investigação adequados aos desafios atuais do desenvolvimento digital, sob pena de sair frustrada a aplicação efetiva das regras da concorrência. Particularmente relevante a propósito do primado do Direito da União e da sua relevância na transposição da Diretiva ECN+, assumem-se o assumem-se o parecer do Professor Doutor Miguel Poiares Maduro, igualmente disponível para consulta pública consulta pública e o Acórdão proferido em 21.12.2020, pelo TRL, no âmbito do processo n.º 18/19.OYUSTR-D.

W. De resto, a própria Lei da Concorrência - n.º 2 do artigo 3.º da sua redação atual - reia firmar a necessidade de esta ser interpretada e aplicada de modo conforme ao Direito da União Europeia.

X. A primeira questão deverá ser respondida no sentido da inexistência de qualquer inconstitucionalidade contida na norma decorrente da alínea c) do n.º 1 do artigo 18.º da Lei da Concorrência, quando interpretada no sentido de que, no domínio contraordenacional da concorrência, é permitida a apreensão de correio eletrónico, independentemente de o mesmo se encontrar marcado como lido ou não lido.

Sobre a pretensa inconstitucionalidade da norma contida na alínea c) do n.º 1 do artigo 18.º da Lei da Concorrência, quando interpretada no sentido de que o mesmo prevê a possibilidade de examinar, recolher e/ou apreensão de mensagens de correio eletrónico "abertas" ou "lidas" em processo contraordenacional da concorrência

333
F

TRIBUNAL CONSTITUCIONAL

Y. Em todo o caso e endereçando-rios à apreciação da segunda questão: independentemente da delimitação e do âmbito subjetivo do n.º 4 do artigo 34.º da CRP que se sustentou na Secção precedente, o caso sub judice continuaria a não convocar a tutela emergente daquele artigo em razão de as mensagens de correio eletrónico apreendidas nos presentes autos estarem sinalizadas como abertas/ lidas e, nessa medida, não integrarem o conceito de correspondência aplicável apenas a mensagens ainda em circulação.

Z. Pese embora não se perfilhe, atualmente, semelhante entendimento, as primeiras decisões sobre a possibilidade de apreensão de correio eletrónico no regime jurídico da concorrência e a sua conformidade com o n.º 4 do artigo 34.º da CRP, proferidas quer pelo TCRS, quer pelo TRL, conchíram que o artigo 34.º da CRP apenas pretendia incluir o correio eletrónico fechado/por ler, pois só este convocaria a (especial) necessidade de proteção de correspondência.

AA. Embora, reitere-se, não nos pareça, presentemente, o critério mais rigoroso, particularmente à luz da Diretiva ECN+, da nova Lei da Concorrência que a transpõe e do próprio Acordão n.º 687/21 deste Tribunal - ainda que proferido num contexto distinto a verdade é que, no caso sub judice, a AdC só pesquisou e apreendeu mensagens de correio eletrónico lidas, razão pela qual, mesmo não se perfilando o entendimento que a privacidade salvaguardada pelo n.º 4 do artigo 34.º da Constituição sofre as suas limitações em contexto empresarial, cabe justificar por que razão a interpretação feita pela AdC (e pelas duas instâncias judiciais de recurso) da alínea c) do n.º 1 do artigo 18.º não padece de nenhuma inconstitucionalidade.

BB. De acordo com a jurisprudência que perfilha semelhante entendimento, o que é salvaguardado pelo n.º 4 do artigo 34.º da CRP é a privacidade em sentido formal, ou seja, a interação e o processo comunicativo (ou o ato comunicativo em si) ao invés do objeto da comunicação, isto é, do seu conteúdo. É no processo dinâmico de transmissão da informação estabelecido desde o momento em que a correspondência é fechada e circula até ao momento em que é aberta pelo seu destinatário que vigora a vontade de a manter confidencial. A partir do momento em que o correio é lido e armazenado no computador, deixa de subsistir a vontade de o tornar confidencial e privado da curiosidade alheia, passando a valer como um mero documento, desprotegido de tutela constitucional.

CC. O domínio da ingerência nas telecomunicações ou outros meios de comunicação diz respeito a uma realidade dinâmica, que está "em trânsito", "em circulação", "em transmissão", de um emissor para um receptor, remetendo, na prática, para casos de interceção e gravação de comunicações telefónicas, apreensão de cartas em trânsito, ou, caso seja possível, a recolha e apreensão de uma mensagem de correio eletrónico no decurso da transmissão via rede do emissário para o destinatário. Coisa diferente é o objeto ou produto dessa mesma comunicação, o qual, para o que interessa no caso concreto, é merecedor de um tratamento equivalente a "documento", porquanto a proteção conferida pelo artigo 34.º da CRP não deve ser extensível à situação em análise.

DD. Propugnando por semelhante destriña para afastar a tutela do n.º 4 do artigo 34.º da CRP, vejam-se os Acordãos do TRL proferidos no âmbito do processo n.º 71/18.3YUSTR-D.L2 (04.03.2020), no âmbito do processo n.º 744/09-1 S5LSB-A.L1-9 e no processo n.º 229/18.5YUSTR-L2, assim como as Sentenças do TCRS nos processos n.º 71/18.3YUSTR-I, de 23.09.2019 e n.º 159/10.3.YUSTR (apêndices A e B), de 03.10.2019.

EE. Este entendimento tem sido igualmente partilhado por parte da doutrina produzida em contexto criminal (mas cujo entendimento conceptual é extensível ao regime jurídico da concorrência). Vejam-se as posições de Santos Cabral, Conde Correia, Fernando Gama Lobo, Pedro Verdelho e Manuel Costa Andrade.

FF. Em face do exposto - mas sem prejuízo da posição tomada supra a propósito da exclusão da tutela do n.º 4 do artigo 34.º quanto à apreensão de correio eletrónico em meio empresarial, independentemente de este se encontrar lido ou não lido, também a segunda questão deverá ser apreciada no sentido de inexistir qualquer inconstitucionalidade da norma contida da alínea c) do n.º 1 do artigo 18.º da Lei da Concorrência, quando interpretada no sentido de permitir a apreensão de mensagens de correio eletrónico sinalizadas como abertas / lidas.

Sobre a pretensa inconstitucionalidade da norma extraída dos artigos 18º a 21.º da Lei da Concorrência, quando interpretada no sentido da admissibilidade de as buscas e apreensões de mensagens de correio eletrónico poderem ser simplesmente autorizadas pelo ministério público

GG. O facto de a Lei da Concorrência prever, como condição sine qua non à busca e apreensão de correio eletrónico, in casu aberto e lido, uma prévia decisão de autorização fundamentada pelo Ministério Público transparece uma



TRIBUNAL CONSTITUCIONAL

334
K.

predeterminação normativa que exprime uma repartição de competências entre a autoridade judiciária e a autoridade administrativa e, bem assim, um equilíbrio sistémico entre poderes.

HII. É ao Ministério Público que cabe assegurar a proporcionalidade da medida, apreciando previamente a sua adequação à finalidade da diligência, a sua necessidade ou indispensabilidade (cf. n.º 2 do artigo 18.º e artigo 21.º da Lei n.º 19/2012), balizando a atuação da AdC.

II. Já essa apreciação caberá ao JJC, de acordo com a lei, caso estejam em causa (i) buscas domiciliárias; (ii) buscas em escritório de advogado; (iii) buscas em consultório médico e (iv) apreensão, em bancos e outras instituições de crédito, documentos abrangidos pelo sigilo bancário (cf. n.ºs 1 e 7 do artigo 19.º e no n.º 6 do artigo 20.º da Lei n.º 19/2012).

JJ. Da leitura do precedimento legal decorre que o próprio legislador já efetuou uma ponderação em torno da legalidade da medida, da sua natureza coerciva e da afetação que dela resulta para os direitos fundamentais da empresa visada, subordinando a atuação da AdC à prévia decisão do Ministério Público ou do JJC consoante a medida em causa.

KK. O facto de a busca e apreensão de correio eletrónico, in casu aberto e lido, estarem dependentes de autorização prévia do Ministério Público não garante uma proteção menor aos direitos, liberdades e garantias da empresa visada.

LL. O Ministério Público assume-se como uma autoridade judiciária independente, garante da legalidade democrática e da realização da justiça (cf. n.º 1 do artigo 219.º da CRP), externa e imparcial, sem interesse direto ou confundível com o da AdC na investigação da prática anticoncorrencial. Não é o Ministério Público que dirige o inquérito em processo contraordenacional da concorrência, ou que o conforma. Não é o Ministério Público que investiga, que acusa, mas a AdC. Não é o Ministério Público o requerente da medida de autorização da diligência de busca, exame e apreensão de correio eletrónico, neste caso aberto e lido, mas a AdC.

MM. A pergunta que se impõe responder é a de saber se o mandado emitido pelo Ministério Público, nesta sede, viola o princípio constitucional de reserva de juiz, constitucionalmente plasmado, designadamente no artigo 202.º e no n.º 4 do artigo 32.º da CRP. Tendo-se já debatido sobre este princípio, o Tribunal Constitucional aponta, como a sua razão de ser, ou razão para justificar a intervenção prévia do JJC, uma conexão entre uma situação de grave afetação ou ingerência em direitos fundamentais e a necessidade de uma tutela jurisdicional para esse efeito.

NN. Quanto às diligências de busca propriamente ditas, estas são necessariamente coercivas, e logo lesivas da esfera da empresa. Quanto à diliggência específica em discussão no presente processo da apreensão de correio eletrónico aberto e lido, também esta será lesiva pela sua própria natureza, mas não constitui uma ingerência intolerável no direito fundamental da empresa à inviolabilidade do sigilo de correspondência nos termos do n.º 1 do artigo 34.º da CRP, não tendo de ser acarretada nos termos do seu n.º 4, mediante despacho judicial prévio.

OO. Em rigor, o que é afetado pela diligência prevista na alínea c) do n.º 1 do artigo 18.º é o direito da empresa à privacidade ou à propriedade da documentação apreendida, não à privacidade da correspondência. O que é apreendido não é correspondência, mas documentação (in casu correio eletrónico aberto e lido), razão pela qual não está em causa um direito constitucionalmente tutelado nos termos do n.º 1 do artigo 34.º da CRP que tenha de ser acarretado nos termos do seu n.º 4.

PP. Perguntar-nos-emos, ainda assim, se está em causa uma ingerência que impõe a reserva de juiz a um nível garantístico, nos termos do n.º 4 do artigo 32.º da CRP. Contudo, trata-se de uma norma apenas projetada e dirigida ao processo penal. No âmbito do direito contraordenacional, a CRP não prevê um modelo quanto à entidade que assegura direitos, liberdades e garantias no processo contraordenacional, não estabelecendo, para esse efeito, qualquer divisão entre Ministério Público e JJC.

QQ. Por esse motivo, a repartição de competências prevista no artigo 21.º da Lei da Concorrência (quer na redação conferida pela Lei n.º 19/2012, quer na redação recente conferida pela Lei n.º 17/2022), e a opção legislativa pelo mandado do Ministério Público enquanto título habilitante à diligência de busca e apreensão de correio eletrónico não obedece a um modelo constitucionalmente garantístico, mas não quer dizer que não seja suficientemente idónea para o efeito.

RR. O prévio escrutínio da diligência por parte de uma autoridade judiciária constitucionalmente configurada como garante da legalidade e da realização da justiça assegura (i) a proteção da esfera privada contra intromissões abusivas e arbitrárias resultantes do exercício de poderes públicos; (ii) garante a proporcionalidade da diligência; (iii) delimita a ação da AdC, evitando que esta modele a diligência segundo os seus próprios juízos de oportunidade e conveniência e (iv) não se opõe ao exercício de contraditório por parte da empresa visada, objeto da diligência.



TRIBUNAL CONSTITUCIONAL

SS. Com efeito, a empresa pode escrutinar o mandado emitido pelo Ministério Público e o despacho de fundamentação que o acompanha ora reclamando para o seu superior hierárquico, ora impugnando judicialmente a execução do mandado junto da AdC, com recurso para o TCRS e para o TRL e ainda, através de recurso de impugnação judicial de uma decisão final, nos termos do artigo 87.º da Lei da Concorrência, onde o TCRS e o TRL conhecem de qualquer invalidade, ao abrigo dos seus poderes de pleno controlo jurisdicional (artigo 88.º da Lei da Concorrência).

TT. É certo que a empresa objeto de busca e apreensão nos termos da alínea c) do n.º 1 do artigo 18.º da Lei n.º 19/2012 não goza de qualquer contraditório prévio à diligência - sendo, no entanto, incontornável que uma diligência necessariamente coerciva não possa depender da disponibilidade ou do exercício de contraditório prévio da empresa visada, sobretudo quando sobre esta recai um dever de colaboração sob pena de obstaculizar a eficácia da diligência e a utilidade do processo sancionatório e incorrer numa denegação desse dever e na obstrução do exercício dos poderes da Autoridade, em violação da própria Lei da Concorrência (cf. alínea j) do n.º 1 do artigo 68.º) e da CRP (cf. n.º 2 do artigo 266.º).

UU. Não quer isto dizer que a tutela do possível não esteja assegurada, ou que o facto de a diligência depender de autorização e fundamentação do Ministério Público, e não de intervenção judicial do JIC, ofenda o n.º 4 do artigo 32.º da CRP por não acantelar a intervenção preventiva de um terceiro imparcial, o JIC, capaz de acantelar os direitos dos visados, compensando a falta de contraditório anterior.

VV. É que a ação do Ministério Público em sede de processo contraordenacional de concorrência não se confunde, nem formal, orgânica ou legalmente, com a posição que este assume em processo penal. Em rigor, no direito sancionatório da concorrência, o Ministério Público goza de competência própria atribuída pela lei, e, nessa qualidade, age como um terceiro imparcial e neutro à investigação, exercendo funções de controlo materialmente homólogas àquelas exercidas pelo JIC em processo penal no que respeita à proporcionalidade das medidas restritivas de direitos fundamentais. Neste caso, cabe ao Ministério Público assegurar a adequação, necessidade e imprescindibilidade da medida.

WW. Aqui chegados, não se vislumbra qualquer ofensa dos preceitos constitucionais - a conjugação dos enunciados normativos previstos na alínea c) do n.º 1 e n.º 2 do artigo 18.º, n.º 1 do artigo 20.º e artigo 21.º da Lei n.º 19/2012 não violam a CRP. Não há qualquer violação do princípio constitucional de reserva de juiz.

XX. A ausência de despacho judicial prévio não ofende o n.º 4 do artigo 32.º da CRP, porquanto esta norma não é extensível ao processo contraordenacional, nem pode ser interpretada enquanto tal, à revelia da configuração constitucional do Ministério Público prevista no artigo 219.º da CRP e das competências próprias que lhe foram conferidos pelo legislador no quadro sancionatório da concorrência.

YY. É o facto de a diligência prevista na alínea c) do n.º 1 do artigo 18.º ser precedida por uma autoridade judicidária (na qual se enquadra o Ministério Público) que confere a AdC um contexto de legalidade e proporcionalidade que delimitam a sua ação.

ZZ. Aqui chegados, restam evidentes as diferenças da estrutura do processo contraordenacional da concorrência para o processo penal que afastam um subsídio útil relativamente ao Acórdão deste Tribunal n.º 687/21. No primeiro, a entidade que investiga, acusa e instrui o processo (a AdC) não é a mesma a quem caberá autorizar as diligências de busca, exame e apreensão - função reservada ao Ministério Público e, em alguns casos particulares, ao próprio juiz de Instrução Criminal.

AAA. Esta separação orgânica, funcional e material de entidades acantela assim a necessidade de isenção, neutralidade e imparcialidade exigidas, mesmo pelo crito do referido Acórdão de fiscalização preventiva - improcedendo, por essa razão, o argumentário dos Recorrentes a este respeito.

BBB. Assim, deverá a terceira questão colocada pelos Recorrentes ser decidida pela inexistência de qualquer inconstitucionalidade da norma contida na alínea c) do n.º 1 do artigo 18.º no sentido de admitir o exame, recolha e apreensão de mensagens de correio eletrónico em processo contraordenacional da concorrência, autorizadas pelo Ministério Público e devidamente salvaguardadas as concretas situações previstas na Lei da Concorrência em que se exige autorização prévia do Juiz de Instrução Criminal.

Nestes termos e nos demais de Direito, deverão ser julgadas improcedentes as três questões de inconstitucionalidade suscitadas pelos Recorrentes.”



TRIBUNAL CONSTITUCIONAL

336
L.

Cumpre apreciar e decidir.

*

II. Fundamentação

6. Na redação que importa ao caso *sub iudicio* (a conferida pela Lei n.º 19/2012, de 08 de maio), as normas que importam ao objeto do presente recurso possuem o teor que seguidamente se indica, assinalando a ***bold*** o segmento compreendido no pedido de fiscalização:

“Artigo 18.”

Poderes de inquirição, busca e apreensão

1 - No exercício de poderes sancionatórios, a Autoridade da Concorrência, através dos seus órgãos ou funcionários, pode, designadamente:

- a) Interrogar a empresa e demais pessoas envolvidas, pessoalmente ou através de representante legal, bem como solicitar-lhes documentos e outros elementos de informação que entenda convenientes ou necessários para o esclarecimento dos factos;*
- b) Inquirir qualquer outras pessoas, pessoalmente ou através de representantes legais, cujas declarações considere pertinentes, bem como solicitar-lhes documentos e outros elementos de informação;*
- c) Proceder, nas instalações, terrenos ou meios de transporte de empresas ou de associações de empresas, à busca, exame, recolha e apreensão de extratos da escrita e demais documentação, independentemente do seu suporte, sempre que tais diligências se mostrem necessárias à obtenção de prova;*
- d) Proceder à selagem dos locais das instalações de empresas e de associações de empresas em que se encontrem ou sejam suscetíveis de se encontrar elementos da escrita ou demais documentação, bem como dos respetivos suportes, incluindo computadores e outros equipamentos electrónicos de armazenamento de dados, durante o período e na medida estritamente necessária à realização das diligências a que se refere a alínea anterior;*
- e) Requerer a quaisquer serviços da Administração Pública, incluindo as entidades policiais, a colaboração que se mostrar necessária ao cabal desempenho das suas funções.*

2 - As diligências previstas nas alíneas c) e d) do número anterior dependem de decisão da autoridade judiciária competente.

3 - A autorização referida no número anterior é solicitada previamente pela Autoridade da Concorrência, em requerimento fundamentado, devendo o despacho ser preferido no prazo de 48 horas.

4 - Os funcionários que, no exterior, procedam às diligências previstas nas alíneas a) a c) do n.º 1 devem ser portadores:

- a) Nos casos das alíneas a) e b), de credencial emitida pela Autoridade da Concorrência, da qual constará a finalidade da diligência;*
- b) Nos casos da alínea c), da credencial referida na alínea anterior e do despacho previsto no n.º 3, que é, nesse momento, notificado ao visado.*

5 - A notificação a que refere a alínea b) do número anterior é realizada na pessoa do representante legal ou, na ausência do mesmo, na de qualquer colaborador da empresa ou associação de empresas que se encontre presente.

6 - Na realização das diligências previstas nas alíneas c) e d) do n.º 1, a Autoridade da Concorrência pode fazer-se acompanhar das entidades policiais.



TRIBUNAL CONSTITUCIONAL

332
5

7 - Não se encontrando nas instalações o representante legal do visado, trabalhadores ou outros colaboradores, ou havendo recusa da notificação, a mesma é efetuada mediante fixação de duplicado do termo da diligência em local visível das instalações.

8 - Das diligências previstas nas alíneas a) a d) do n.º 1 é elaborado auto, que é notificado aos visados.

9 - A falta de comparecência das pessoas convocadas a prestar declarações junto da Autoridade da Concorrência não obsta a que os processos sigam os seus termos."

No presente recurso suscitam-se três questões de constitucionalidade, relativas a outras tantas dimensões normativas do artigo 18.º, n.º 1, alínea c), do RJdC. O pedido comprehende a fiscalização deste preceito quando interpretado no sentido de: (i) conferir poderes a AdC para proceder ao exame, recolha e apreensão de mensagens de correio eletrónico *no âmbito de processo por contraordenação*; (ii) conferir poderes a AdC para realizar exame, recolha e apreensão de mensagens de correio eletrónico *assinaladas como «abertas» ou «lidas»*; (iii) conferir poderes a AdC para realizar o exame, recolha e apreensão de mensagens de correio eletrónico *sem necessidade de autorização judicial, bastando a concedida pelo Ministério Público* (enquanto autoridade judiciária).

Para além de o fraseamento adotado pelos recorrentes ser muito semelhante, está bom de ver que os pedidos e respetivas temáticas sobrepõem-se entre si. Por outro lado, a segunda questão definida está comprehendida nas outras duas, constituindo apenas uma especialidade que se explica pela *ratio decidendi* da decisão recorrida e da busca e apreensão que se questionava na causa principal. Assim, ser-nos-á permitido, estamos em crer, agrupar todo o objeto do processo numa mesma formulação que nos permita uma avaliação conjunta e unitária de todas as matérias colocadas.

Assim, é de concluir que conforma objeto dos recursos interpostos por ambos os recorrentes a fiscalização do disposto no artigo 18.º, n.º 1, alínea c), do RJdC, quando interpretado no sentido de *permitir a Autoridade da Concorrência, em processo contraordenacional, o exame, recolha e apreensão de mensagens de correio eletrónico assinaladas no sistema informático como «abertas» ou «lidas», sem necessidade de autorização judicial prévia, bastando a que tenha sido concedida pelo Ministério Público*.

Colocada que está a controvérsia, passemos à apreciação de mérito.

8. A Jurisprudência constitucional sobre a Norma fiscalizada

8.1. O Tribunal Constitucional procedeu já a fiscalização do disposto no artigo 18.º, n.º 1, alínea c), do RJdC (Acórdãos do TC n.ºs 91/2023 e 314/2023, que remete para o primeiro), tendo



TRIBUNAL CONSTITUCIONAL

338
T

concluído pela sua inconstitucionalidade material por violação dos artigos 34.º, n.ºs 1 e 4 e 32.º, n.º 4, ambos da Constituição da República Portuguesa, quando interpretado no sentido de que “*se admite o escame, recolha e apreensão de mensagens de correio eletrónico em processo de contraordenação da concorrência, desde que autorizado pelo Ministério Público, não sendo necessário despacho judicial prévio*”.

O Acórdão do TC n.º 91/2023 que inaugurou esta jurisprudência realiza uma análise exaustiva dos parâmetros constitucionais em causa e convoca abundante doutrina e jurisprudência constitucional sobre a matéria. Com uma (importante) exceção, que assinalaremos já de seguida, não dissidimos sobre a forma como aí se comprehende a tutela de comunicações conferida pelo artigo 34.º, n.ºs 1 e 4, da Lei Fundamental e inherente necessidade de autorização jurisdicional para atos de autoridades públicas que conformem ingerências nesse espaço de proteção (artigo 32.º, n.º 4, da Constituição da República Portuguesa). Nesse pressuposto e tendo em vista enquadrar o tema, podemos iniciar o nosso percurso chamando à colação o aí exposto a este propósito:

“O Tribunal Constitucional dispõe de um considerável acervo jurisprudencial sobre o sentido e alcance do n.º 4 do artigo 34.º que comprehende, como adiante melhor se verá, ambas as vertentes do preceito.

15.1. Em primeiro lugar, resulta dessa jurisprudência que a proteção das comunicações entre pessoas dispõe de assento constitucional próprio, nos termos do disposto nos n.ºs 1 e 4 do artigo 34.º da Lei Fundamental. Como se afirmou no Acórdão n.º 241/2002, «[i]ndependentemente da questão de saber se o sigilo das telecomunicações se inscreve sempre, numa relação de especialidade, com a tutela da vida privada (sendo embora seguro que o direito a tal sigilo garante o direito à reserva da intimidade da vida privada) certo é que aquele tem na Constituição um tratamento específico», que deriva do regime consagrado em matéria de inviolabilidade da correspondência e dos outros meios de comunicação privada. Quer isto dizer que, não obstante o direito à inviolabilidade das comunicações constituir uma regra de outros direitos constitucionalmente tutelados (como o direito à reserva da intimidade da vida privada), a Constituição autonómiza a proteção de uma esfera de privacidade e de sigilo no domínio específico das comunicações interpessoais, associando-lhe uma garantia constitucional autónoma face àquela que já decorreria do n.º 1 do artigo 26.º da Constituição. Criou, assim, «um regime especial de tutela do direito à reserva da intimidade da vida privada» (Germano Marques da Silva e Fernando Sá, “Anotação ao artigo 34.”, Constituição Portuguesa Anotada, Tomo I, 2.ª Edição, org. Jorge Miranda e Rui Medeiros, Coimbra Editora, 2010, p. 756), que abrange as comunicações eletrónicas.

O conceito de telecomunicações o termo utilizado no n.º 4 do artigo 34.º — refere-se a uma realidade mais ampla do que as tradicionais escutas telefónicas, que integra indubbiamente o correio eletrónico. Este entendimento, seguido nos Acórdãos n.ºs 486/2009, 403/2015, 420/2017 e 464/2019, foi recentemente explicitado no Acórdão n.º 687/2021 da seguinte forma:

«A proteção constitucional conferida à correspondência privada compreende todas as variantes de correspondência entre indivíduos, desde as formas tradicionais de correspondência postal — cartas, postais, telegramas — até ao correio eletrónico, entendido como tráfego de informação privada, sob a forma escrita, figurativa ou equivalente, entre destinatários definidos e apenas acessível por estes, transmitido através de um suporte de internet. Tutela equivalente é conferida, para efeitos de aplicação do n.º 4 do artigo 34.º, às telecomunicações, envolvendo telefonemas, mensagens de voz, conversas por via de VoIP e similares, bem como, em geral, a quaisquer formas de comunicação humana, de caráter privado. Efectivamente, a diversidade



339

X

TRIBUNAL CONSTITUCIONAL

*das formas de transmissão da informação privada e dos respetivos suportes não justifica uma diferença de tutela juridical, na medida em que esta visa garantir, do ponto de vista material, a possibilidade de comunicação privada, enquanto regra do interesse individual na reserva de intimidade da vida privada». A tutela especialmente conferida pelos n.ºs 1 e 4 do artigo 34.º da Constituição visa, pois, garantir a confiança nas comunicações em sentido objetivo, independentemente do caráter sigiloso ou não sigiloso da mensagem: ao assegurar-se a confidencialidade das comunicações, qualquer que seja o conteúdo das informações transmitidas, protege-se a liberdade da própria pessoa, garantindo-lhe o direito de comunicar com segurança, sem restrições, censuras ou ingerências (cfr. Ana Rita Castanheira Neves, *As ingerências nas comunicações electrónicas em processo penal*, Coimbra Editora, 2011, p. 52). No fundo, as telecomunicações, a correspondência e as comunicações electrónicas materializam uma específica situação de perigo, que se caracteriza pelo facto de a mensagem se encontrar exposta às incidências do circuito ou sistema de transmissão, no qual remetente e destinatário são obrigados a confiar, independentemente de ser ou não privado o conteúdo da missiva. É essa a razão pela qual a Constituição tutela a inviolabilidade das comunicações: garante a todos quantos carecem de um terceiro para comunicar — trate-se de um serviço de correio, de um operador de telecomunicações ou de um fornecedor de serviços de correio eletrónico ou de mensagens instantâneas, que a confiança que nele depositam não poderá ser gorada através de intrusões alheias no processo comunicativo (cfr. Costa Andrade, «Bruscamente no verão passado», a reforma do Código de Processo Penal — Observações críticas sobre uma lei que podia e devia ter sido diferente», Revista de Legislação e Jurisprudência, Ano 137, n.º 3951, p. 340).*

15.2. Da jurisprudência do Tribunal em matéria de garantia da inviolabilidade das telecomunicações decorre também que a proteção conferida pelos n.ºs 1 e 4 do artigo 34.º da Constituição não abrange apenas o conteúdo das comunicações, estendendo-se ainda aos dados gerados a seu propósito — designadamente aos chamados dados de tráfego. Como se sublinhou no Acórdão n.º 403/2015:

O acesso aos dados das comunicações efetivamente realizadas ou tentadas põe em causa direitos fundamentais das pessoas envolvidas no ato comunicacional. E não é apenas a invasão ou intrusão no conteúdo informacional veiculado pelos meios de transmissão (dados de conteúdo), que os afetam, mas também as circunstâncias em que a comunicação foi realizada (dados de tráfego).

Com efeito, mesmo que não haja acesso ao conteúdo, a interconexão entre dados de tráfego pode fornecer um perfil complexo e completo da pessoa em questão — com quem mais conversa, que lugares frequenta, quais os seus horários, etc. A verdade é que, como refere Costa Andrade, «no seu conjunto, os dados segregados pela comunicação e pelo sistema de telecomunicações se revelam, muitas vezes, mais significativos que o próprio conteúdo da comunicação em si. O que, de resto, bem espelha o interesse com que, reconhecidamente, a investigação criminal procura maximizar a recolha de dados ou circunstâncias da comunicação, também referenciados como dados de tráfego» (cfr. «Bruscamente no verão passado — A Reforma do Código de Processo Penal», Revista de Legislação e Jurisprudência, Ano 137, julho-agosto 2008, pág. 338).

Deste modo, ao proibir a ingerência das autoridades públicas fora das condições previstas no segmento final do n.º 4 do artigo 34.º, a Constituição veda o acesso a uma comunicação privada quer quanto ao conteúdo da mensagem, quer quanto aos elementos funcionais da comunicação, designadamente direção, destinatários, data, via e percurso de uma determinada mensagem — os chamados “dados de tráfego” (Acórdão n.º 687/2021). Quer isto dizer que se incluem no âmbito da proteção constitucional «todos os meios de comunicação individual e privada, e toda a espécie de correspondência entre pessoas, em suporte físico ou eletrónico, incluindo não apenas o conteúdo da correspondência, mas o tráfego como tal (espécie, hora, duração, intensidade de utilização), excluindo-se apenas a categoria residual de dados pessoais, isolados de qualquer processo de comunicação, efetivo ou tentado» (Acórdão n.º 464/2019).”

O problema com que o Tribunal se debateu, logo de seguida, consistia em saber *qual o momento* em que uma mensagem de correio eletrónico poderia deixar de ser entendida «comunicação», perdendo esta forma especial de tutela e tendo em vista delimitar a respetiva cobertura



TRIBUNAL CONSTITUCIONAL

3400
R

constitucional. A justificação para o reforço na proteção, como se vem de expor, reside na *especial vulnerabilidade* decorrente do *trânsito* da mensagem, já que, perdendo autor e destinatário o seu controlo durante o percurso entre autor e destinatário, emerge um risco específico de apropriação por terceiros ou de extração do seu conteúdo, vulnerabilizando a proteção da privacidade, dissuadindo a utilização de meios de telecomunicação e promovendo o isolamento do Ser humano.

Assim e por necessária deriva, quando uma mensagem *deixa de estar em trânsito*, ou seja, quando não se ache sob domínio de terceiro encarregue da sua entrega ao destinatário (sinalizando a especial situação de vulneração do conteúdo e da personalidade dos intervenientes), a proteção constitucional do artigo 34.º, n.ºs 1 e 4, da Constituição da República Portuguesa não se colocará.

O Acórdão do TC n.º 91/2023 começa por debater este problema enunciando o tratamento doutrinário sobre a questão análoga colocada quanto ao correio postal:

“No domínio da correspondência postal, vem sendo entendido que a proteção especialmente conferida pelos n.ºs 1 e 4 do artigo 34.º da Constituição apenas é aplicável até ao momento de abertura da carta, o mesmo é dizer, enquanto esta se mantém em trânsito. A tutela consiste na proteção da informação em trânsito ou em circulação, cessando a partir do momento em que a mensagem é recebida pelo destinatário por então terminar a realidade dinâmica da comunicação. A partir daí, a mensagem é equiparada a qualquer outro documento, deixando de gozar da tutela constitucional da inviolabilidade das comunicações.”

São essencialmente duas as razões que suportam este entendimento.

Por um lado, tem-se em conta a específica situação de perigo em que a mensagem se encontra durante o processo de comunicação, altura em que o emissário e o destinatário não têm controlo sobre ela. Se a [a] tutela jurídica da inviolabilidade das telecomunicações radica [...] na “específica situação de perigo” decorrente do domínio que o terceiro detém — e enquanto o detém — sobre a comunicação (conteúdo e dados) e que lhe confere «a possibilidade factiva de intromissão arbitrária, subtraída ao controlo dos comunicador(es)» (Manuel da Costa Andrade, “Bruscamente...”, cit., n.º 3951, p. 338), então ela bá de cessar com a chegada mensagem ao destinatário, por nesse momento fundar a situação de vulnerabilidade que caracteriza a transmissão da mensagem (a sua colocação no poder de um terceiro, o operador), passando o destinatário a dispor de todos os meios para evitar a intromissão (arquivando-a, guardando-a ou mesmo destruindo-a).

Por outro lado, assume-se que correspondência suscetível de ser violada é apenas aquela que dispõe de uma proteção física exterior, que faz com que a mensagem se encontre fechada, tornando o respetivo conteúdo inacessível por terceiros; uma vez violado o envelope que protege fisicamente o conteúdo da mensagem, esta deixa de se encontrar coberta pelo sigilo, uma vez que passa a estar em condições de poder ser lida por terceiros — é essa, aliás, a razão pela qual se defende que os simples postais não se encontram abrangidos pela proteção decorrente dos n.ºs 1 e 4 do artigo 34.º da Constituição (cf. Germano Marques da Silva e Fernando Sé, “Anotação ao artigo 34.º”, Constituição Portuguesa Anotada, Tomo I, 2.ª edição, Coimbra Editora, 2010, p. 772).”

Transitando para o sistema de correio eletrónico em debate, o Tribunal enfrentou então a distinção, comcurso jurisprudencial e doutrinário, entre mensagens de webmail *abertas* e *fechadas*, termos que se reportam a certa forma de etiquetagem de mensagens generalizada nos programas e

341
L

TRIBUNAL CONSTITUCIONAL

aplicações de correio eletrónico. Tendo em vista facilitar a organização do arquivo de webmail pelo utilizador, é habitual que o interface exponha a listagem de mensagens da conta sinalizando por alguma forma de grafismo as que não foram ainda tratadas pelo utilizador. Em linguagem coloquial, as mensagens assinaladas são ditas «*abertas*» e as desprovidas do sinal gráfico dizem-se «*fechadas*».

Idealizando um paralelismo com o correio postal e tendo por base o presumível acesso à mensagem pelo destinatário que o grafismo assinala, alguma jurisprudência veio entendendo que as mensagens *abertas* se encontrariam na situação de uma *carta desenvolvida*, que é dizer, de um escrito-mensagem cujo *círculo de comunicação* se concluiu e que, como tal, não beneficia da proteção conferida pelo artigo 34.º, n.ºs 1 e 4, da Constituição da República Portuguesa, reduzindo-se à natureza de *documento*. É também numa conceção semelhante do problema que assentou o juízo de não-inconstitucionalidade sobre a norma fiscalizada alcançado pelo Tribunal “*a quo*” (associando-lhe ainda o caráter coletivo da pessoa jurídica titular da informação contida nas mensagens).

O Acórdão do TC n.º 91/2023, alinhando com a doutrina e jurisprudência mais recentes (Acórdão do TC n.º 687/2021), não encontrou mérito nesta parametrização da questão colocada:

“impõe-se começar por verificar se o facto de «a busca e apreensão de mensagens de correio eletrónico» ter por objeto «mensagens marcadas como abertas» coloca a norma sindicada fora do âmbito de incidência da proibição constante do n.º 4 do artigo 34.º. Não sendo disputável a possibilidade de apreensão de elementos de prova em suporte eletrónico — trata-se, em face do movimento de digitalização e desmaterialização característico das sociedades contemporâneas, de uma realidade material omnipresente na vida comunitária» (Acórdão n.º 687/2021) —, importa concretamente perceber se as mensagens de correio eletrónico, ao encontrarem-se marcadas como abertas, se convertem ou tornam equiparáveis a simples documentos e, por via disso, passam a poder ser submetidas às condições em que a busca e apreensão destes pode ter lugar; ou, pelo contrário, continuam a beneficiar da tutela inerente à proteção da correspondência, telecomunicações e outros meios de comunicação entre pessoas, assegurada pelos n.ºs 1 e 4 do artigo 34.º da Constituição.

Ainda que não seja decisiva, a resposta que se dé num ou outro sentido, também não é isenta de consequências. É que, caso se conclua, como fez o Tribunal recorrido, que as mensagens de correio eletrónico, uma vez abertas e lidas, deixam de ser consideradas «correspondência», que apenas se refere à «comunicação que está em trânsito», e por isso não gozam da tutela constitucional fornecida pelo art. 34.º da Constituição da República Portuguesa, o acesso por autoridades públicas não se encontrará mais circunscrito aos termos da exceção contemplada no segmento final do n.º 4 do referido artigo 34.º, embora as normas que previjam esse acesso fiquem sujeitas à observância das condições em que podem ser restringidos outros direitos fundamentais — como sejam os direitos à privacidade e à autodeterminação informativa, protegidos pelo artigo 26.º da Constituição —, designadamente aos limites fixados no artigo 18.º, n.º 2, às leis restritivas de direitos, liberdades e garantias. (...)

18.1. A decisão recorrida transpõe para o correio eletrónico a conceção defendida para a correspondência postal, concluindo que a proteção constitucional da inviolabilidade das comunicações vigora até ao momento da abertura da mensagem pelo destinatário, al terminando o processo comunicativo. O que releva para este efeito não é o facto de a mensagem permanecer disponível na caixa de correio do destinatário, mas sim a sua chegada efetiva ao domínio deste:

342
T.

TRIBUNAL CONSTITUCIONAL

quando a mensagem está a aguardar ser lida na caixa de correio do destinatário, ela está ainda em trânsito, o que deixa de verificar-se após a respetiva abertura.

*A favor desta posição, que faz cessar a especial proteção constitucional do correio eletrónico no momento em que as mensagens são abertas pelo destinatário, depois, como vimos, o argumento segundo o qual, uma vez recebida a mensagem, funda a especial situação de perigo decorrente do domínio do terceiro sobre a missiva, deixando a mesma de constituir um meio de comunicação. Uma vez sob controlo do destinatário — que pode optar por arquivar o seu conteúdo, protegê-lo com sistemas de segurança (codificação criptica, firewalls, etc.) ou destruí-lo —, a mensagem passa a ser somente um documento informático, cuja reserva é protegida por outras normas da Constituição. O critério da posse do objeto da comunicação é, assim, determinante para se dar por terminado o processo comunicativo e, com isso, a especial garantia de inviolabilidade conferida pelos n.ºs 1 e 4 do artigo 34.º da Constituição: a mensagem eletrónica chegada ao destinatário não beneficia de proteção maior do que aquela que gozam as cartas em papel recebidas e guardadas numa gaveta ou num cofre, uma vez que, «depois de recebido, lido e guardado no computador do destinatário, um e-mail deixa de pertencer à área de tutela das telecomunicações, passando a valer como um normal escrito. E, como tal, sujeito ao mesmo regime em que se encontra um qualquer ficheiro produzido pelo utilizador do computador e nele arquivado. Podendo, como tal, figurar como objeto idóneo da busca, em sentido tradicional» (Manuel da Costa Andrade, «Bruscam...», cit., n.º 3951, p. 338; no mesmo sentido, Ana Rita Castanheira Naves, *As ingerências...*, pp. 263-265).*

Este entendimento vem sendo, contudo, crescentemente posto em causa, ainda que com apoio em pontos de vista diversos.

*Com efeito, opõem-se-lhe não apenas aqueles que defendem que o correio eletrónico, em si mesmo, constitui uma realidade diversa da correspondência escrita, devendo ser para todos os efeitos encarado como mero documento em suporte informático (cf. Rogério Bravo, «Da não equiparação do correio eletrónico ao conceito tradicional de correspondência por carta», *Polícia e Justiça*, n.º 7, 2006, p. 209), como aqueles que, no polo oposto, consideram que as mensagens de correio eletrónico constituem sempre comunicações, mesmo depois de lidas — posição que parece, aliás, subjacente à opção do legislador processual penal em sujeitar as «conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio eletrónico» ao regime das escutas telefónicas, ainda que «guardadas em suporte digital» (artigos 187.º e 189.º do Código de Processo Penal) — ou mesmo que o correio eletrónico é insuscetível de assimilar a distinção entre aberto e não aberto, demandando por essa razão o estabelecimento de um outro critério para a determinação do momento em que a mensagem deixa de poder ser vista como comunicação (Gonçalo Anastácio e Diana Alfaos, «Auotação ao artigo 20.º», *Lei da Concorrência — Comentário Coimbricense*, 2.ª edição, Almedina, 2017, p. 342; Paulo Pinto de Albuquerque, *Comentário do Regime Geral das Contraordenações à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, Universidade Católica, 2011, p. 159; Rui Cardoso, «Apreensão de correio eletrónico e registos de comunicações de natureza semelhante — artigo 17.º da Lei n.º 109/2009, de 15.IX», *Revista do Ministério Público*, n.º 158, 2018, p. 177).*

Desta tendência den particular nota o Acórdão n.º 687/2021 no trecho que se segue:

*Assim, tem-se caminhado em direção a uma disciplina tendencialmente unitária da apreensão de correio eletrónico em processo penal, permitindo enfrentar as questões levantadas por tal realidade, levando em consideração os bens jurídico-constitucionalmente tutelados que a propósito dela devem ser convocados (como a privacidade, o sigilo da correspondência, a autodeterminação informativa, a proteção conferida aos dados pessoais e aos dados informáticos), e contribuindo para ultrapassar os desencontros provocados pelo «enquadramento categorial e normativo dos e-mails nas fases e ao tempo em que se encontram guardados no e-mail account do provider: tanto na fase intermédia, em que a mensagem não foi ainda chamada nem aberta ou lida pelo destinatário; como na fase final, nas constelações em que, depois de aberto e lido, o e-mail é depositado no server do provider, a que só é possível aceder através da internet, isto é, através de um ato de telecomunicação» (M. COSTA ANDRADE, «Comentário ao artigo 194.º do Código Penal», in *Comentário Coimbricense do Código Penal*, Tomo I, 2.ª Edição, Coimbra Editora, maio de 2012, ponto 28). Efetivamente, a verdade é que é, hoje, possível «com um simples clique, marcar como lida uma mensagem de correio eletrónico não lida e vice-versa. O sujeito pode aceder ao correio eletrónico através de*

3493
C

TRIBUNAL CONSTITUCIONAL

vários dispositivos e em uns deles a mensagem surgir como lida e outros como não lida, dependendo do tipo de sincronização existente entre os diversos dispositivos. A fronteira entre correio eletrónico lido e não lido é, assim, difícil de estabelecer. O legislador, reconhecendo o anacronismo e a inadequação daquela distinção de regimes, optou por atribuir uma tutela acrescida à mensagem em formato digital, submetendo-a ao regime do artigo 17.º, independentemente de ter ou não sido lida pelo seu destinatário” (SÓNIA FIDALGO, “A apreensão de correio eletrónico e a utilização noutro processo das mensagens apreendidas”, in Revista Portuguesa de Ciência Criminal, Ano 29, n.º 1, janeiro-abril de 2019, GestLegal, p. 69).

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

Dai que, no arresto citado, o Tribunal não tenha feito qualquer distinção entre correio eletrónico marcado como aberto ou fechado, colocando a possibilidade de apreensão de um e de outro na dependência da verificação dos mesmos pressupostos ou condições, à face do que dispõem os «artigos 26.º, n.º 1, 34.º, n.º 1, 35.º, n.ºs 1 e 4, 32.º, n.º 4, e 18.º, n.º 2, da Constituição».

18.2. Tal entendimento é de manter aqui.

No domínio do correio eletrónico, a marcação de certa mensagem como aberta constitui um evento imprestável para determinar o fim da sua natureza de comunicação — e, em consequência, a paralisação da proteção especialmente concedida pelo artigo 34.º da Constituição —, devendo entender-se que a garantia constitucional de inviolabilidade das comunicações abrange as mensagens de correio eletrónico enquanto permanecerem na caixa (virtual) de correio eletrónico, independentemente da circunstância, contingencial e aleatória, de a mensagem ostentar o estado de “aberta” ou de “fechada”.

Pelo menos duas razões apontam claramente nesse sentido.

Em primeiro lugar, verifica-se que o principal argumento invocado para justificar a cessação da tutela constitucional da correspondência postal no momento em que esta é aberta — a eliminação da barreira física que protege o conteúdo comunicado até ao momento da abertura da carta — não tem pura e simplesmente aplicação no âmbito das mensagens eletrónicas. Daí que se sustente que «uma mensagem de “correio-eletrónico” nunca é, nem nunca está “fechada”» (Rogério Bravo, “Da não equiparação...”, cit., p. 212), já que nunca é «envelopável» (idem, p. 214). No correio eletrónico, a abertura e leitura do conteúdo da mensagem encontra-se, em ambos os casos, dependente do mesmo exato gesto (a seleção e abertura, à distância do mesmo clique digital); e a violação dessa barreira física é exteriormente indecidível, porquanto depois de lida bastará marcar a mensagem como “não lida” (Rui Cardoso, “Apreensão...”, cit., 2018, p. 187), caso em que, a ser este o critério relevante, se “reativaría” a tutela constitucional especialmente conferida às comunicações.

Em segundo lugar — e como decorre do ficou dito —, a distinção entre mensagens abertas e fechadas é, no caso do correio eletrónico, artificial e fátilvel. Artificial, porque o destinatário pode marcar, livremente, as mensagens como abertas ou fechadas, mediante a seleção de uma simples opção no computador; independentemente de ter lido ou não a mensagem, está na sua total disponibilidade classificá-la como não lida ou como lida. Fátilvel, porque nada garante que uma mensagem marcada como aberta tenha já esgotado a sua natureza de comunicação, tendo sido efectivamente lida. Essa marcação pode constituir apenas o resultado de uma passagem accidental do cursor sobre a mensagem; da activação de uma opção de sinalização de todas as mensagens que acabam de chegar; ou, tendo em conta que o sujeito pode aceder à caixa de correio eletrónico através de diferentes dispositivos (telefones, computadores, relógios, tablets), até mesmo do facto de o utilizador ter simplesmente aberto a aplicação num dos equipamentos, podendo acontecer que a mesma mensagem esteja sinalizada como lida em alguns deles e como não lida nos outros. Ao contrário do que sucede com a correspondência postal — que não é aberta sem consciência clara do ato de abertura —, uma mensagem de correio eletrónico pode ficar marcada como aberta sem que o utilizador disso se aperceba e sem que daí se possa inferir uma chegada efectiva à esfera de posse do destinatário. Nessa medida, nega-se hoje a validade (técnica e jurídica) da dissocição entre correio eletrónico lido e não lido, duvidando-se mesmo, pelo menos em alguns casos, da possibilidade de a estabelecer (Sónia Fidalgo, “A apreensão de correio eletrónico e a utilização noutro processo das mensagens apreendidas”, Revista Portuguesa de Ciência Criminal, Ano 29, n.º 1, 2019, p. 69; Gonçalo Anastácio



TRIBUNAL CONSTITUCIONAL

e Diana Alfaosar, cit. p. 342; Rui Cardoso, "A apreensão de correio eletrónico após o Acórdão do Tribunal Constitucional n.º 687/2021: do juiz das liberdades ao juiz purificador investigador?", Revista Portuguesa de Direito Constitucional, n.º 1, 2021, p. 149, nota n.º 8; David Silva RAMALHO, Métodos ocultos de investigação criminal em ambiente digital, Almedina, 2017, p. 279).

Este conjunto de objeções à possibilidade de distinção entre correio eletrónico lido e não lido tem, do ponto de vista da proteção especialmente concedida pelos n.ºs 1 e 4 do artigo 34.º da Constituição, plena razão de ser.¹⁹

Concluindo pelo caráter insatisfatório desta classificação, o arresto desenvolve depois outro paradigma de localização do momento em que a mensagem de webmail deixa de possuir a natureza de comunicação, por essa via conferindo uma outra geometria à proteção do correio eletrônico.

O Acórdão do TC n.º 91/2023 veio a concluir que, em mensagens de email, a especial situação de perigo que fundamenta a tutela prevista no artigo 34.º, n.ºs 1 e 4, da Lei Fundamental “apenas cessa quando o destinatário retira a mensagem da caixa de correio eletrônico virtual e a arquiva em outro lugar do computador” (Acórdão do TC n.º 91/2023). Enquanto ali se encontrar, prossegue o arresto, a mensagem acha-se ainda sob domínio do *email account provider* e, sendo assim, é indiferente que esteja assinalada como *lida* (aberta) ou *não lida* (fechada): trata-se ainda de uma fase de transmissão de informação sob controlo de terceiro, por isso subsumível à noção de telecomunicação.

Convocando o Acórdão do TC n.º 687/2021, acrescenta-se também que o simples acesso à «caixa virtual» por oficiais públicos importa, supostamente, a aquisição de certas informações relativas às mensagens assinaladas como não-lidas, referentes às circunstâncias em que foram elaboradas e atributos dos dados nelas contidas, que, se não constituem o conteúdo transmitido, beneficiam também da proteção constitucional conferida às telecomunicações (“*a simples visualização de uma "caixa de correio eletrônico", sem que sequer se abra cada uma das mensagens individuais ali gravadas, pode permitir o conhecimento não apenas de elementos respeitantes à concreta comunicação ou mensagem (como, por exemplo, o "assunto"), como também de elementos relativos ao emissor e destinatário das mensagens*”).

Também por este motivo, diz-se, apenas o êxodo de uma mensagem da *caixa de correio eletrônico virtual* por ação do utilizador a desproverá da proteção conferida pelo artigo 34.º, n.º 4, da Constituição da República Portuguesa: o “*critério decisivo de que a mensagem chegou definitivamente ao destinatário não será, por conseguinte, a marcação da mensagem como lida, mas sim o seu arquivamento definitivo, fora da caixa de correio eletrônico virtual*” (Acórdão do TC n.º 91/2023, sublinhado nosso):

“Se o fundamento subjacente à cessação da tutela constitucional das comunicações tem que ver com a possibilidade de o destinatário, uma vez lida a mensagem, poder adotar e desenvolver a proteção que entender — inclusivamente



TRIBUNAL CONSTITUCIONAL

destruindo-a —, a circunstância de uma mensagem estar marcada como «lida» constitui um elemento de fraco préstimo para suportar a conclusão de que aquela chegou efectivamente ao destinatário e de que este pode protegê-la. Diferentemente do que sucede na correspondência postal ou com as mensagens SMS que já foram lidas pelo destinatário, não pode afirmar-se que o processo de comunicação (a especial situação de perigo) cessou pela primeira abertura do correio eletrónico ou que o destinatário se encontra com total domínio sobre a mensagem. Enquanto a mensagem se mantiver na caixa de correio — sem ser definitivamente armazenada em qualquer lugar do computador do destinatário e eliminada dos servidores do provider —, ela está sob controlo do fornecedor de serviços eletrónico. Sendo certo que na maioria dos protocolos de correio eletrónico (IMAP, webmail), de cada vez que o interessado pretender ler a mensagem, estabelece-se uma comunicação eletrónica, podendo mesmo o acesso ao conteúdo dos dados fornecidos pelo servidor constituir uma comunicação restrita (e, nesse sentido, privada), pelo facto de a mensagem só poder ser acedida mediante introdução de dados de identificação (nome de utilizador e palavra passe). E mesmo que o utilizador faça uso de um protocolo que descarrega a mensagem do servidor (v.g., POP3), ela é copiada para o computador do destinatário, passando a estar simultaneamente no servidor do fornecedor e no equipamento do indivíduo (Rui Cardoso, "Apreensão...", cit., 2018, p. 181). Nessa medida, dúvidas não há de que se mantém — ainda que a mensagem tenha já sido lida — a situação de «domínio que o terceiro detém — e enquanto o detém sobre a comunicação (conteúdo e dados). Domínio que lhe assegura a possibilidade fáctica de intromissão arbitrária, subtraída ao controlo dos comunicador(es)» (cfr. Manuel da Costa Andrade, "«Bruscamente...», cit., n.º 3951, p. 339). A autotutela que se assume sobrevir quando uma mensagem chega ao seu destinatário («o destinatário passa a dispor de meios de autotutela, desde a instalação de sistemas de segurança, programas antivírus, codificação criptica, firewalls [programas que vigiam o tráfego na internet e avisam o titular do computador das tentativas de envio de programas do género "cavalo de troia"] até ao apagamento ou destruição, pura e simples, dos dados» — idem, p. 340) não existe enquanto a mensagem estiver na caixa de correio eletrónico e o fornecedor de correio eletrónico mantiver controlo sobre a mensagem. Esta «específica situação de perigo» apenas cessa quando o destinatário retira a mensagem da caixa de correio eletrónico virtual e a arquiva em outro lugar do computador — passando, só então, a ter o controlo total e exclusivo sobre ela, deixando de ter de confiar no sistema de comunicações e podendo protegê-la como entender. Confiança essa que, como se viu, é o âmago da tutela especialmente conferida pelo artigo 34.º da Constituição: quem comunica à distância carece da «medição necessária de terceiro, isto é, de um fornecedor de serviços de comunicação à distância», o que supõe um «procedimento em que, como precisa o Tribunal Constitucional Federal (22.8.2006), vai envolvida uma "perda de privacidade" (Verlust an Privatheit), uma vez que quem comunica tem de fazê-lo submetendo-se às especificidades e exigências daquele sistema de comunicação e confiar nele, para não dizer confiar-se a ele» (ibidem, p. 338). E se a proteção suplementar das comunicações radica na necessidade de confiança no terceiro que assegura o processo comunicativo, isso bá de implicar que sobre o utilizador não recaia o ônus de apagar diariamente as mensagens sob domínio do provider (ou de as marcar como "não lidas") para poder beneficiar da inviolabilidade do sistema. É esta, em suma, a razão pela qual, no caso do correio eletrónico, a proteção constitucional do direito à inviolabilidade das comunicações não abrange apenas as mensagens ainda não lidas («o conhecimento do destinatário pressupõe da parte deste um gesto necessário de "chamada" da mensagem, gesto que desencadeia um ato de telecomunicação [do provider para o destinatário]»), estendendo-se ainda às mensagens já abertas — os «e-mails que continuam (e enquanto continuam) no domínio — e, por causa disso, expostos à intromissão arbitrária — do provider» (cfr. ibidem, p. 342). O critério decisivo de que a mensagem chegou definitivamente ao destinatário não será, por conseguinte, a marcação da mensagem como lida, mas sim o seu arquivamento definitivo, fora da caixa de correio eletrónico virtual.

18.3. Em benefício da recondução das mensagens de correio eletrónico sinalizadas como abertas ao âmbito de incidência da proibição que se extrai dos n.ºs 1 e 4 do artigo 34.º da Constituição, uma terceira razão pode ser ainda invocada. É que, ainda que fosse possível operar com um critério baseado na distinção mensagens lidas e não lidas, certo continuaria a ser que o acesso a uma caixa de correio eletrónico em que se mantenham mensagens abertas envolve necessariamente a intromissão em comunicações indiscutivelmente abrangidas pelo direito à inviolabilidade das comunicações. Com efeito, tendo-se concluído que a proteção constitucional das comunicações abrange os dados de tráfego, é bom de ver que a admissibilidade de consulta de uma caixa de correio eletrónico — que contenha algumas



TRIBUNAL CONSTITUCIONAL

mensagens abertas e outras por abrir — revela um conjunto de informações das mensagens fechadas necessariamente abrangido pelo disposto no artigo 34.º da Constituição.

Como se concluiu no Acórdão n.º 687/2021:

«Efectivamente, a simples visualização de uma «caixa de correio eletrónico», sem que sequer se abra cada uma das mensagens individuais aí gravadas, pode permitir o conhecimento não apenas de elementos respeitantes à concreta comunicação ou mensagem (como, por exemplo, o “assunto”), como também de elementos relativos ao emissor e destinatário das mensagens, número de interações comunicativas, suas data e hora, volume de dados transmitidos, ou IP de origem, que se configuram como dados de tráfego. Ou seja, se no caso de apreensão de correspondência postal passa a ser do conhecimento das autoridades o remetente, o destinatário e a data do carimbo de correio, no caso do correio eletrónico a informação de tráfego disponivel é bastante mais vasta, sendo possível saber, por exemplo, a data e hora específicas a que um e-mail foi enviado, se continha, ou não, documentos anexos, se se dirigia a mais destinatários (e quais) e se constituiu resposta a ou reencaminhamento de mensagens anteriores.»

Diferentemente do que sucede na correspondência postal não lida (em que a única informação exterior é o carimbo do correio e, porventura, a indicação do remetente), as mensagens de correio eletrónico — mesmo antes de lidas e abertas — revelam um conjunto de informações mais amplo e sensível, compreendendo especialmente o se, o quando, o como, entre que pessoas ou entre que aparelhos a comunicação teve lugar ou foi tentada (Manuel da Costa Audruze, “Bruscamente...”, cit., n.º 3951, p. 340). Nessa medida, uma norma que atribua à AdC o poder de acceder a uma caixa de correio eletrónico para busca de mensagens já abertas tem sempre como resultado facultar-lhe o acesso a dados relativos a mensagens não abertas e não lidas (comunicações, indiscrimivelmente), o que sempre alivaria a tutela especialmente conferida pelos n.os 1 e 4 do artigo 34.º da Constituição, ainda que aquelas não estivessem tuteladas, como efectivamente estão, pelo regime relativo à inviolabilidade das comunicações ali estabelecido.”

Em suma, para esta jurisprudência, todas as mensagens que se encontram na «caixa de correio eletrónico virtual» e que não hajam sido previamente transferidas para «outro local do computador» beneficiam da tutela próprias às telecomunicações, que é dizer, a sua apreensão ficará sujeita a reserva de processo criminal (artigo 34.º, n.º 4, da Constituição da República Portuguesa) e sob o amplo leque de garantias decorrente desse estatuto, incluindo a necessidade de autorização por juiz para efetivação do ato de ingerência (artigo 32.º, n.º 4, da Constituição da República Portuguesa).

8.2. O Tribunal Constitucional, no citado Acórdão n.º 91/2023, embateu de imediato com uma dificuldade indissociável da doutrina que afirmava, esta respeitante ao facto de ações dirigidas à obtenção como meio de prova de mensagens de correio eletrónico nas descritas condições ficarem circunscritas ao processo criminal (cfr. artigo 34.º, n.º 4, parte final, da Constituição da República Portuguesa). Tendo por base este entendimento, desde que o utilizador omitisse a descrita deslocação da mensagem da «caixa de correio eletrónico virtual» para “outro local do seu computador”, a invulnerabilidade do acervo de mensagens de webmail cederia apenas para o ambiente processual-penal, resistindo a qualquer outra iniciativa pública de aquisição como elemento probatório.



347
R

TRIBUNAL CONSTITUCIONAL

Ora, porque, no ordenamento português, todas as infrações contra a concorrência estão catalogadas como *contraordenações* e porque a fase de investigação e aquisição de prova ocorre sob titularidade da Autoridade da Concorrência (Adc), assim sem a natureza de processo jurisdicional, a doutrina adotada no Acórdão n.º 91/2023 equivaleria à *exclusão absoluta* de registos de mensagens de webmail como meio de prova nas descritas condições, como não permitiria qualquer quadro legal destinado a viabilizar a sua recolha para prova no âmbito de infrações contra o Direito da concorrência. Isto, acrescentamos nós, e como veremos, em contexto em que o acesso direto e o gozo da informação estão garantidos ao titular da conta de webmail pelas funcionalidades que lhe são conferidas pelo programa informático no que respeita a todas as mensagens na «*caixa de correio eletrónico virtual*», sem necessidade de prévio «*arquivamento definitivo em outro lugar do computador*».

Esta observação é tanto mais grave quando as infrações à concorrência envolvem, com frequência, práticas de cooperação ou de coordenação (ilícita) entre empresas tendo em vista enviesar mecanismos de mercado (pelo menos, as mais graves: concertação de preços, distribuição de mercados, limitação da oferta, concertação de licitações em concursos públicos: artigo 9.º, n.º 1, alíneas a) a c), do RJdc). A ser assim, a respetiva prova será pouco menos que impossível sem acesso ao histórico de comunicações entre representantes de agentes económicos que caracterizam (e executam) essas práticas. Ao tempo atual, em que a troca de informação é realizada, na sua quase totalidade e particularmente em contexto empresarial, através de meios digitais, será *incontornável* que as autoridades possam utilizar como prova os documentos que resultam desses fluxos de comunicação e que disponham de meios de obtenção de prova adequados para o seu apossamento, única forma de *reconstruir* e de comprovar *acordos e concertações de práticas* lesivas da concorrência.

A jurisprudência do Acórdão do TC n.º 91/2023, em oposição, facultaria a qualquer agente económico a possibilidade de erguer uma muralha impenetrável sobre o seu acervo de mensagens eletrónicas (que considera *eterna e permanente «em trânsito»* enquanto permanecerem na «*caixa de correio eletrónico virtual*»), sem com isso importar qualquer forma de limitação relevante no acesso do titular ao seu arquivo de histórico e sem diminuir a aptidão que lhe está conferida de sobre ela realizar todos os atos de gestão característicos do domínio. Ficaria assim criado, diríamos, algo como uma «*offshore de informação*», um espaço onde esta permanece inalcançável às autoridades públicas, sem com isso se prejudicar o pleno gozo em território nacional de todas utilidades que confere ao seu titular e de desempenho da respetiva aptidão para toda a constelação conjecturável de atos ilícitos.



348
R

TRIBUNAL CONSTITUCIONAL

A conciliação entre a forma adotada de observar a proteção constitucional das mensagens de webmail e a praticabilidade das investigações por infrações à concorrência foi encontrada pela reformulação do âmbito da *reserva de processo penal* às intrusões em telecomunicações, como agora passaremos a ver.

8.3. O Tribunal Constitucional veio a entender no Acórdão n.º 91/2023 que a exceção à regra de inviolabilidade das comunicações estabelecida na parte final do artigo 34.º, n.º 4, da Constituição da República Portuguesa (“*salvo os casos previstos na lei em matéria de processo criminal*”) compreendia, não apenas os processos criminais (ou seja, os procedimentos judiciais instaurados para investigação e julgamento de um facto catalogado na Lei como crime), como quaisquer outras fórmulas processuais dirigidas a desempenhar a função de tutela de um bem jurídico passível de tutela penal, ainda que desprovido de norma incriminatória prévia. Explica-se no aresto:

“Partindo da premissa segundo a qual os preceitos constitucionais devem ser interpretados à luz da própria Constituição, enquanto unidade dotada de uma coerência a ciência intrínseca, tal posição sustenta que os «fins e interesses», «direitos ou valores» para a salvaguarda dos quais é concedida ao legislador autorização para restringir o direito à inviolabilidade das comunicações «em matéria de processo criminal» são aqueles que a própria ordem constitucional consente que sejam inseridos nesse específico âmbito ou domínio da regulação. O conteúdo positivo da exceção à proibição de ingerência nos dados de comunicação constante do inciso final do n.º 4 do artigo 34.º é recortado assim, não a partir do conceito formal de crime — segundo o qual crime será tudo, mas só aquilo que o legislador considerar como tal (Jorge de Figueiredo Dias, *Direito Penal, Parte Geral, Tomo I*, Coimbra, GestLegal, 2019, p. 121) —, mas a partir do conceito material de crime — aquele que a ordem a ciência jurídico-constitucional integra e reflete —, essencialmente constituído pela noção de bem jurídico, enquanto «valor jurídico-constitucionalmente reconhecido em nome do sistema social total» (idem, p. 136).

Partindo desta premissa, à questão de saber «o que é exatamente «materia de processual criminal» respondeu-se nessa declaração da seguinte forma:

«É todo o domínio da regulação que participe da natureza própria do «direito penal total», cuja propriedade essencial é a função específica de proteção dos bens fundamentais da vida em comunidade organizada, através da prevenção de lesões futuras e da repressão de lesões passadas.

Nos casos de tutela retroativa, a defesa dos bens fundamentais da comunidade — precisamente aqueles que a Constituição consagra e incumbe o Estado de proteger — encontra o seu arquétipo de concretização no âmbito do processo criminal: é através da instauração de um processo que se determina se foi praticado determinado crime e quem foi o seu autor, e, em caso afirmativo, se decide qual a pena que a este deverá ser aplicada de modo a assegurar a reafirmação contrafáctica da validade e vigência da norma penal violada e, em última instância, a defesa da ordem constitucional.

Ora, é nesta particular e relevantíssima finalidade, desempenhada paradigmaticamente pelo processo penal, que reside a razão de ser da autorização excepcional de acesso a dados de comunicação prevista no segmento final do n.º 4 do artigo 34.º da Constituição: ao limitar os possíveis casos de ingerência à matéria de processo penal, a Constituição assegura que o acesso a dados de comunicação apenas poderá ser autorizado pelo legislador ordinário quando a medida que o concretiza participar da finalidade de defesa dos bens



TRIBUNAL CONSTITUCIONAL

fundamentais da comunidade, e se mantiver, por via disso, dentro do critério de valor que caracteriza e singulariza o domínio da vida que justifica tal restrição.”
É esta a posição que aqui se seguirá.”

Desenvolvendo esta noção, o Acórdão do TC n.º 91/2023 sinaliza a *concorrência* como valor jurídico-penal, que é dizer, como interesse normativo dotado de dignidade penal e passível de suportar uma iniciativa de criminalização contra as condutas dele lesivas. Observando depois que se inscreve na liberdade conferida ao Legislador optar entre a tipificação da lesão deste bem jurídico como crime e outros modelos sancionatórios (v. g. o Direito das contraordenações), conclui-se que, caso a escolha não recaia na criminalização (como, hoje e entre nós, sucede no que tange infrações ao Direito da concorrência), isso não poderá representar restrições constitucionais à prova em prejuízo da efetividade da proteção, precisamente por conta do valor máximo que lhe está conferido pela Lei Fundamental e tanto mais quando esta faculdade parlamentar possui larga medida de discricionariedade e é impassível de fiscalização. Explica ainda o Tribunal que, se não fosse assim, a importância do interesse normativo poderia conduzir a que o Legislador se visse obrigado a criminalizar certas condutas ainda que outras formas de tutela (menos intrusivas) se mostrassem aptas a assegurar a sua proteção (*desnecessidade de pena*), isto tendo em vista garantir nada mais que certos meios de prova (*comunicações*) pudesssem ser utilizados nos processos respetivos.

O arresto finaliza posicionando-se pela viabilidade de um modelo processual que capacitasse a AdC a proceder à apreensão e utilização como meio probatório de mensagens de correio eletrónico qualificáveis como comunicações para instrução de processos por infrações ao Direito da concorrência, ou seja, ainda que se encontrem na «*caixa de correio eletrónico virtual*» e não «*armazenadas noutra local do computador*» e se destinem a instruir processos contraordenacionais.

Apesar do exposto, a preterição de autorização por Juiz para a realização da diligência de apreensão de webmail que caracterizava, de forma essencial, a segunda dimensão normativa do artigo 18.º, n.º 1, alínea c), do RjdC (à semelhança da norma-objeto do caso *sub iudicio*) cuja fiscalização se realizava, levou a que esta fosse considerada materialmente inconstitucional.

“O direito da concorrência, nacional e europeu, destina-se a garantir a integridade do funcionamento dos mercados. As respetivas normas protegem os consumidores e as empresas de práticas comerciais concertadas que tenham por finalidade ou efeito impedir, restringir ou falsear o livre desenvolvimento dos mercados, assegurando aos primeiros reais possibilidades de escolha e franqueando às segundas o ingresso num circuito livre de «obstáculos» gerados por quem dela beneficia, de modo a permitir-lhes criar riqueza e emprego” (Considerando 1 da Diretiva ECN+).

350
K

TRIBUNAL CONSTITUCIONAL

Trata-se, assim, de um conjunto de normas que se inscrevem, por um lado, na incumbência prioritária do Estado fixada na alínea f) do artigo 81.º da Constituição, que o vincula a «[a]segurar o funcionamento eficiente dos mercados, de modo a garantir a equilibrada concorrência entre as empresas, a contrariar as formas de organização monopolistas e a reprimir os abusos de posição dominante e outras práticas lesivas do interesse geral, e se reconduzem, por outro, ao direito fundamental dos consumidores «à proteção [...] dos seus interesses económicos», consagrado no n.º 1 do artigo 60.º da Lei Fundamental, constituindo um dos principais eixos da tutela a estes constitucionalmente devida contra práticas comerciais manipuladoras e abusivas, designadamente aquelas que «mantêm os preços de produtos e serviços artificialmente elevados» (Considerando 1 da Diretiva ECN+).

Dispondo o bem jurídico tutelado pelo direito sancionatório da concorrência de inequívoco assento jurídico-constitucional — protegê-lo constitui mesmo, como vimos, um dever prioritário do Estado —, não há dúvida de que nos encontramos em matéria que a Constituição permite que o legislador situe no (ou aloque ao) domínio do direito penal, substantivo e adjetivo. Do ponto de vista da Constituição (...), o controlo do chamado «poder de mercado» constitui um valor da «máxima relevância jurídica» (expressão utilizada no Acórdão n.º 377/2015), cuja proteção o legislador se encontra por isso legitimado a prosseguir através da ameaça de sanções penais, que são «aquelas que em geral maiores sacrifícios impõem aos direitos fundamentais» (Acórdão n.º 99/2002). (...)

Contudo, é sabido também que a presença de um bem jurídico dotado de dignidade penal — no caso, o livre desenvolvimento dos mercados — constitui uma condição necessária, mas não uma condição suficiente para validar a decisão político-criminal que conduza a sancionar, não com coimas, mas com penas, os comportamentos suscetíveis de o lesar ou fazer perigar — aqui, as práticas restritivas da concorrência. Uma vez que, por força da natureza subsidiária ou de ultima ratio que o princípio da proibição do excesso também fixa no direito penal (artigo 18.º, n.º 2, da Constituição), este apenas poderá intervir, com «o arsenal das suas sanções específicas», «nos casos em que todos os outros meios da política social, em particular da política jurídica não penal, se revelem insuficientes ou inadequados» (Jorge de Figueiredo Dias, «Direito Penal»..., cit., p. 147), o sancionamento das práticas anticoncorrenciais através de medidas penais — e, consequentemente, no âmbito de um processo penal — está materialmente vinculado à comprovação de que, para além de em causa se encontrar a proteção de um direito ou interesse constitucionalmente relevante, essa proteção não pode ser suficiente e adequadamente garantida de outro modo. (...)

(...) uma leitura da autorização contida no segmento final do n.º 4 do artigo 34.º da Constituição que reserve a possibilidade de «busca e apreensão de mensagens de correio eletrónico abertas» à investigação ou produção de prova no âmbito de um processo penal pende de subverter dramaticamente os termos desta ponderação, sobretudo se não se perder de vista que, em matéria de criminalização, o Tribunal Constitucional só deve proceder à censura das opções legislativas quando o recurso a sanções penais se apresente manifestamente arbitrário ou excessivo (..., por todos, os Acórdãos n.ºs 643/1993, 99/2002, 494/2003). (...)

Já se se entender que o sentido da exceção contida no inciso final do n.º 4 do artigo 34.º da Constituição é o de autorizar o legislador a lançar mão de meios de obtenção de prova que impliquem a ingerência de autoridades públicas nas telecomunicações sempre que, mas apenas quando, o mecanismo de que concretamente se trate for adequado, necessário e proporcional à tutela de um bem da «máxima relevância jurídica» segundo a axiologia subjacente à própria ordem jurídico-constitucional, independentemente de essa tutela ocorrer através da ameaça de uma pena ou, por escrupuloso respeito ao princípio da subsidiariedade (o mesmo é dizer, ao princípio da proibição do excesso), mediante a intervenção da ordem sancionatória não privativa da liberdade representada pelo direito das contravenções, será possível ao legislador dotar a AdC de «meios para [aplicar] as regras de forma eficaz», evitando que «as práticas anticoncorrenciais [fiquem] impunes, porque [...] não se conseguem recolher elementos de prova de práticas anticoncorrenciais» (Considerando 6 da Diretiva), sem renunciar à função de ultima ratio que a Constituição fixa no direito penal.

Como é bom de ver, apenas esta compreensão do âmbito de incidência da exceção contida no segmento final do n.º 4 do artigo 34.º eliminará o risco de que a opção pela criminalização de determinado comportamento — no caso, as práticas restritivas da concorrência — se fique verdadeiramente a dever, não à necessidade da pena, mas à necessidade de assegurar o acesso a determinados meios de obtenção de prova, não disponíveis de outro modo e — o que é mais relevante ainda —, permitirá que a ordem jurídico-constitucional se realize por inteiro, enquanto sistema axiológico coerente e unitário, livre de aporias e de insanáveis contradições. (...)



TRIBUNAL CONSTITUCIONAL

351
T

[o] conceito de «instrução» constante do n.º 4 do artigo 32.º da Constituição compreende os atos destinados a instruir probatoriamente uma futura acusação que contendam diretamente com direitos fundamentais (Acórdão n.º 7/1987, n.º 2.4.) — o que, independentemente da natureza da sanção aplicável, converte o juiz de instrução na entidade exclusivamente competente para praticar, ordenar ou autorizar certos atos processuais singulares que, na sua pura objetividade externa, se traduzem em ataques a direitos, liberdades e garantias das pessoas constitucionalmente protegidas» (Jorge de Figueiredo Dias, «Sobre os sujeitos processuais no novo Código de Processo Penal», *O Novo Código de Processo Penal*, Almedina, Coimbra, 1988, p. 16) —, seja porque, ao prever-se da exceção à proibição da inviolabilidade das comunicações em matéria de processo penal prevista no n.º 4 do artigo 34.º da Constituição, o legislador se mantém vinculado ao princípio da proibição do excesso a que o n.º 2 do artigo 18.º sujeita as medidas restritivas de direitos, liberdades e garantias — o que inviabiliza a opção por um regime de acesso que não se encontre numa relação de justa medida com a posição do titular do direito atingido □, é inevitável concluir que, também em processo contraordenacional por prática restritiva da concorrência, a busca e apreensão de mensagens de correio eletrónico marcadas como abertas apenas será constitucionalmente viável se for, em regra, precedida da intervenção do juiz de instrução. Isto é, se for sujeita a um controlo judicial prévio, destinado a aferir, à semelhança do que ocorre com a realização de buscas domiciliárias, a gravidade da infração investigada, a relevância dos meios de prova procurados, o nível de indicação da participação da empresa ou associação de empresas envolvidas e a razabilidade da convicção de que a diligência pretendida é indispensável para a descoberta da verdade dos factos ou de que a prova tida em vista seria impossível ou muito difícil de obter por meios alternativos, menos intrusivos para os direitos do(s) visado(s).

É este o elemento que dita a incompatibilidade com a Constituição da solução globalmente alcançada pelo Tribunal recorrido. Não a circunstância de a busca e apreensão de mensagens de correio eletrónico abertas ocorrer no âmbito de um processo sancionatório por práticas restritivas da concorrência, mas o facto de ser realizada com dispensa das garantias inerentes ao modelo de autorização judicial privativa, o mesmo é dizer, sem que um juiz seja chamado a formular um julgo de ponderação suscetível de assegurar, no caso concreto, a adequação, necessidade e proporcionalidade daquele meio de obtenção de prova, tendo em conta a gravidade das práticas anticoncorrenciais indicadas, a consistência das razões invocadas para justificar a necessidade da ingerência nas mensagens de correio eletrónico marcadas com abertas e a indispensabilidade da diligência para a realização das finalidades que com ela se pretendem prosseguir.”

Posto isto, e tomado prioridade sobre todas as demais questões, importa avaliar o ponto mais inovador do arresto, respeitante a esta forma de observar a reserva de processo criminal contida no artigo 34.º, n.º 4, da Constituição da República Portuguesa. O Acórdão do TC n.º 91/2023, assumidamente, afastou a posição que vinha sendo adotada com contornos de unanimidade por doutrina e jurisprudência até aqui, impondo-se por isso tomar posição sobre essa matéria.

9. A Reserva de Processo criminal nas Ingerências em Telecomunicações

9.1. A jurisprudência e doutrina constitucionais sempre entenderam que o n.º 4, do artigo 34.º, da Constituição da República Portuguesa, estabelece uma proibição absoluta de ingerência nas telecomunicações fora do quadro jurídico-processual penal, entendido em sentido *formal e próprio*.



TRIBUNAL CONSTITUCIONAL

Isto significa que qualquer fórmula de intrusão em telecomunicações, designadamente por via de institutos destinados a obtenção de prova, só será admissível no interior da disciplina legal do *processo-crime*. É dizer, medidas legislativas que as autorizem terão de estar integradas na regulação do exercício de pretensão de Direito público de sancionamento por *crime* – entendido este como a infração como tal classificada por Lei prévia e vigente –, ficando sujeitas à inherente reserva parlamentar (artigo 165.º, n.º 1, alínea c), parte final, da Constituição da República Portuguesa) e em respeito pelo respectivo estatuto constitucional específico (artigo 32.º, n.ºs 1 a 9, da Constituição da República Portuguesa). Significa também que os atos que as materializem apenas poderão ter lugar no interior de processo jurisdicional formalizado ao abrigo dessa moldura legal adjetiva:

“Ao definir o campo de incidência da lei restritiva do direito à inviolabilidade das comunicações pela ‘máteria de processo criminal’ a Constituição ponderou a tomou posição (em parte) sobre o conflito entre os bens jurídicos protegidos por aquele direito fundamental e os valores comunitários, especialmente os da segurança, a cuja realização se dirige o processo penal. Não obstante as restrições legais ao direito à inviolabilidade das comunicações que o legislador está autorizado a estabelecer devorem obedecer à ponderação do princípio da proporcionalidade, a preferência abstrata pelo valor da segurança em prejuízo da privacidade das comunicações só pode valer em matéria de processo penal. É que a não inclusão de outras matérias do âmbito da restrição do direito à inviolabilidade das comunicações, não é contrária ao plano ordenador do sistema jurídicoconstitucional. Ainda que se pudesse considerar, em abstrato, que há outras matérias em que o valor da segurança sobreleva os valores próprios do direito à inviolabilidade das comunicações, a falta de cobertura normativa da restrição em matérias extraprocessuais não frustra as intenções ordenadoras do atual sistema, porque há razões político-jurídicas que estão na base da abstenção do legislador constitucional. (...) Nada autoriza, pois, a admitir uma eventual extensão do âmbito da ressalva final do n.º 4 do artigo 34.º - para a qual, aliás, o intérprete, neste contexto concreto, não dispõe de instrumentos metodológicos adequados.

De facto, a referência ao processo criminal não é apenas uma indicação teleológica, mas também a localização da restrição à proibição de ingérvia numa área estruturada normativamente em termos de oferecer garantias bastantes contra intrusões abusivas. Ao autorizar a ingérvia das autoridades públicas nos meios de comunicação apenas em matéria de processo penal, e não para quaisquer outros efeitos, a Constituição quis garantir que o acesso a esses meios, para salvaguarda dos valores da justiça e da «segurança», fosse efetuado através de um instrumento processual que também proteja os direitos fundamentais das pessoas. Porque a ingérvia nas comunicações põe em conflito um direito fundamental com outros direitos ou valores comunitários, considerou-se que a restrição daquele direito só seria autorizada para realização dos valores da justiça, da descoberta da verdade material e restabelecimento da paz jurídica comunitária, os valores que ao processo criminal incumbem realizar. Assim, remeteu para o legislador processual penal a tarefa de «concordância prática» dos valores conflituantes na ingérvia nas comunicações privadas: por um lado, a tutela do direito à inviolabilidade das comunicações; por outro, a viabilização da justiça penal. Na verdade, como escreve FIGUEIREDO DLAS, «o processo penal é um dos lugares por excelência em que tem de encontrar-se a solução do conflito entre as exigências comunitárias e a liberdade de realização da personalidade individual» (cf. Direito Processual Penal, Coimbra Editora, 1974, pág. 59).

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

353
R

TRIBUNAL CONSTITUCIONAL

(Acórdão do TC n.º 403/2015; v., também, Acórdãos do TC n.ºs 420/2017, 464/2019 e 687/2021 e declaração de voto no Acórdão n.º 91/2023 do C. Conselheiro Afonso Patrão)

"A previsão da ressalva relativa aos casos previstos na lei em matéria de processo criminal inscrita na parte final do artigo 34.º, n.º 4, da Constituição visa, em primeira linha, dar observância à injunção constitucional de que a restrição de direitos fundamentais se encontre expressamente prevista na Constituição (cf. artigo 18.º, n.º 2). A menção específica ao domínio do processo criminal procura, em segunda linha, restringir a potencialidade restritiva das normas limitadoras deste direito fundamental a esse preciso espaço. Trata-se, pois, de uma restrição das restrições normativas que o legislador possa porventura lançar sobre o âmbito normativo desta norma jusfundamental. Precisamente aquilo que é característico das normas de reserva qualificada em matéria de limitações de direitos fundamentais: a norma que impõe a previsão constitucional expressa das restrições a normas de direitos fundamentais pretende reduzir a gama de restrições normativas constitucionalmente legítimas."

(v. NUNO BRANDÃO, *Apreensão de Webmail em Processo Contra-Ordenacional e Reserva de Processo Criminal – Contraponto a uma Nova Jurisprudência Constitucional Duplamente Equivocada*, in *Revista Portuguesa de Direito Constitucional*, n.º 3, 2023, separata, AATRIC, p. 233; v., também, se bem que em termos mais concisos, J. GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, Vol. I, Coimbra, 2007, p. 544 e GERMANO MARQUES DA SILVA e F. SÁ, in *Constituição Portuguesa Anotada* (org. JORGE MIRANDA/RUI MEDEIROS), Vol. I, 2.ª ed., Lisboa, 2020, p. 562-563)

Esta foi uma opção do Legislador constitucional *expressa, literal e plena de intenção* e, se sem dúvida importa a *exclusão* desta classe de meios de obtenção de prova de todas as outras fórmulas processuais e de todas as formas de procedimento administrativo (sejam quais forem os interesses normativos ali em causa), essa é uma consequência indissociável do juízo de prevalência conferido pela Lei Fundamental à garantia de inviolabilidade das comunicações. Diríamos mesmo que é, precisamente, esse *efeito excludente* que se pretende alcançar pela sobredita norma constitucional, que será por isso impassível de, ao mesmo passo, se arvorar em fundamento de solução antagonista, ainda que daí resultem dificuldades acrescidas para a comprovação e punição de certas práticas.

Quando falamos de ingerências em telecomunicações, falamos, com toda a certeza, de *escutas telefónicas* (artigos 187.º-188.º, do CPP), de *interceção de comunicações eletrónicas* (artigo 18.º da Lei n.º 109/2009, de 15 de setembro) e de *interceção de correio postal fechado* (artigo 179.º do CP), ou seja, de atos que podem importar pouco menos que uma verdadeira *manobra de cerco* à pessoa visada pela instalação de pontos de extração de informação ao longo de toda sua rede de comunicações interpessoais: no limite, toda os *inputs e outputs* comunicacionais que realize com terceiros estarão sob vigilância, realizando uma imensa recolha de dados pessoais relativos aos intervenientes (aqui se incluindo os terceiros com quem contacte) em tempo real e durante a sua vida de quotidiano.



TRIBUNAL CONSTITUCIONAL

35/2
R

A norma do artigo 34.º, n.º 4, da Lei Fundamental, como acima se disse, tem por escopo não relegar a admissibilidade deste tipo de atividade de recolha de prova a juízos casuísticos de proporcionalidade (artigo 18.º, n.ºs 2 e 3, da Constituição da República Portuguesa), antes garantiu que se cingiria ao espaço de atuação do Direito penal, convocando os seus peculiares atributos de *ultima ratio*, *subsidiariedade* e *fragmentariedade* para delimitar um ponto de estrangulamento à iniciativa legislativa nesse sentido. Na gestão de interesses que lhe cabe, o Legislador constitucional desvalorizou liminarmente a utilidade que estes meios de obtenção prova (sem nenhuma dúvida) possuiriam em outros segmentos da regulação adjetiva da ação pública para tutela de bens jurídicos, por tributo à violência do registo de intrusão que corporizam em direitos, liberdades e garantias.

Por outro lado, o Acórdão do TC n.º 91/2023 supõe que será possível destacar de entre os valores jurídicos que beneficiam de agasalho constitucional um catálogo de maior estatuto jurídico e dotado de *dignidade penal*, mas cuja defesa, no plano do Direito ordinário, possa estar entregue a outros ramos do Direito punitivo, seja porque a pena é desnecessária à sua proteção, seja porque o Legislador omitiu a incriminação. Deste grupo distinguir-se-á um outro, que será composto por valores constitucionais cuja defesa ficará relegada para outros ramos do Direito, designadamente o contraordenacional. O arresto não avança, porém, metodologia ou critério para proceder a esta ordenação binária de valores jurídico-constitucionais e essa tarefa não parece ser viável.

O que distingue o ilícito de mera ordenação do ilícito penal e que permite efetuar uma delimitação material entre ambos os ramos do Direito sancionatório não é o diferente catálogo de bens jurídicos que protegem, mas a *fórmula de lesão* que sancionam. É dizer, a especial dimensão ético-social que caracteriza o crime encontra-se nos especiais atributos da conduta punida e do registo (qualitativo) do respetivo impacto, não na disparidade de atributos entre interesses constitucionais tutelados por forma que permitisse hierarquizá-los em dois grupos distintos.

Vendo melhor, enquanto o crime reage a uma forma de lesão no bem jurídico que precede qualquer forma de proibição de Direito ordinário, respondendo a uma especial valoração ético-axiológica da conduta, o ilícito de mera ordenação conexiona-se de forma especial com uma norma (administrativa) proibitiva de um comportamento que é instrumental à defesa do interesse normativo. Com HASSEMER, frisamos que qualquer “*proibição que não consiga reportar-se a um bem jurídico seria terrorismo estatal*” (*apud* C. ROXIN, *Sobre o recente Debate em torno do Bem jurídico, in Novos Estudos de Direito Penal*, Alaor Leite (Org.), Marcial Pons, 2014, p. 42), pelo que, em ambos os domínios do



TRIBUNAL CONSTITUCIONAL

Direito punitivo citados, tem-se em vista a proteção de bens jurídicos, por vezes até do *mesmo* bem jurídico, sem que os distinga diferente registo de valor constitucional. Por isso se entende inviável a “*delimitação material do ilícito penal e do ilícito de mera ordenação social na base de não poder reconhecer-se a existência de um ilícito ético-socialmente indiferente, mesmo que ele seja de «mera ordenação social».*” (v. J. FIGUEIREDO DIAS, *Direito Penal, Parte Geral*, Tomo I, Coimbra Ed., 2.ª edição, 2007, p. 161).

A delimitação substancial entre os ramos do Direito sancionatório reportar-se-á, pois, às *condutas* em si mesmas, não aos bens jurídicos que tutelem, já que a algumas delas “*corresponde um mais amplo desvalor moral, cultural ou social*”, por contraponto a outras, que se cingem à dimensão infracional de uma proibição específica que desempenha uma função de proteção: o “*que no direito de mera ordenação social é axiológico-socialmente neutro não é o ilícito, mas a conduta em si mesma, divorciada da proibição legal; sem prejuízo de, uma vez conexionada com esta, ela passar a constituir substrato idóneo de um desvalor ético-social. É este o critério decisivo que está na base do princípio normativo fundamentador da distinção material entre ilícito penal e ilícito de mera ordenação social.*” (v. J. FIGUEIREDO DIAS, *op. cit.*, pp. 161-162).

Ilustrando o exposto, ninguém duvidará que conduzir um automóvel do lado direito da rodovia, por oposição ao esquerdo [artigo 13.º, n.º 1, do Código da Estrada (CE)], constitui um comando arbitrário e desprovido de validade axiológica. A condução em desrespeito pela posição de marcha obrigatória é, como tal, punível como contraordenação (artigo 145.º, n.º 1, alínea f), do CE), já que a estrutura da conduta típica assenta na violação de um vínculo meramente ordenatório, não ético-jurídico. O valor normativo tutelado pelo tipo e pela proibição, porém, é a *segurança das linhas de comunicação rodoviária*, que se arvora em interesse penalmente tutelado em, pelo menos, quatro tipos criminais diferentes do nosso ordenamento jurídico-penal (artigos 291.º e 292.º, ambos do Código Penal e artigo 3.º, n.ºs 1 e 2, da Lei n.º 2/98, de 3 de janeiro – v. PAULA RIBEIRO DE FARIA, *Commentário Conimbricense do Código Penal, Parte Especial*, Tomo II (Artigos 202.º-308.º), Coimbra Editora, 1999, pp. 1079-180 e 1093-1094; Acórdão do Tribunal da Relação de Lisboa de 03.12.2009 no Proc. 84/08.3SQLSB.L1-9, Acórdão do Tribunal da Relação do Porto de 18.04.2007 no Proc. 0647206 e Acórdão do Tribunal da Relação de Coimbra de 19.10.2011 no Proc. 241/09.5GEACB.C2).

Talvez mais denotativo do que dizemos serão os casos em que o tipo criminal se distingue do contraordenacional por mero critério *quantitativo* que, porém, adquire expressão *qualitativa* para efeitos da caracterização da infração ético-axiológica estrutural ao crime (v. J. FIGUEIREDO DIAS, *op. cit.* p. 163). Nestes casos, a identidade entre bens jurídicos protegidos será tanto mais evidente.

356
A.



TRIBUNAL CONSTITUCIONAL

A conduta típica do crime de fraude fiscal, p. p. pelo artigo 103.º, n.º 1, alínea a), do Regime Geral das Infrações Tributárias (RGIT) (v. g., ocultação de factos fiscalmente relevantes em livros de contabilidade), é punida como contraordenação, p. p. pelo artigo 118.º, n.º 1, do RGIT, quando o prejuízo fiscal não excede € 15.000,00 (artigo 103.º, n.º 2, do RGIT). Se a partir deste valor de dano se tem por justificada a qualificação do comportamento como “*ética-socialmente relevante*”, passando a “*constituir substrato suscetível de a ele se ligar a respetiva criminalização, atento o salto «qualitativo» que naquele limite sofre [o dano] social da conduta e a sua censurabilidade ética (isto se cifrando a sua correspondência a uma prévia e mais ampla valorização)*” (v. J. FIGUEIREDO DIAS, *op. cit.* p. 163), tudo isto se referencia ao *grau de lesão do mesmo bem jurídico* (usualmente caracterizado com relação à *afunção social* do imposto – v. MÁRIO FERREIRA MONTE, *Da Legitimização do Direito Penal Tributário, em Particular, os paradigmáticos casos de facturas falsas*, 2007, Coimbra Editora, pp. 275-279 e ANABELA RODRIGUES, *Contributo para a fundamentação de um discurso punitivo em matéria penal fiscal in AAVV, Direito Penal Económico e Europeu: Textos Doutrinários*, Vol. II, Problemas Especiais, Coimbra, 1999, pp. 481-489), não a uma tutela de interesses distintos que permitisse contrapor o ilícito criminal ao de mera ordenação a esse título.

Aproximando o exposto do caso *sub iudice*, veja-se que concluir, com o Acórdão do TC n.º 91/2023, pela dignidade penal da *concorrência*, não significa que todas as atividades lesivas desse valor constitucional sejam passíveis de incriminação. Haverá que distinguir as condutas que se podem entender caracterizar uma lesão ético-axiológica, instalada *a montante* de proibições legais (v. F. N. LOUREIRO, *Direito Penal da Concorrência*, Almedina, 2017, pp. 229 e ss, justificando a necessidade de criminalização *apenas* quanto a certos cartéis), os comportamentos que se entenderão mera infração ou insuficiente observância de comandos proibitivos de práticas comerciais, sejam eles acordos, ou decisões associativas, lesivos do paradigma concorrencial (ou seja, que estejam conexionadas de forma específica com proibições legais) e, ainda, as que, impactando no bem jurídico, se podem entender toleradas ou consentidas, face ao seu caráter *de minimis* ou pela presença de outros interesses jurídicos: no primeiro caso, a incriminação é possível; no segundo, a falta de relevo ético-jurídico interditará incriminação, ainda que a tutela do bem jurídico possa justificar outra forma de sancionamento; no terceiro, a intrusão em direitos, liberdades e garantias será inviável, por tributo ao princípio da proporcionalidade (artigo 18.º, n.º 2, da Constituição da República Portuguesa).

Daqui decorre que a pretendida classificação de valores jurídico-constitucionais que definisse um conjunto fechado passível de tutela penal para efeitos de delimitação da reserva



TRIBUNAL CONSTITUCIONAL

357
X

estabelecida pelo n.º 4, do artigo 34.º, da Constituição da República Portuguesa, por contraponto a outro conjunto, cuja defesa não careceria dessa forma de proteção e a que o segredo de telecomunicações ofereceria impedimento jurídico-constitucional, não é viável, nem adequada: na verdade, o que empresta singularidade ao crime é a *conduta* que pune, não o bem jurídico que defende, já que partilhará o desempenho desta função com muitos outros ramos do Direito.

A insuficiência deste critério tem ainda o especial (e grave) inconveniente de conduzir a uma *abertura excessiva* da reserva de processo criminal a intrusões em telecomunicações. Se se diz que a concorrência é penalmente tutelável e, por isso, que a tutela contraordenacional autoriza a intrusão em telecomunicações em processos por infrações de outra natureza (ilícitos de mera ordenação), impõe-se ia questionar se o bem jurídico complexo protegido pelo crime de fraude fiscal qualificada, p. p. pelos artigos 103.º e 104.º, do RGIT, ofereceria idêntica permissão quanto à contraordenação que pune lapsos ou omissões em declarações fiscais (artigo 119.º do RGIT). Ninguém duvidará que o bem jurídico em causa nas infrações fiscais (em todas elas) não é de segunda linha, o que bem se denota pela introdução de tipos criminais nesse âmbito e pelo registo de penas aplicáveis, mas não é menos evidente (mesmo antes de um juízo de proporcionalidade ao abrigo do artigo 18.º, n.º 2, da Constituição da República Portuguesa) que a reserva de processo criminal de telecomunicações proibirá ingerências dessa natureza na investigação de tipos com este registo insípido de danosidade jurídica. Esta conclusão explica-se, pois, pela inexistência de um desvalor ético-axiológico na *conduta* considerada, não pelo menor valor do bem jurídico que protege.

Serve por dizer, resulta do exposto que o critério adotado pelo Acórdão n.º 91/2023 descaracterizaria a reserva do artigo 34.º, n.º 4, da Lei Fundamental enquanto reserva de “*lei em matéria criminal*”, já que conduz a admitir intrusões em comunicações em todos os processos referentes a infrações tutelares de bens jurídicos dotados de dignidade penal, ainda que a forma de lesão que sancionem não seja passível de integrar um tipo de crime do ponto de vista dogmático.

É disto bom exemplo o proposto juízo de admissibilidade de ingerência em comunicações no âmbito de *toda e qualquer* infração (contraordenacional) ao Direito da concorrência, quando o respetivo catálogo não é certo que puna, em todos os casos, condutas criminalizáveis.

9.2. Pelo exposto, ao delimitar uma reserva de processo penal, a norma do artigo 34.º, n.º 4, da Constituição da República Portuguesa, será entendida no sentido de condicionar a ingerência

358
X

TRIBUNAL CONSTITUCIONAL

em telecomunicações à adjetivação de uma pretensão punitiva que constitua reação jurídica a um comportamento cuja peculiaridade residirá na *imprescindibilidade da pena* para o desempenho de uma função de tutela *suficiente* do bem jurídico em causa. É, precisamente, este o elemento que conduz a Lei Fundamental a ceder sobre a inviolabilidade que prescreve para as comunicações, porque por ele se assegura que a cedência é realizada no interior dos espaços mais sensíveis da ordem jurídica.

Outra solução esvaziaria o alcance da norma como *restrição* a intrusões nesta garantia:

"prevalece entre nós a ideia de que «a justificação de uma restrição normativa não pode deixar de assentar numa norma constitucional». Temos então que uma interpretação da reserva qualificada de restrição prevista no artigo 34.º, n.º 4, no sentido de que se refere ao conceito material de crime e portanto às intervenções para tutela de direitos e interesses constitucionalmente protegidos nada de substancial acrescenta aquilo que sempre se exigiria, em termos gerais, se nenhuma menção constitucional fosse feita à possibilidade de limitação do direito à inviolabilidade das telecomunicações: esta restrição também só seria constitucionalmente admissível se se mostrasse voltada para a salvaguarda de direitos ou bens constitucionalmente garantidos.

Com isto se percebe que, mesmo de um ponto de vista substancial, o conceito de matéria criminal a que o artigo 34.º, n.º 4, da Constituição alude tem necessariamente de conter um plus que o diferencia e singularize de outras expressões normativas, sancionatórias ou não, que visem a proteção de interesses com guarda constitucional. Esse extra, não partilhado por normas restritivas de direitos fundamentais a que pode ser reconhecida dignidade penal (v.g., de natureza contra-ordenacional), corresponde à necessidade de pena. Por definição, os factos objecto de uma intervenção penal legítima são aqueles que para além do ostentarem dignidade penal (sc., atentam de forma qualificada contra bens jurídicos com um referente constitucional) reclamam a aplicação de uma pena criminal. Daí que se deve entender, acompanhando o Conselheiro Afonso Patrão, que «a Constituição sentenciou que só podem ter lugar as medidas de investigação mais intrusivas para as condutas relativamente às quais, em cada momento, o legislador considerou haver dignidade criminal e carença de pena, retirando ao intérprete o espaço para encontrar distinta operação de concordância prática».

Como é bom de ver, a necessidade de pena pressuposta pelo conceito de matéria de processo criminal constante do artigo 34.º, n.º 4, da Constituição, é um elemento constitutivo de legitimação estranho às contra-ordenações. Nessa medida, também por esta razão, diferentemente do que conclui o Tribunal Constitucional [no Acórdão n.º 91/2023], não podem as normas contra-ordenacionais restritivas do direito fundamental à inviolabilidade das telecomunicações ser qualificadas como matéria de processo criminal no âmbito da qual só autorização constitucional para a sua limitação."

(v. NUNO BRANDÃO, *op. cit.*, pp. 236-237)

Podemos também acrescentar que o entendimento adotado pelo Acórdão do TC n.º 91/2023 eliminaria outras dimensões de alcance da reserva de processo penal, também nessas vertentes representando uma erosão irrazoável das garantias conferidas pela norma constitucional.

Na verdade e em primeiro lugar, a reserva em processo penal impõe que a medida ingerente em telecomunicações dependa de prévia criminalização do comportamento que subjaz à pretensão punitiva e, bem assim, que seja consagrada no respetivo regime processual penal. Isto significa que



TRIBUNAL CONSTITUCIONAL

ambas as iniciativas dependem de iniciativa parlamentar (artigo 165.º, n.º 1, alínea c), da Constituição da República Portuguesa), ao contrário do que sucede no Direito das contraordenações, em que tanto a introdução de tipos como inovações na Lei processual estão compreendidas na competência legislativa do Governo (cfr. artigos 165.º, n.º 1, alínea d), e 198.º, n.º 1, alínea a), ambos da Constituição da República Portuguesa – embora vinculada aos limites do respetivo regime geral, também inscrito na reserva relativa da Assembleia da República).

A obrigatoriedade de intervenção parlamentar, inibindo a iniciativa legislativa do Governo, terá de se entender instrumento de garantia da limitação dos instrumentos de ingerência na autonomia comunicativa e adquire especial relevo quando se considere que, *in casu*, debatemos pretensões punitivas de Direito público em que se confrontam Estado-administração e particulares.

A reserva de processo penal, observada em sentido formal, impõe também que a intrusão em telecomunicações seja apenas admissível em *processos jurisdicionais* (artigo 32.º, n.ºs 4 e 5, da Constituição da República Portuguesa) colocados sob titularidade de Juiz ou de Magistrado do Ministério Público, com benefício de *independência* e de *autonomia* (artigos 203.º e 219.º, n.º 2, ambos da Constituição da República Portuguesa). A *judiciarização* das medidas intrusivas em telecomunicações é, também, penhor de garantias acrescidas para particulares, excluindo cedências quanto à sua inviolabilidade em processos sob titularidade de entidades administrativas (designadamente contraordenacionais), nessa medida circunscrevendo a autoridade do poder estadual e maximizando a conexão material da intrusão para com o referente legitimador.

De resto, cabe assinalar que se nos afigura algo contraditório que se defenda, por um lado, que o artigo 34.º, n.º 4, da Constituição da República Portuguesa, não se refere ao processo criminal regulado pelo artigo 32.º da Lei Fundamental e, por outro, se conclua que qualquer ato material de intrusão em telecomunicações estará dependente de autorização por Juiz, tanto mais quando se funda esta orientação pela chamada da jurisprudência firmada pelo Acórdão do TC n.º 687/2021.

Isto, desde logo, porque o entendimento da reserva de processo criminal adotado pelo Acórdão n.º 91/2023 tem por atributo essencial a excisão do «*exclusivo judiciário*» sobre intrusões em comunicações, determinando a sua partilha com iniciativas punitivas de caráter administrativo.

Em segundo lugar, porque o artigo 34.º, n.º 4, da Lei Fundamental não estabelece a obrigatoriedade de intervenção judicial de atos intrusivos na autodeterminação comunicativa, ao contrário do que se observa (v. g.) quanto a intrusões em *domicílio* (no n.º 2, do mesmo articulado),



TRIBUNAL CONSTITUCIONAL

363
X.

na *liberdade* [artigos 27.º, n.ºs 2 e 3, alíneas c) a e), 28.º e 30.º, n.º 2] ou no *direito a permanência em território nacional* (artigo 33.º, n.ºs 2 e 7). O Acórdão do TC n.º 687/2021 defende que a pesquisa e apreensão de mensagens eletrónicas está dependente de autorização judicial por entender que o n.º 4, do artigo 34.º, da Lei Fundamental, remete para o estatuto de garantias do *processo penal* constante do artigo 32.º da Constituição da República Portuguesa (assim em sentido formal); em concreto, recorre a uma leitura especial do n.º 4 deste preceito, quando confere competências exclusivas a Juiz em matéria de direitos fundamentais. Mais que não aderir a este entendimento, o Acórdão n.º 91/2023 defende solução oposta, elaborando um conceito de «*processo penal*» autónomo que não se identifica com o regime adjetivo do Direito do crime. É, pois, difícil de perceber onde se encontra a norma injuntiva de autorização judicial que suportou o juízo de inconstitucionalidade material.

Prosseguindo, também o estatuto de defesa do arguido em processo-crime é convocado para entender a reserva de processo criminal das ingerências em telecomunicações em sentido formal, por constituir uma medida de contrapeso da violência operada na personalidade do visado pela invasão das comunicações ao serviço da reunião de prova de valor condenatório. Aderimos a este entendimento e não nos parece convincente a crítica que o Acórdão n.º 91/2023 lhe dirige.

É certo, como bem ali se assinala, que a generalidade das intrusões em telecomunicações em inquérito-crime (senão a *totalidade*) ocorre *antes* de o visado adquirir aquele estatuto jurídico-processual (de arguido) e sem a possibilidade de exercício dos direitos conferidos a esse título para a prevenir. Isto é assim e bem se comprehende: *escutas telefónicas* e *intercepção de comunicações eletrónicas*, por exemplo, possuirão pouca ou nenhuma utilidade como meios de obtenção de prova se o visado estiver alarmado para a investigação. No entanto, é indesmentível que, uma vez adquirido o estatuto de arguido, a Lei Fundamental confere ao visado um arsenal de instrumentos jurídicos de reação e de impugnação à pretensão punitiva incomparável (porque superlativo) às garantias constitucionais do processo contraordenacional. É assim, designadamente, quanto a acesso e obrigatoriedade de representação por defensor, de presença, de contraditório, de presunção de inocência, de celeridade, de observância de juiz natural e de acesso a Tribunais superiores (artigo 32.º, n.ºs 1, 2, 3, 5, 6 e 9, da Constituição da República Portuguesa). No plano constitucional, as garantias de processo de contraordenação bastam-se com direitos de *audiência* e de *defesa* (artigo 32.º, n.º 10, do diploma), o que não apenas representa menor capacidade de reação aos efeitos da ação intrusiva na inviolabilidade das comunicações (v. g., contra a sua documentação e perspetivas de exposição



TRIBUNAL CONSTITUCIONAL

no âmbito do processo sancionatório em que se haja efetivado a operação), como condicionantes importantes à defesa em matéria de consideração e valoração da prova adquirida por aquela via.

Serve por dizer, a reserva de processo penal empresta maior equilíbrio ao confronto intra-processual, assegurando que o volume de informação importado por via de uma medida altamente intrusiva na esfera pessoal do visado em abono da pretensão punitiva encontrará uma defesa dotada de armas processuais suficientes e adequadas a oferecer-lhe contradição e confronto.

Por outro lado, é possível inverter o argumento central do Acórdão do TC n.º 91/2023: se a indisponibilidade de meios de prova que resultem de ingerências em telecomunicações será apta a criar um viés no juizo legislativo tendente a promover a criminalização para, com isso, franquear o acesso a eles, a doutrina proposta será o seu anverso, sinalizando, talvez, riscos piores.

Dispensado de criar tipos-de-crime para esse efeito, uma inflexão autoritária estadual sentir-se-á encorajada a optar pela sobretipificação de contraordenações, com isso desprovendo o processo de caráter judiciário (também quanto à titularidade da ação punitiva a cargo de uma Magistratura autónoma) e relegando os Tribunais para uma função de mero controlo da punição administrativa, daí obtendo um sensível alívio sobre garantias processuais do visado, incluindo quanto a contraditório pleno e acesso a Tribunais superiores para revisão de decisão condenatória.

Este fenómeno será mais facilmente conjectável nos ramos do Direito dirigidos, essencialmente, à repressão de práticas protagonizadas por entidades coletivas, como é o caso do Direito contraordenacional da concorrência, já que nesse domínio sanções económicas ou de natureza patrimonial possuem maior importância e dimensão punitiva, descentrando o catálogo de sanções das medidas privativas da liberdade, que se entenderão exclusivas ao Direito penal.

A instrumentalização administrativa do processo contraordenacional para com isso promover a devassa e vigilância de pessoas e entidades será também um horizonte equacionável, já que não se afigura convincente a existência de reserva de autorização judicial defendida por esta parte da jurisprudência sem mobilizar o estatuto de garantias exclusivo ao processo criminal.

Concluímos, por tudo, que a posição introduzida pelo Acórdão do TC n.º 91/2023 (e seguida pelo aresto n.º 314/2023) não é satisfatória, impondo-se, por isso, renovar a jurisprudência constitucional que se enraizou entre nós até então (Acórdãos do TC n.ºs 403/2015, 420/2017, 464/2019 e 687/2021). O exposto serve-nos, porém, para delimitar o âmbito da cobertura do parâmetro constitucional colocado, impondo-se, agora, recentrar a nossa análise na compreensão

362
A

TRIBUNAL CONSTITUCIONAL

da norma do artigo 18.º, n.º 1, do RJDc e perceber de que forma se pode entender impactar na garantia conferida pelo disposto no artigo 34.º, n.º 4, da Constituição da República Portuguesa.

10. Mensagens de Correio Eletrónico e Telecomunicações

10.1. A norma do artigo 18.º, n.º 1, do RJDc, transcrita *supra*, confere autoridade à AdC para proceder à apreensão de mensagens de correio eletrónico que se integrem no estabelecimento da entidade particular visada, incluindo o poder de realizar buscas e revistas para o efeito.

Impõe-se apurar se estas mensagens se podem entender, ou não, *comunicações* para efeitos do respetivo regime de inviolabilidade, o acórdão recorrido adotou o entendimento de que, (i) porque tratava de mensagens «*didas*» e (ii) referentes a uma *pessoa coletiva*, seria inaplicável o regime de proteção conferido pelo artigo 34.º, n.º 4, da Constituição da República Portuguesa (cfr. pp. 100-102). O Acórdão do TC n.º 91/2023, colocado perante argumentação semelhante, não reconheceu mérito ao caráter empresarial/coletivo da entidade buscada ou à distinção entre correio «*dido*» e «*não-lido*» para efeitos de classificação de comunicações, já o sabemos, tanto menos se importassem distinções de tutela.

Quanto à primeira questão colocada, o aresto expandiu a seguinte argumentação sobre o caráter empresarial do beneficiário da proteção constitucional sobre comunicações:

“Quanto à natureza não privada das mensagens apreendidas, não parece haver dúvida de que se trata de circunstância que não afasta a proibição constante do n.º 4 do artigo 34.º da Constituição. A garantia da inviolabilidade da correspondência que decorre dos n.ºs 1 e 4 do artigo 34.º não supõe o caráter pessoal ou particular do conteúdo da mensagem, não sendo posta em causa nem pelo facto de os endereços de correio eletrónico serem “profissionais”, nem pela eventualidade de o conteúdo das mensagens não se ligar à esfera da vida privada das pessoas envolvidas no circuito comunicativo.

A autonomização da proteção da inviolabilidade das comunicações faz ao direito à reserva da intimidade da vida privada tem justamente este sentido: a Constituição garante a segurança das comunicações, independentemente da qualidade do destinatário ou da natureza da mensagem. Como refere Manuel da Costa Andrade, «[n]ão se trata da privacidade em sentido material mas, antes, de um caso paradigmático da privacidade em sentido formal. Desde logo, é indiferente o conteúdo das missivas ou telecomunicações, não se exigindo que versem sobre coisas privadas ou íntimas nem que contendam com segredos. Pode tratar-se de matérias inteiramente abdinas, da troca de informações comerciais entre empresas ou mesmo da circulação de ofícios ou protocolos entre órgãos ou agentes da Administração Pública, em princípio expostos às regras da transparéncia» (Comentário ao artigo 194.º, Comentário Conimbricense ao Código Penal, Tomo I, 2.ª edição, 2012, p. 1084). É por esta razão que a inviolabilidade da correspondência consubstancia um direito referente às comunicações mesmo que dirigidas a pessoas coletivas e ainda que o conteúdo apenas diga respeito a pessoas coletivas (Maria João Antunes, Processo Penal e Pessoa Coletiva Arguida, Almedina, 2020, p. 52). O que é tutelado é a interação comunicativa em si mesmo considerada — a confiança na segurança e reserva dos



TRIBUNAL CONSTITUCIONAL

sistemas de comunicações —, o que abrange as comunicações eletrónicas enviadas e ou recebidas através de correio eletrónico profissional de uma empresa ou dos seus representantes.

Não é outra, de resto, a orientação desde há muito sufragada na jurisprudência constitucional. Como este Tribunal cedo reconheceu, o direito à inviolabilidade das comunicações e da correspondência é titulado também pelas pessoas coletivas, abrangendo desse modo as missivas (eletrónicas ou postais) destinadas ou remetidas a endereços de pessoas coletivas: nas palavras do Acórdão n.º 198/1985, «este é um direito fundamental de que também tais pessoas gozam, nos termos do n.º 2 do artigo 12.º da Constituição».

Tal orientação, note-se ainda, encontra-se perfeitamente alinhada com a jurisprudência dos Tribunais europeus: quer com a do Tribunal de Justiça, que afirmou, ainda em momento anterior à CDFUE, a existência de um princípio geral de direito comunitário que consagra a proteção contra as intervenções arbitrárias e desproporcionadas do poder público na esfera da atividade privada de uma pessoa singular ou coletiva (Acórdão do Tribunal de Justiça de 22 de outubro de 2002, Roquette Frères, proc. C-94/00), aceitando a titularidade desses direitos por parte de pessoas coletivas; quer com a do Tribunal Europeu dos Direitos do Homem (TEDH), que estende a proteção do artigo 8.º da Convenção aos e-mails enviados e recebidos em contexto empresarial (sfr. Acórdão do TEDH de 3 de outubro de 2007, Copland c. Reino Unido, proc. n.º 62617/00, §§ 41 e 42).»

Na sua generalidade, concordamos com esta posição, mas importa assinalar (ainda que não possua especial importância para a decisão do caso *sub iudice*) que, ao contrário do que este excerto pode sugerir, o benefício da autodeterminação comunicativa por pessoas coletivas não significa a equiparação entre âmbitos de garantia efetiva do direito face às pessoas singulares e a isso não se opõe o caráter *formal* do seu objeto de tutela. Na realidade, ainda que o disposto no n.º 4, do artigo 34.º, da Lei Fundamental acobrete *qualquer conteúdo* em comunicação, não deixa por esse motivo de constituir uma derivação especial (e particularmente intensa) da defesa da personalidade, o que determina uma certa medida de assimetria entre beneficiários, consoante se trate de pessoas humanas ou instrumentos jurídicos destinados à ordenação de interesses (pessoas coletivas).

Este imperativo de diferenciação em matéria de sigilo de correspondência (postal) é, de resto, sublinhado pelo Acórdão do TC n.º 198/1985, citado por aquele aresto. Quanto a estoutro, fiscalizava-se o disposto no artigo 1216.º do CPC (na redação anterior ao Decreto-Lei n.º 329-A/95, de 12 de dezembro), que determinava a notificação dos CTT para que procedesse ao reencaminhamento da correspondência dirigida a empresa falida para o administrador nomeado pelo Tribunal. Questionando-se a compatibilidade desta norma para com a garantia de inviolabilidade de comunicações, entendeu o Tribunal Constitucional no Acórdão n.º 198/1985:

“Não que se conteste, em geral, a afirmação de que o direito ao sigilo da correspondência não é incompatível com a natureza das pessoas coletivas e de que, portanto, este é um direito fundamental de que também tais pessoas gozam, nos termos do n.º 2 do artigo 12.º da Constituição. Ao contrário: não apenas se compartilha o asserto, como podem mesmo invocar-se, em abono dele, vários apoios doutrinários, tanto na literatura nacional como na estrangeira. Assim:



TRIBUNAL CONSTITUCIONAL

V. Andrade, ob. cit., p. 176, nota 68; G. Canotilho-V. Moreira, ob. cit., artigo 12.º, anot. IV, p. 146; Oehler, ob. cit., p. 611; e ainda A. Pace, ob. cit., p. 98.

*Simplesmente, a «aplicação» dos direitos fundamentais às pessoas colectivas não pode deixar de levar em conta a particular natureza destas — e de tal modo que seguramente tem de reconhecer-se que ainda quando certo direito fundamental seja compatível com essa natureza, e portanto susceptível de titularidade «colectiva» (*boc sensu*), daí não se segue que a sua aplicabilidade nesse domínio se vá operar exactamente nos mesmos termos e com a mesma amplitude com que decorre relativamente às pessoas singulares. Tem a doutrina chamado a atenção para o ponto, e designadamente para o facto de o «conteúdo» dos direitos fundamentais poder ser diferente (e mais estreito) quando o respectivo titular for uma pessoa colectiva, antes que uma pessoa singular (assim, V. Andrade, ob. cit., pp. 176 e seg.).*

Oras, se não for exactamente isto (uma diferença de «conteúdo») que se verifica no caso do direito ao sigilo de correspondência, certo é, de todo o modo, que a própria estrutura da personalidade colectiva exclui que esse direito, enquanto direito de uma sociedade comercial, se possa dizer violado ou ilegitimamente restringido pelo disposto no artigo 1216.º do Código de Processo Civil (ainda que assim devam entender-se as coisas quando esteja em causa um falso singular).

Neste sentido se posiciona a doutrina recente, também citada no Acórdão do TC n.º 91/2023:

*“(...) o direito ao sigilo da correspondência não é incompatível com a natureza das pessoas coletivas (...) é um direito fundamental de que também tais pessoas gozam nos termos do n.º 2, do artigo 12.º, da Constituição. Simplesmente, a ‘aplicação’ dos direitos fundamentais a pessoas coletivas não pode deixar de levar em conta a particular natureza destas (...) tem de reconhecer-se que ainda quando certo direito fundamental seja compatível com essa natureza e portanto susceptível de titularidade «colectiva» (*boc sensu*), daí não se segue a sua aplicabilidade nesse domínio se vá operar exactamente nos mesmos termos e com a mesma amplitude com que decorre relativamente às pessoas singulares.”* (v. M. JOÃO ANTUNES, *Processo Penal e Pessoa Coletiva Arguida*, Almedina, 2022, p. 53 *apud* M. P. ANTUNES, *Prática restritiva da Concorrência – busca e apreensão de mensagens das empresas por mandado do Ministério Público*, in *Revista do Ministério Público*, 176, 2023)

É igualmente desta forma que a jurisprudência do Tribunal Europeu dos Direitos do Homem (TEDH) configura o direito de reserva sobre comunicações do artigo 8.º na Convenção dos Direitos do Homem (CEDH), ali assimilado à proteção do domicílio. O TEDH faz ver que “*em certas circunstâncias, os direitos garantidos pelo artigo 8 da Convenção podem ser interpretados como inclinando*” a tutela de sociedades comerciais, sem por isso deixar de assinalar que “*o direito de ingerência dos Estados pode ir mais longe*” nesses casos, por contraponto ao tratamento reservado a pessoas singulares (v., também, Acórdão do TEDH *Delta Pekární vs. República Checa* de 2 de janeiro de 2015; também *Niemitz v. Alemanha*, de 16 de dezembro de 1992 e *Société Colas e outros v França*, de 21 de outubro de 1998).

Deixada esta ressalva, assentamos na conclusão que o artigo 34.º, n.º 4, da Constituição da República Portuguesa, estende proteção a comunicações de pessoas coletivas e, ainda que o âmbito



TRIBUNAL CONSTITUCIONAL

de proteção efetiva conferida possa importar diferenças de tratamento face a pessoas singulares, a sua completa negação, adotada pelo Tribunal “*a quo*”, não é juízo que mereça a nossa adesão.

10.2. Já sobre a caracterização de mensagens de webmail como *comunicações*, o Acórdão do TC n.º 91/2023, como vimos, afastou a distinção entre correio «*lido*» e «*não lido*» e introduziu outro critério para delimitar a respetiva tutela: enquanto as mensagens eletrónicas permanecerem na «*caixa de correio eletrónico virtual*» do utilizador de webmail, serão entendidas como «*informação em trânsito*» já que nessa fase se encontram, ainda, *sob controlo do prestador do serviço de webmail* e, como tal, na especial situação de vulnerabilidade característica à comunicação. A mensagem apenas perderá essa natureza (e inerente proteção) quando for objeto de «*arquivamento definitivo noutra local do computador*»: apenas então se admitirá que mensagens de webmail ou de sistemas análogos (v. g., mensagens instantâneas) sejam qualificadas como documentos e, por inerência, resultem excluídas do espectro de defesa definido pelo n.º 4, do artigo 34.º, da Constituição da República Portuguesa.

Ora, um primeiro problema que salta à vista é que a «*caixa de correio eletrónico virtual*» a que se alude não é um «*local*», um ponto no espaço onde alguma coisa possa ser acondicionada ou mantida, ou de onde algo (seja uma mensagem, um ficheiro digital, ou o que se queira considerar) possa ser *retirado* para outro local qualquer. A «*caixa postal*» é uma representação gráfica de informação contida em ficheiros informáticos, uma *ilusão* gerada pelo programa com recurso a grafismos que tem por escopo funcional permitir o processamento dos dados pelo utilizador de forma intuitiva.

Uma «*caixa postal*» de correio eletrónico, enfim, não tem «*forro*», nem «*dentro*», já que, em bom rigor, *nem sequer existe*. Talvez melhor, a existência de uma «*caixa de correio eletrónico virtual*» cinge-se ao cérebro humano, produto da especial interação que o programa informático promove entre o sistema e o aparelho sensorial do utilizador, mas nada mais que isso: daí ser designada «*virtual*».

Em segundo lugar, não é verdade que o *webmail account provider* retenha controlo sobre os ficheiros digitais cuja informação é acedida no interface de «*caixa postal virtual*». Desde logo, a mensagem de correio eletrónico não realiza um percurso em sentido próprio, não se desloca do ponto “A” para o ponto “B”, antes é *reproduzida* e *fixada* em dispositivos, incluindo o terminal do titular da conta. A percepção de que a mensagem se acha numa espécie de «*presença latente*» no aparelho do utilizador durante a consulta da «*caixa postal*» e que, com o *log out* ou o fecho da página, ela *abandona-o e regressa* ao servidor, é também apenas uma ilusão gerada pelo programa de interface.



TRIBUNAL CONSTITUCIONAL

Rigorosamente toda a informação visualizada na «caixa de correio eletrónico virtual» foi prévia e inteiramente transferida para o sistema local e acha-se contida nas suas componentes de fixação de dados, sob controlo do utilizador nas mesmas condições que os demais ficheiros armazenados no computador, quer tenham sido extraídos da web ou importados de outra fonte (v. g., de *pen drive*, disco rígido externo, CD-DVD, etc.). O circuito de extração de webmail assenta na *reprodução* do ficheiro da mensagem e na sua *gravação* no aparelho do utilizador, sendo a partir daí a informação processada pela memória operativa para ser exibida pelo programa de interface da aplicação ou do *browser*; não existe *deslocação* de dados sob controlo do *service provider*, do servidor para o utilizador e vice-versa, ao sabor de comandos a partir do terminal ou dos *log in* e *log out* que se realizem.

Sendo assim, já se antevê do exposto que o conceito de “*armazenamento definitivo*” da mensagem “*em outro lugar do computador*” que não a «caixa postal», não é adequado como critério para definir o momento em que esta perde a natureza de comunicação e fica desprovida deste regime de tutela. Diríamos mesmo difícil de alcançar aquilo a que pretende aludir esta descrição, já que, como se disse, a caixa virtual não é, de si, «um lugar no computador» de que pudesse existir “*outro*”, e porque nada de identificável com uma «*operação de armazenamento definitivo*» se encontra entre as operações realizadas por protocolos de webmail ou de entre o vasto leque de ferramentas disponíveis aos utilizadores para processamento local da informação.

Também é difícil de perceber o valor da observação relativa à possibilidade de visualizar informações sobre mensagens *fechadas* quando se aceda à «caixa postal virtual». É que uma diligência de busca e apreensão de registos de mensagens de correio eletrónico não importa acesso ao interface utilizado pelo titular da conta para visualizar e gerir mensagens (a «caixa de correio virtual»). A busca realiza-se pela extração de informação de discos rígidos do sistema através de sistemas de rastreio e deteção de ficheiros, sem que implique acesso ao grafismo que exibe informações sobre mensagens (*abertas/fechadas*) ao utilizador a que o acórdão parece aludir.

Se pretendermos delimitar a cobertura constitucional conferida ao correio eletrónico, impõe-se, antes de mais, compreender devidamente a tecnologia em causa, já que o seu perfil comercial e a utilização de terminologia e imagens próprias a outros meios de comunicação (*maxime*, ao correio tradicional) no grafismo adotado pelos interfaces de utilizador, bem como em sinais distintivos de empresas exploradoras, sugerem uma realidade paralela, induzindo em confusões conceptuais que se introduziram na linguagem corrente e na sensibilidade adquirida sobre o



TRIBUNAL CONSTITUCIONAL

fenómeno pela consciência coletiva. A simples designação do sistema, «*correo electrónico*», «*e-mail*», ou «*webmail*», de imediato mobiliza a arquitetura mental inerente ao vetusto «*correo postal*», oferecendo por tentação equivalência de conceitos, gerando dessa forma um viés que compele o observador a precipitar-se quanto a conclusões sobre a qualificação jurídica dos atos e operações envolvidas neste tipo de tecnologia informática. Se esta observação das coisas é simples, sedutora e muito difundida, inevitavelmente desrespeita a diferença abissal que existe entre as realidades colocadas, que na verdade possuem muitas dissemelhanças, criando entorses no plano do tratamento jurídico.

10.3. Procurando agrupar algumas noções que utilizaremos adiante, a *comunicação* protegida pelo disposto no artigo 34.º, n.ºs 1 e 4, da Constituição da República Portuguesa, pode ser entendida como o *processo de transmissão de informação de uma pessoa para outra*. «*Meios de comunicação*» e «*telecomunicações*», de sua parte, serão os *instrumentos* dirigidos a obter esse resultado funcional quando os interlocutores não se encontrarem na presença um do outro (v. M. COSTA ANDRADE, *Comentário coimbricense do Código Penal, Parte especial*, Tomo I, Coimbra Ed., 1999, pp. 759-760).

Em alguns casos, a comunicação deixa um *suporte* que preserva o conteúdo comunicado ou certas informações ou atributos específicos ao fluxo de informação realizado. A esse suporte físico chamamos *documento*. Este desempenha uma importante função de evidência no tráfego jurídico, permitindo aos intervenientes no processo comunicacional recordar o conteúdo entre eles trocado (v. g., o que declarei/o que me foi declarado; o que entreguei/o que me foi entregue) e adquire, por isso, valência probatória externa para diversos efeitos (v. g., para instrução de processos disciplinares, administrativos ou judiciais, para suporte de lançamentos contabilísticos, etc.).

Como decorre da definição, o documento é estranho ao conceito de *comunicação* ou de *meio de comunicação*, constituindo apenas *restígio* incidental da primeira e resíduo libertado pelo desempenho da atividade funcional do segundo. Para conservar o conteúdo até que chegue ao destinatário, é, por vezes, necessário um instrumento de *fixação* (na carta, uma folha de papel; no e-mail, um ficheiro informático) e é a sua existência subsequente, depois de *concluído* o fluxo de informação, que se arvora em *documento*, passível de representar factos ou pessoas.

Já resulta do que fica dito, o documento não é sequer consequência necessária da utilização de um meio de comunicação, já que alguns não carecem de componentes de fixação da informação e, por isso, não deixam rasto da troca realizada: a existência de elementos que registem ou permitam

368
L

TRIBUNAL CONSTITUCIONAL

reconstruir o processo comunicacional ou os dados transmitidos ficará dependente das opções dos intervenientes sobre meios de comunicação que se encontram ao seu dispor. Em boa parte dos casos, de resto, este será escolhido pelo autor em função da sua aptidão para gerar um suporte que certifique o conteúdo transmitido ou outra informação relativa à comunicação, ou, em contrário, será eleito tendo em vista minimizar o risco de geração deste tipo de elementos a ela relativos.

Numa interpelação ao cumprimento entre contratantes ou na apresentação de uma peça processual a juízo, por exemplo, o locutor (interpelante/sujeito processual) escolherá um meio de comunicação que lhe ofereça garantias de vir a poder comprovar a data em que o fluxo de dados ocorreu e respetivo conteúdo (v. g., carta registada), tendo em vista poder comprovar o exercício de pretensão e a observância de prazo; durante tratativas negociais, as partes poderão optar por trocar mensagens de correio eletrónico tendo em vista manter um espólio documental completo sobre as suas comunicações que enriquecerá a compreensão das estipulações contratuais finalizadas, na eventualidade de contencioso; pretendendo intimidar o interlocutor ou realizar uma afirmação por outro motivo inconfessável, dada pessoa poderá optar por realizar uma chamada de voz por telefone, tendo em vista minimizar os vestígios libertados pelo fluxo de informação.

Assim, tal como num processo de locomoção de uma pessoa *uma passada* não se confunde com a *pegada* que deixa sobre um chão de terra molhada, também uma *communicação* não é confundível com os documentos que dela subsistam e que dela ofereçam testemunho: estes podem permitir reconstruir os processos de que são consequência, mas não se confundem com eles.

A tutela constitucional conferida pelo n.º 4, do artigo 34.º, da Constituição da República Portuguesa, é evidente, respeita *exclusivamente* à primeira, não aos segundos, o que, claro, não significa que não beneficiem de outras formas de proteção constitucional, como adiante veremos.

10.4. A Tecnologia de Correio Eletrónico e Sistemas análogos

10.4.1. Um primeiro ponto que importa reter é que a tecnologia de correio eletrónico não pode e não deve ser entendida *apenas* como um meio de telecomunicação. Esta é apenas uma das utilidades que oferece ao utilizador, mas não é, sequer, a mais importante e a que introduziu maior disruptão na organização da vida moderna. Por outro lado, e ao contrário do que se conceptualiza sobre o sistema, a *telecommunicação* não é serviço prestado por *webmail account providers* aos subscritores



363
R

TRIBUNAL CONSTITUCIONAL

dos seus serviços e estes não podem, por isso, ser entendidos como *velhos ou executores* de processos comunicacionais realizados por terceiros (autor e destinatário de uma mensagem eletrónica).

Na verdade, a maior e principal valência que decorre da subscrição de uma conta de correio eletrónico reside no benefício de acesso a uma poderosa plataforma de arquivo remoto mantida pelo *webmail account provider*, que se constitui depositário do espólio de documentação de mensagens do aderente, sem o privar de poderes de consulta e de gestão personalizada. O operador oferece a qualquer pessoa a possibilidade de se aliviar de dossiers, armários e outras peças de mobiliário para organizar, manter e governar o seu histórico de comunicações escritas (eletrónicas) com terceiros, preservando e controlando todo o acervo de informação em servidores remotos e permitindo o seu acesso, individual ou por uma pluralidade de utilizadores, a partir de qualquer ponto do planeta.

Neste contexto, os sistemas de interface de webmail disponibilizam, hoje em dia, recursos e funcionalidades específicas para a ordenação e gestão dos documentos, sejam eles pastas, subpastas, *tags* e outras formas de catalogação. Este arquivo remoto, note-se, não é uma circunstância incidental, nem pode ser entendido como *instrumental ou inerente* à utilização desta ferramenta, antes corporiza o serviço de facto fornecido pelo operador de correio eletrónico: é da maior utilidade para o utilizador e é absolutamente peculiar, face a outros modelos tecnológicos.

Denotativo do que se disse, veja-se que a empresa *Microsoft* disponibiliza a cada subscriptor na sua plataforma *Hotmail* 15 GB de memória em servidor para armazenamento de correio eletrónico (support.microsoft.com) e a mesma capacidade é oferecida pelo serviço *Gmail* que a *Alphabet* distribui para subscrição universal e gratuita (one.google.com). Tratando-se, talvez, das plataformas de webmail mais difundidas, não será ousado afirmar que será este o *benchmark* da indústria a este respeito. A plataforma *Gmail* comercializa também um serviço *Premium* que facilita ao cliente um espaço de memória acrescido, de 100 GB, que, anuncia-se, atingirá em breve 1 TB.

Como é óbvio, esta dantesca capacidade de armazenamento não se explica pela necessidade de reter em memória os ficheiros a título transitório, enquanto se realiza o fluxo de comunicação entre remetente e destinatário. É dizer, este volume de memória disponível não é condição, nem instrumento, do desempenho de uma função de telecomunicação. Uma mensagem *SMS* (*Short Message System*), por exemplo, oferece nada mais que 116 bytes de memória ao utilizador, o que foi o bastante para que se tornasse um dos meios de comunicação mais utilizados do globo. O envio de certo tipo de ficheiros reclama por maior capacidade (v. g., vídeos, fotografias, etc.), mas, para



370
CR

TRIBUNAL CONSTITUCIONAL

cada email (ou seja, para cada fluxo de informação), *Hotmail* e *Gmail* não disponibilizam mais de 25 MB a título de capacidade de envio, um drástico contraste com a memória de arquivo oferecida.

A *Comcast Corporation, LLC* (Xfinity), a terceira maior operadora de telecomunicações dos EUA (2023), estima que um email de texto tenha por dimensão média 0,035 MB, uma mensagem instantânea 0,024 MB e um e-mail com anexos (folhas de cálculo Excel ou textos Word) 0,2 MB (xfinity.com). Isto significa que cada conta *Hotmail* e *Gmail* de utilização gratuita e universal (ou seja, mesmo deixando de parte produtos especializados ou Premium) atribui ao utilizador capacidade suficiente para armazenar em servidor e em permanência 42.667 mensagens instantâneas, 29.257 emails de texto ou 5.210 emails com anexos associados. Está bom de ver, se cingidas à operacionalização do envio e receção de mensagens de correio eletrónico, estas superestruturas dir-se-iam *grosseiramente excessivas*, importariam uma despesa de aquisição e de gestão para o operador injustificáveis e seriam inúteis, em absoluto, para os subscritores do serviço.

Noutro sentido, o poder de armazenamento dos servidores caracteriza, como começámos por dizer, instalações fixas destinadas a servir o arquivo permanente da correspondência digital do universo de utilizadores, não (apenas) a viabilizar trocas de comunicação entre eles. Este serviço é, pois claro, associável à função de telecomunicação, mas consubstancia a principal (e autónoma) prestação oferecida pela empresa a quem com ela contrate a instalação de uma conta de email.

10.4.2. A prestação típica das operadoras de serviços webmail reside, pois, na disponibilização ao subscritor de um arquivo de correio eletrónico nos seus servidores, mas esse serviço depende ainda que os operadores organizem um sistema apto à receção da informação enviada por remetentes de emails e que, bem assim, permita ao subscritor aceder a ela.

Se se pretender um exemplo análogo fora do ambiente digital, podemos imaginar uma empresa que se dispõe a ceder dada volumetria num gigantesco armazém para arrumação de cartas e outra correspondência de clientes interessados em ali sediarem o seu arquivo de correio postal recebido e enviado. Estando a transferência da informação confiada aos serviços postais, a empresa terá, sendo assim, de organizar nas suas instalações gabinetes dedicados à recolha e processamento da correspondência à chegada (proveniente do subscritor ou de quem a ele dirija missivas), a selecionar a correspondência que deva ser transferida para outros destinatários e, também, a garantir o acesso pelos subscritores do serviço às cartas em arquivo que lhes dizem respeito.

321
K

TRIBUNAL CONSTITUCIONAL

No serviço webmail, estes processos de gestão dos *inputs e outputs* de informação são assegurados por programas automatizados que organizam a associabilidade dos servidores de diferentes operadores webmail, entre si e com os sistemas locais dos utilizadores. Tendo em vista perceber como se processam estas operações no âmbito do webmail e melhor distinguir as funções de arquivo e de comunicação em que o sistema, visto na sua globalidade, se desdobra, importa realizar uma abordagem aos protocolos que operacionalizam a gestão de dados, já que daqui se receberão subsídios importantes para a boa compreensão da realidade colocada e, por inerência, para perceber os espaços de proteção por direitos fundamentais, a que nos dedicaremos *infra* (v., sobre o que diremos, M. T. BANDAY, *Techniques and Tools for forensic Investigation of E-Mail*, *International Journal of Network Security & Its Applications* (IJNSA), Vol. 3, n.º 6, Nov. 2011; L. LAZIC, *Techniques and Tools for forensic Investigation of one Court Case*, in *Journal of Information Technology and Applications*, 2018, pp. 63-74).

A tarefa a este respeito está simplificada, já que, em resposta à proliferação de empresas no setor e à necessidade de assegurar a cooperação entre uma pluralidade de *account providers*, a indústria global uniformizou os modelos que regulam as operações de transferências de dados no correio eletrónico. Quanto à organização dos fluxos entre servidores e subscritores de contas de serviço webmail (processos de extração), importa conhecer os protocolos POP (*Post Office Protocol*) e IMAP (*Internet Message Access Protocol*) e, no que respeita aos fluxos entre servidores (ou seja, entre plataformas de webmail – processos de envio), o protocolo SMTP (*Simple Mail Transfer Protocol*).

Começando por este último, o SMTP surgiu em resposta ao crescimento do público consumidor de webmail e tendo em vista a implementação de um modelo que coordenasse os sistemas dos diversos *webmail account providers* ao nível horizontal da estrutura, integrando dois módulos de tarefas nos servidores de cada operador. Pretendeu-se, assim, obter a otimização da operacionalidade global do sistema por via da melhor distribuição de funções operativas.

O modelo SMTP inicia-se com a receção dos dados enviados por um subscritor do serviço (*mail user agent* – «remetente@servidorremetente.com») no módulo recipiente (*mail submission agent*) do servidor com quem o primeiro subscreveu o serviço de correio eletrónico («@servidororigem.com»). A informação é depois transferida (*relay*) para um segundo módulo, que se ocupa da localização do servidor da conta de destino (*mail transmission agent*) indicado pelo remetente da mensagem («@servidordestino.com»). A informação é então transmitida pela internet para o módulo de receção deste segundo servidor (*mail exchanger*) e, daí, para um segundo módulo no seu sistema (*mail delivery*



TRIBUNAL CONSTITUCIONAL

agent), que permitirá a extração de dados a partir da conta de destino («destinatário@servidordestino.com»).

Implementando este modelo de cooperação entre estruturas de exploradores de plataformas, o SMTP permitiu a massificação do webmail, evitando sobrecargas nos sistemas e dificuldades colocadas pelos limites de memória operativa face ao elevado volume de solicitações.

Já no que respeita a protocolos de extração da informação (ou seja, aos processos de transmissão de dados *de servidores para utilizadores*), o POP foi desenvolvido num período em que a internet conhecia importantes limitações técnicas quanto à largura de banda, já que a rede era essencialmente constituída por linhas telefónicas de capacidade condicionada (ligações *«dial up»*).

O protocolo caracteriza-se por realizar a transmissão de blocos significativos de informação no momento inicial da ligação do utilizador à rede do seu servidor, relegando as tarefas de gestão da correspondência em interface (v. g., visualização e edição de mensagens ou *drafts*, anexação de ficheiros, etc.) para ambiente *offline*, ou seja, sem ligação à internet. Este modelo – em desuso, mas ainda com algum curso ao tempo corrente –, minimiza as necessidades de largura de banda sem perturbar a operacionalidade do serviço, já que todas as funcionalidades, salvo a extração de dados do servidor, são realizadas localmente, utilizando apenas os recursos do sistema do utilizador.

Já o IMAP operacionaliza um modelo de extração da informação que assenta num diálogo permanente entre o servidor e o sistema do utilizador, repartindo tarefas entre ambos. Ao invés de proceder à extração da informação à cabeça e em bloco (à semelhança do POP), o IMAP implementou um sistema *dinâmico* e em constante atualização via internet, que operacionaliza a transmissão *gradual* da informação para o sistema local em função de solicitações do utilizador.

Aquando do acesso ao interface de caixa postal, é transmitido apenas um conjunto moderado de dados (v. g., listagem de mensagens; geralmente também com indicação de alguns dados sumários, seja conta de origem, assunto indicado pelo autor, data de envio, denominação de ficheiros anexos, etc.), ficando a extração integral da informação (*maxime*, conteúdos) dependente de comandos subsequentes. O protocolo permite também a receção de novos pacotes de dados oriundos do servidor enquanto se trabalha *online* pelo *refresh* da página do *browser* ou da aplicação.

Assim, e ao contrário do arquétipo do protocolo POP, no IMAP os recursos do aparelho do utilizador são utilizados gradualmente e em coordenação com o sistema do servidor (*online*), recebendo e fixando informação no dispositivo na medida em que aquele lhe reconheça utilidade.

377
T

TRIBUNAL CONSTITUCIONAL

10.4.3. O exposto permite-nos já concluir pela existência de um conjunto de diferenças conceptuais inconciliáveis e abissais entre o serviço de webmail e o serviço de correio postal.

Neste último, a mensagem é envelopada ou encerrada noutro tipo de contentor, deixando-a inacessível ao operador de telecomunicações e tem por único recipiente o destinatário da mensagem: a empresa de correio postal opera meramente como *instrumento* das partes e simples *veículo* da mensagem, assegurando a deslocação do seu suporte físico entre dois pontos no espaço.

Ao contrário, um email não é dirigido, nem remetido, pelo autor da mensagem ao pretendido destinatário, mas ao operador com quem este último contratou o serviço de arquivo digital. O *webmail account provider* terá acesso ao conteúdo da comunicação, procederá ao seu armazenamento na sua estrutura como estipulado nas condições de serviço e torná-la-á acessível ao destinatário do conteúdo pela faculdade de extração da informação compreendida no sistema. Esta faculdade consiste, como vimos, na possibilidade de gerar um segundo fluxo de dados (comunicação), este do servidor para o aparelho do subscritor de destino, mas, como se vê, não se trata de um processo indissociável da lógica inerente ao serviço de correio eletrónico: este último fluxo pode, ou não, vir a ocorrer, em função da vontade e disponibilidade do utilizador, cuja decisão de gestão do seu arquivo remoto poderá consistir em *ignorar perpetuamente* a informação acumulada.

Vendo melhor, na preparação inicial do email pelo remetente, a indicação que se realiza para a *«morada»* de destino da mensagem de correio eletrónico desde logo identifica como ponto de chegada do fluxo de informação (prestes a iniciar-se) o servidor a quem o destinatário da mensagem atribuiu esta função de arquivo. O ponto de chegada é ilustrativamente designado na linguagem oral pela preposição inglesa *«to»*, identificadora de uma *localização* (v. g., «@servidor.com»). Na indicação de destino é também incluída, não qualquer elemento de identificação pessoal do indivíduo a quem a mensagem se dirige, mas a designação por que o *email account provider* reconhecerá a conta de um dado subscritor (v. g., «destinatário@») tendo em vista a indexação da informação, ou seja, para que lhe seja possível associar a informação recebida a dada conta.

A informação assim transmitida ficará depositada no servidor e não é correto afirmar-se que *«está em trânsito»*, em *«hibernação»*, ou que aguarda por qualquer outra operação para ficar completa. Como dissemos, ao operador fica conferida a *obrigação* e o *direito* de armazenar a informação destinada à conta do subscritor e esse processo fica *finalizado* neste ponto, assim no

374
R

TRIBUNAL CONSTITUCIONAL

âmbito da funcionalidade de arquivo a que responde a capacidade de memória em servidor alocada a cada conta de correio eletrónico (o que acima comparámos ao *outsourcing* de arquivo postal).

O interesse do *webmail provider* reside, precisamente, no controlo sobre a informação que lhe é conferido nestas condições: a par da exposição de utilizadores a anúncios publicitários, a grande fonte de receita das empresas gestoras de plataformas de webmail reside na pesquisa de informação nas mensagens de utilizadores (por eles enviadas ou a eles destinadas) através de programas automatizados, tendo em vista sinalizar perfis de consumidor e hábitos de consumo; a venda desta informação a empresas comerciais permite a estas últimas direcionar anúncios publicitários e promover campanhas de marketing de forma mais eficiente, viabilizando a monetarização de serviços webmail de subscrição gratuita. Por contrapartida, mas ilustrando também a função de arquivo desempenhada pelo operador, a este não é permitido eliminar a mensagem armazenada («apagar» o ficheiro) depois de dela obter os dados que interessam à sua atividade. Ainda que lhe fosse vantajoso fazê-lo (v. g., para aliviar as necessidades de recursos de memória em servidor, dispendiosos em estrutura e manutenção), porque o vínculo do *webmail account provider* reside na disponibilização do espaço em servidor necessário ao arquivo de correio digital, é ao subscritor que cabe decidir se mantém ou elimina dados, para o que o sistema lhe disponibiliza ferramentas que não carecem sequer da intervenção do operador para execução.

O facto de o *account provider* revestir a natureza de uma pessoa jurídica e de adquirir posição de gozo sobre a informação, utilizando-a em seu proveito próprio, achando-se em posição de exercer poderes de facto sobre a mensagem e o ficheiro de suporte, caracteriza-o da perspetiva subjetiva como *destinatário* destes fluxos, geradores de um banco de dados que constitui seu ativo imaterial. É, aliás, perante esta peculiaridade que emergiu uma tendência para impor a empresas titulares de servidores obrigações de fiscalização da atividade dos seus clientes e a criação de canais de cooperação com autoridades, isto ao abrigo de um princípio geral de *accountability empresarial* (v. *Guide for Establishing Law Enforcement Cooperation with Technology Companies in Countering Terrorism*, United Nations Office of Counter-Terrorism, The International Criminal Police Organization, 2023). Estes sistemas são muito utilizados para armazenar e difundir informação associada a atividades criminais ou terrorismo, de que a empresa se pode tornar cúmplice pela inação (*enabling*). A vinculação de empresas exploradoras de webmail e de outras plataformas digitais de difusão de informação a sistemas de *compliance* e à observância de canais de colaboração com autoridades, nacionais e



TRIBUNAL CONSTITUCIONAL

internacionais, vem impondo a organizações de delinquentes a reorientação das suas políticas de ação e de propaganda, recorrendo a sistemas que não importem alojamento em servidor ou recorrendo à alternância sucessiva entre plataformas (v. C. BOCKSTETTE, *Jihadist Terrorist Use of Strategic Communication Management Techniques*, Marshall Center Occasional Paper, n.º 20, Dez. 2008).

Em paralelo, a partir do momento em que a informação fica depositada no servidor, é possível a todos os que disponham de acesso à conta de destino (`<destino@servidor.com>`) acederem ao sistema e solicitarem ao operador o envio da informação (*upload*), tendo em vista recebê-la (*download*) no respetivo aparelho eletrónico (computador, *smartphone*, etc.), isto para que lhes seja possível tomar conhecimento do conteúdo e processar os dados pela forma que entendam. Como dissemos, este é um segundo fluxo de informação (*extração*), agora entre o arquivo (servidor) e o subscritor, que depende da iniciativa deste último e cuja relação com o primeiro é *conjuntural*, já que não lhe oferece continuidade, nem com ele se confunde. Pense-se em contas de correio eletrónico abandonadas (v. g., por advento de melhor fornecedor), esquecidas (v. g., o utilizador não recorda o nome atribuído à conta de cliente, ou a palavra-passe escolhida) ou que, por qualquer outro motivo, passaram a ser alvo de desinteresse pelo subscritor. Embora as mensagens permaneçam preservadas no servidor de acordo com o modelo de arquivo estipulado na adesão ao serviço, esses conteúdos *jamais* serão objeto de fluxo de extração, sem que por isso se possa falar de comunicações incompletas, já que atingiram, em efeito, o destino a que foram dirigidas (`<@servidordestino.com>`).

Também será bom notar que, ao contrário do que sucede com o correio postal, em todo este conjunto de operações só podemos falar de *portento de uma mensagem* em sentido impróprio, ou *alegórico*, se se preferir. Isto porque um manuscrito enviado por carta, de facto, realiza uma *viagem*, um trajeto pelo espaço: uma carta abandona as mãos do remetente, que dela se vê despojado, transita entre colaboradores dos serviços postais, seus edifícios e meios de transporte, e, quando sai do poder destes últimos com a entrega, cai sob domínio exclusivo do destinatário.

Este fenómeno de *alternância no domínio de facto* do suporte físico da mensagem, sem que com isso se confira acesso ao conteúdo a terceiros à comunicação – que caracteriza uma forma de controlo precário da informação em trânsito –, em *nada* se assemelha ao serviço de correio eletrónico: este caracteriza-se, já o sabemos, pela *duplicação e fixação* sucessivas dos dados, conferindo aos operadores acesso e domínio, próprio e direto, sobre a informação que corporizam.



35
8

TRIBUNAL CONSTITUCIONAL

Ao preparar uma mensagem num sistema local (mediante interface web ou aplicação), o aparelho local gera um conjunto de dados que são retidos pela memória operativa do processador (RAM) e remetidos via web para os computadores do servidor. No ponto de destino, este agrupa e reconstrói a informação num ficheiro digital, que armazena em disco rígido (*server hard drive*).

Quando o subscriptor da conta de destino aciona o fluxo de extração da mensagem indexada à sua conta, o sistema *reproduz* a informação constante do ficheiro memorizado e remete-a pela web, mantendo o controlo e disponibilidade sobre o ficheiro que, inicialmente, resultou do primeiro processo de comunicação. Recebida a informação no aparelho do utilizador pelo segundo fluxo de informação, esta é então armazenada em disco rígido, resultando viável a reconstrução do conteúdo da mensagem por um programa que a exibe ao utilizador em forma assimilável pelo sistema cognitivo humano. É a este *meio interface* que se pode chamar «*caixa postal virtual*».

Será de sublinhar, uma vez mais, que, como vimos quando descrevemos o protocolo SMTP, participarão nos fluxos de informação diferentes servidores sempre que o *webmail account provider* do autor do conteúdo da mensagem e o seu destinatário não seja o mesmo. Quando assim suceda (como será, em boa parte dos casos), os dados do email permanecerão em arquivo tanto na estrutura do servidor do remetente (arquivo de correio *enviado*), como nos dispositivos do servidor utilizado pelo destinatário final (arquivo de correio *recebido*), que entre si trocarão também um fluxo de informação, autónomo face aos realizados com os titulares das contas, tal como se explicitou.

Como está bom de ver, o processo próprio ao correio eletrónico não possui nenhuma semelhança com o serviço de correio postal, que transporta «*uma única carta*» do ponto “A” até ao ponto “B”, caracterizando uma única operação de telecomunicação. No correio eletrónico, a informação é transmitida múltiplas vezes entre aparelhos mediante jatos intermitentes de energia que, processados como “00” e “11” por microprocessadores por (uma de entre várias) linguagem binária, permitem a *replicação e memorização* do conteúdo transmitido em todos os dispositivos envolvidos no sistema. Existe, pois, e de uma parte, uma *multiplicidade* de ficheiros contendo toda a informação da mensagem e, de outra, também uma pluralidade de remetentes e de destinatários envolvidos neste processo – tantos quantos os fluxos de comunicação realizados –, todos eles com acesso e conhecimento irrestrito aos dados transmitidos e todos eles os arquivando para satisfação de uma carteira de interesses, próprios e de terceiros, de forma independente face aos demais.

~~SECRET~~



TRIBUNAL CONSTITUCIONAL

Em suma, os operadores de plataformas webmail não podem ser considerados intermediários ou transportadores das mensagens de correio eletrónico e tanto menos são equiparáveis às empresas de serviços postais. Ainda que o conteúdo comunicado seja referente a outras pessoas, a estrutura do sistema, o poder e controlo que lhes é conferido sobre a informação e a função de armazenamento a que estão adstritos, impõe que se entendam, num patamar do processo, como *destinatários* de comunicações e como *autores* de comunicações (consoante o fluxo de informação que se considere, de envio ou de extração); e, noutro, como *depositários* da informação transmitida, por conta e no interesse dos subscritores do respetivo serviço webmail e para satisfação de uma carteira de interesses própria, essencialmente de angariação de receita.

10.4.4. Aqui chegados, importa acrescentar uma outra nota, agora para os sistemas de mensagens instantâneas (*WhatsApp*, *Messenger*, *Telegram*, *We Chat*, etc.) a que se reporta também a Diretiva ECN+ e a norma fiscalizada, também porque estes adquiriram grande notoriedade na última década e porque constituem um sistema análogo ao webmail em escopo e operacionalidade.

Quanto a estes, porque o modelo não envolve a necessidade de colaboração entre mais do que um fornecedor do serviço, a indústria digital não sentiu necessidade de uniformizar protocolos e é por isso frequente que cada operador desenvolva a sua própria tecnologia de processamento da informação para transmissão via web, que resulta, assim, exclusivo para cada uma das aplicações comercializadas [são disso exemplo os protocolos *MQTT* (*Message Queuing Telemetry Transport*), *AMQP* (*Advanced Message Queuing Protocol*), *DDS* (*Data Distribution Service*), *XMPP* (*Extensible Messaging and Presence Protocol*), etc.]. Embora existam algumas diferenças técnicas entre os protocolos desta vasta constelação, é possível reconduzi-los a dois modelos essenciais.

No primeiro, o protocolo operacionaliza as trocas de informação entre o remetente da mensagem, o servidor (fornecedor do serviço de mensagens instantâneas) e o destinatário final, desdobrando o processo em fluxos de *envio* e de *extração*, assim de forma muito aparentada ao webmail e de acordo com uma lógica triangular em tudo semelhante. Este processo importa também o registo da informação em servidor e impõe o inerente acesso aos dados pelo operador do serviço, mas não implica a troca de informação entre mais do que um *service provider*, já que os fluxos de comunicação têm lugar no sistema de uma única entidade, com quem tanto o autor como o destinatário do seu conteúdo contrataram e cujo produto digital é por ambos utilizado.

378
R

TRIBUNAL CONSTITUCIONAL

No segundo modelo, o *service provider* opera apenas como «ordenador» dos aparelhos dos utilizadores, ocupando-se da sua «sincronização», de modo a que seja possível a troca de informação diretamente entre eles. Os fluxos de dados, neste caso, realizam-se *exclusivamente* entre aparelhos de utilizadores (*peer-to-peer*), pelo que todas as tarefas de preparação, transferência e processamento ulterior de mensagens recebidas são realizadas localmente pelos respetivos dispositivos (de autor e destinatário do conteúdo da mensagem), sem facultar ao operador acesso à informação trocada em nenhum momento, que por esse motivo, pois claro, não a armazena nos seus servidores.

Algumas aplicações de *instant messaging* combinam estes dois arquétipos, utilizando o primeiro para trocas de informação menos exigentes quanto a memória (v. g., mensagens de texto) e deixando as que reclamam por maior capacidade (v. g., chamadas de vídeo ou de voz) para o modelo *peer-to-peer*, aliviando as necessidades de hardware sem perdas de operacionalidade.

Também por aqui se ilustra, note-se, que a gravação de informação por *webmail account providers* não é coeva ao sistema de mensagens web, antes constitui uma opção destinada a viabilizar a prestação de serviço de arquivo que é típica do produto fornecido por operadores de webmail. Nada impediria que *todos* os fluxos de informação fossem realizados *peer-to-peer*, prescindindo da existência de registo em servidor. Isto, claro, com a contrapartida de, a ser assim, resultar inviável o acesso à informação por mais do que um utilizador e a partir de qualquer terminal ligado à web, já que o sistema imporá que todo o armazenamento de comunicações fique reservado *exclusivamente* a um dispositivo local. Esta opção também não admite a monetarização do acesso a conteúdos pelo *service provider*, que terá de encontrar outras formas de extraír rendimento do serviço que presta.

Com relevo para a análise que faremos, importa ainda acrescentar mais duas notas.

Em primeiro lugar, deixamos impresso que, ao contrário do que sucede com o correio postal, a tecnologia webmail não depende *necessariamente* da intervenção de fornecedores externos.

Existe um numeroso conjunto de empresas e de instituições que dispõem dos seus próprios servidores, integrando equipamentos, software e equipas de técnicos na sua estrutura que lhes permitem desempenhar internamente todas as funções necessárias à implementação de um serviço de correio eletrónico (na gestão de fluxos de comunicação e em arquivo) em tudo semelhante ao fornecido por empresas de tecnologia digital no que tange a generalidade dos utilizadores (quer estes possuam domínio próprio, quer não) e, em especial, às contas webmail de uso universal.



TRIBUNAL CONSTITUCIONAL

Um email enviado e recebido entre colaboradores de uma empresa dotada de serviço webmail próprio (exemplificando, de «*diretor1@empresa1.pt*» para «*diretor2@empresa1.pt*») não envolve a intervenção de entidade terceira nas operações próprias ao correio eletrónico, tanto menos o armazenamento em servidor, cingindo-se todas elas à internalidade da empresa e à sua estrutura de meios em todas as vertentes colocadas (*diretor1/servidor da empresa1/diretor2*).

De forma idêntica, um email enviado e recebido entre colaboradores de duas empresas que utilizem, ambas, serviços webmail próprios (de «*diretor3@empresa2.pt*» para «*diretor4@empresa3.pt*»), circula exclusivamente entre as esferas de controlo destas duas entidades (*diretor3/servidor da empresa2/servidor da empresa3/diretor4*). Também neste caso, não existirá intervenção de *webmail providers* nas operações: porque os processos de webmail não envolvem terceiros, o exercício de controlo e domínio sobre a informação ficará circunscrito às empresas protagonistas das trocas de dados, à semelhança de qualquer outro componente das respetivas estruturas de estabelecimento.

Como segunda nota, será também importante assinalar que a tecnologia utilizada na troca e armazenamento de informação webmail encontrou aplicação em outras áreas de atividade, levando à criação de ferramentas de gestão e de contabilidade que aplicam os mesmos modelos.

Da mesma forma que o advento da web permitiu dispensar arquivos de correspondência, a mesma solução técnica vem sendo hoje aplicada em produtos destinados a organizações empresariais com o escopo de substituir livros de contabilidade e arquivos de evidência (documentos de suporte de lançamentos) em instalações, facilitando a consulta (que passa a ser possível por qualquer colaborador a partir de qualquer terminal web) e aliviando as necessidades de ativo imobilizado destinado ao arquivo de documentação do operador económico.

A *contabilidade digital ou colaborativa*, a que agora nos referimos, tem vindo a generalizar-se e a ganhar espaço no mercado das ferramentas de serviços financeiros e de assessoria, e caracteriza-se por criar um depósito em servidor gerido por uma entidade terceira (*cloud*) de toda a informação contabilística e de gestão de uma empresa. Neste sistema, os lançamentos e o processamento da contabilidade são realizados localmente pelos colaboradores a partir de uma rede de terminais (pense-se em empresas com vários centros de custos dispersos), procedendo-se depois à transferência da informação via web para os servidores do fornecedor do serviço.

O acervo contabilístico da empresa (que é dizer, o universo completo de documentos de registo das operações económicas que realiza), assim armazenado nos computadores do *service*



TRIBUNAL CONSTITUCIONAL

provider, pode ser acedido em qualquer altura a partir de terminais mediante a solicitação de fluxos de extração e por todos a quem esteja conferida autorização de acesso (v. g., administradores, escriturários, contabilistas, etc.), tudo isto de forma identificável com a tecnologia webmail.

Ainda que a informação confiada ao *service provider* não se destine a uma entidade externa à empresa subscritora do serviço (o que, como acima vimos, igualmente não sucede em serviços de webmail internos), todas as trocas de informação coevas ao sistema *cloud* são realizadas entre duas esferas de controlo diferentes (a do utilizador do serviço e a do respetivo fornecedor) e o objetivo funcional do produto reside em permitir que os colaboradores da empresa troquem informação entre si pela partilha de uma plataforma de arquivo contabilístico acessível a todos eles.

Em cada um dos fluxos originados no interior deste sistema fica caracterizado, pois, o *processo de comunicação* em condições indistinguíveis face ao serviço webmail, apenas com a especialidade de se tratar do ambiente específico da gestão e contabilidade de empresas e agentes económicos. Isto significa que a proteção que se entenda conferível ao webmail enquanto instrumento tecnológico característico da era digital importará tratamento *a priori* para as ferramentas de gestão contabilística em *cloud* (e outras semelhantes), o que bem ilustra a dimensão do erro na assimilação do webmail ao serviço postal ou a qualquer tecnologia que se cinja a telecomunicação.

10.4.5. Como vimos acima, os *webmail account providers* ocupam-se do arquivo da informação trocada por utilizadores de correio eletrónico e da coordenação de fluxos de envio e de extração relativos à conta do subscritor do seu serviço. Estas trocas de informação consistem na reprodução e envio pela web de dados contidos em ficheiros digitais e as operações por eles realizadas caracterizam-se pela assunção do papel de *autor* ou de *destinatário* de fluxos de comunicação, já que *não são* eles próprios que gerem os canais por que a informação é comunicada, nem executam as transferências de dados. Porque assim é, e tendo em vista completar a panorâmica pelo sistema webmail, impõe-se conhecer agora o processo técnico que permite a computadores (e a redes locais de computadores) comunicarem entre si, percebendo de que forma a informação é transmitida pela arquitetura de fibra ótica a que chamamos internet e a identidade de quem o realiza e o governa.

O desempenho desta função incumbe aos *Internet Service Providers* (ISP), empresas que asseguram a ligação à estrutura de rede dos terminais de *utilizadores* – neste conceito se incluindo, como é evidente, os servidores e as empresas exploradoras de plataformas de correio eletrónico –



38
R

TRIBUNAL CONSTITUCIONAL

e que executam, monitorizam e gerem os fluxos de energia pelas redes (entre nós, pense-se na Vodafone, na Meo-Altice, na NOS, etc.). Toda a informação em trânsito é governada por estas entidades e fica sob seu controlo: iniciado um fluxo em dado terminal (computador, smartphone, etc.) pela operacionalização de protocolo [geralmente, *Hyper Text Transfer Protocol* (HTTPS), mas, tratando-se de correio eletrónico, também aqueles de que falámos *supra*], a informação é encaminhada para o terminal de destino mediante trânsito por grandes complexos de servidores do ISP (*datacenters*) que realizam as ações que importam à execução dos fluxos de informação.

Ao ISP é conferido também *acesso* à informação transmitida, única forma de lhe ser possível executar o seu trânsito entre pontos de origem e de destino e, bem assim, de gerir a rede, apercebendo-se de nós de congestionamento e reagindo pela moderação de desempenho (*trottling*) com o objetivo de promover o bom funcionamento, global e integrado, de todo o sistema.

Esta cedência de controlo sobre a informação aos ISP, imprescindível ao tráfego pela internet e dele incindível, se os converte em algo próximo a um «*Big Brother Orwelliano*» pela acessibilidade conferida a *todos* os dados que percorrem a web, não significa, porém, autorização para a gravação ou utilização de conteúdos: os ISP assumem-se como *encaminhadores* da informação transmitida, não participantes ativos nos processos de comunicação. Por esse motivo, os únicos dados que são de facto retidos pelos ISP são informações referentes à própria comunicação que executam e que gerem (ou seja, *metadados*), não os dados comunicados (ou seja, conteúdos), já que apenas os primeiros decorrem da (e são necessários à) função que desempenham no sistema e, também, porque seria inviável a fixação em hardware de toda a informação que flui pela internet.

De todo o modo e com o escopo de combater a permeabilidade a intrusão que decorre desta organização de meios, boa parte dos protocolos recorre a sistemas de *encriptação* de dados (como é o caso do HTTPS) antes do *upload*: a informação será convertida num ficheiro operável apenas *depois* de recebida no terminal de destino, através da respetiva ferramenta de desencriptação.

Isto significa que, quando existam ferramentas de encriptação em uso pelos autores da comunicação, o ISP apenas conhece e encaminha pela internet um conjunto de dados *desestruturado* e *incoerente*, mas *integral*, face à informação de fonte. No ponto de chegada, porém, este conjunto permitirá reconstituir a mensagem preparada pelo remetente através do software instalado no terminal do destinatário, que este partilha com o remetente. Assim, pretende-se que da exposição

382
AR

TRIBUNAL CONSTITUCIONAL

e acesso aos dados que decorre da cedência de controlo sobre eles ao ISP durante o processo de transmissão pela internet não decorra a possibilidade de este conhecer o *conteúdo* transmitido.

Os ISP reconduzem-se, pois, a uma função de *executores* dos processos de comunicação, realizando o encaminhamento dos fluxos de energia pela internet processáveis por computadores, assegurando que a informação carregada (*upload*) chega ao destinatário pretendido e que o objeto da descarga (*download*) se identifica com os dados de origem, quer estes hajam sido encriptados, quer não. A função operacional dos ISP é, enfim, e em qualquer caso, a de meros *transmissores* da informação transmitida, de forma inteiramente semelhante às operadoras telefónicas tradicionais, cujos poderes e missão, está bom de ver, replicam no contexto das telecomunicações digitais.

Toda a informação que circula pela internet é transmitida desta forma: quer se trate de comunicação entre terminais ou servidores, originária de particulares ou de prestadores de serviços, independentemente da distância ou do volume de dados transmitidos, os ISP estarão encarregues da gestão e execução dos fluxos de energia que permitirão o processamento local da informação.

Temos, portanto, encontrada a identidade do *operador de telecomunicações* digital por excelência, que é dizer, a entidade em que todos os autores e destinatários de comunicações digitais – sejam eles particulares, instituições públicas, exploradores de plataformas de correio eletrónico, exploradores de serviços de contabilidade em *cloud*, empresas de vendas online, ou quaisquer outros protagonistas – se vêm na contingência de depositar confiança para que lhes seja possível *comunicar* pela internet, ou seja, trocar informação remotamente com alguém também conectado à rede.

11. A Apreensão de Mensagens de Correio eletrónico ao abrigo da Lei da Concorrência (artigo 18.º, n.º 1, alínea c), da Lei n.º 19/2012, de 8 de maio)

11.1. O artigo 18.º, n.º 1, alínea c), do RJdC, confere poderes à AdC para realizar dois tipos de ações no âmbito das suas competências de investigação e tendo em vista a instrução probatória de processos contraordenacionais por infrações ao Direito da concorrência: «*bustas e examem*», por um lado, e atos de «*recolha e apreensão*», por outro. Os primeiros consistem em atividades de pesquisa e de análise, ou seja, na procura e vistoria de objetos ou de lugares tendo em vista localizar elementos úteis à investigação; os segundos consistem na seleção e sujeição destes elementos a custódia pública, transferindo o domínio de facto sobre eles para a entidade investigadora.



TRIBUNAL CONSTITUCIONAL

Relativamente ao *objeto* das ações de recolha e apreensão, o artigo 18.º, n.º 1, alínea c), da Lei n.º 19/2012, de 8 de maio, circunscreve-o a “*documentos*”, ou seja, a qualquer tipo de suporte apto a reproduzir ou a representar um facto (artigo 362.º, n.º 1, do Código Civil), aqui se incluindo conteúdos em formato eletrónico, designadamente *ficheiros digitais* (Decreto-Lei n.º 12/2012, de 9 de fevereiro e § 35 do Reg. (UE) n.º 910/2014 do Parlamento Europeu e do Conselho de 23 de julho de 2014 – a norma indica ainda, expressamente, “*extratos da escrita*”, referindo-se a certos documentos que exibem informação contabilística já processada; o termo é exemplificativo e nada acrescenta à noção).

Estes poderes são passíveis de exercício em todos os espaços e superfícies que se integrem no estabelecimento da entidade sujeita à ação da AdC (“*instalações, terrenos*”) e, bem assim, nos equipamentos que possam ser utilizados para a sua transferência entre locais (“*meios de transporte*”), desde que, em qualquer dos casos, estejam sob domínio da entidade buscada, integrando-se assim na sua estrutura de empresa. As diligências de busca poderão ser efetivadas, enfim, em quaisquer espaços que, sob controlo e domínio da pessoa jurídica visada, constituam componentes da sua estrutura de meios, circunscrevendo-se a ação invasiva à internalidade da sua esfera jurídica.

Está bom de ver, o artigo 18.º, n.º 1, alínea c), da Lei n.º 19/2012, de 8 de maio, de modo nenhum capacita a AdC a realizar a *interceptação* de fluxos de comunicação para obtenção de prova, como não autoriza qualquer forma de aquisição de conteúdos que assente na extração de informação em trânsito pela exploração de vulnerabilidades de meios de telecomunicação. Admite-se, apenas, o acesso integral e pleno aos *elementos documentais do estabelecimento*, nada mais.

Em face do que vai dito, a norma permite que a AdC realize, como terá sucedido *in casu*, pesquisas com ferramentas informáticas em todos os dispositivos eletrónicos incorporados no ativo imobilizado da empresa que sejam aptos à fixação de informação digital (v. g., computadores, *smartphones*, *pendrives*, discos rígidos externos, etc.), tendo em vista localizar *documentos em formato eletrónico* (*ficheiros*) que contenham informação com interesse para o apuramento, julgamento e punição de práticas anticoncorrenciais. De entre eles, será possível localizar ficheiros contendo *mensagens webmail recebidas*, cuja presença nos aparelhos da empresa se explicará por uma de duas formas: ou foram previamente transferidos a partir de dispositivos locais (v. g., de uma *pen drive*, ligada ao aparelho por cabo); ou foram objeto de um fluxo de extração via web, que necessariamente estará *concluído* no momento da sua localização pela Adc aquando da busca.



TRIBUNAL CONSTITUCIONAL

38P
R

Na verdade, e chamando à colação o que expusemos, caso o serviço de webmail escolhido pela empresa utilize o protocolo POP (aos dias de hoje, pouco provável), terá existido um acesso por *browser* ou pela aplicação ao servidor que transferiu a informação de correio para o aparelho local, tendo em vista permitir o seu processamento *offline*. Se o serviço webmail da empresa buscada fizer uso do protocolo IMAP (o que, aos dias de hoje, será quase certo), isso significa que existiu uma ordem específica prévia à busca, pelo utilizador, de extração e transferência dos dados relativos à mensagem para o dispositivo onde foi encontrada. Como dissemos, o IMAP caracteriza-se pela gestão do correio em ambiente *online*, coordenando os sistemas de servidor e de terminal, razão por que cada uma das mensagens que se encontram no sistema local aquando da pesquisa terá de ter sido objeto de comando específico de *download* pelo utilizador, já executado aquando da busca.

Assim, e em qualquer uma das situações, a localização de mensagens eletrónicas no decurso de um exame realizado ao abrigo do artigo 18.º, n.º 1, alínea c), do RJdC e sua sujeição ao domínio da autoridade pública apenas respeitará a ficheiros integrados na estrutura da empresa em condições indistinguíveis face a quaisquer outros documentos (corpóreos) ou ficheiros digitais que se encontram nos seus arquivos, por isso sendo passíveis de apreensão em idênticos termos.

Como está bom de ver, os documentos ou ficheiros informáticos apreendidos nas descritas condições não exibem qualquer especial vulnerabilidade associável à utilização de meios de telecomunicação, já que se acham, em efeito, sob controlo do destinatário, à semelhança de qualquer outra evidência documental ou elemento da empresa. Os meios de defesa conferidos ao particular para manter reserva ou confidencialidade sobre estes elementos, são os mesmos de que beneficia quanto a quaisquer outros. Não sendo objeto de um fluxo de comunicação no momento em que opera a sua sujeição ao poder de uma autoridade pública, enfim, estamos de fom do âmbito de tutela conferido pelo artigo 34.º, n.º 4, da Constituição da República Portuguesa.

Em reforço, podemos convocar a experiência jurisprudencial germânica, que vem firmando conclusões neste sentido:

"[Ao] determinar o âmbito de proteção do artigo 10.º da Lei Fundamental [segredo da correspondência, correio e telecomunicações], o fator decisivo reside em saber se a situação é comparável com a de outra informação armazenada na esfera privada do utilizador, tal como o diretório do telefone pessoal criado pelo utilizador no seu aparelho, ou a informação armazenada no disco rígido do seu computador. A ser assim, não existem já riscos específicos associados ao processo de transmissão que estejam para lá do controlo e influência do utilizador. (...) "[a tutela das comunicações] serve para compensar a privacidade diminuída que resulta da utilização de tecnologia

385
CR

TRIBUNAL CONSTITUCIONAL

e para oferecer resposta ao risco inherent ao processo de transmissão, incluindo o envolvimento de entidade terceira (...). [e] está associada ao uso de um meio de telecomunicação. Depois de o destinatário ter recebido a mensagem, ele deixa de estar exposto ao risco acrescido da sua interceptação por terceiros – incluindo o Estado – que decorre do facto de as partes na comunicação não poderem controlar e monitorizar, na totalidade, o processo de transmissão. A partir daquele momento, a comunicação armazenada e os dados de tráfego não são distinguíveis (em termos de vulnerabilidade) de quaisquer outros ficheiros de informação criados pelos utilizadores da telecomunicação eles próprias.”.

[v. Acórdão do Tribunal Federal Constitucional alemão de 2 de março de 2006 (2 BvR 2099/04); também, v. B. SCHAFER e W. ABEL, *The German Constitutional Court on the Right to Confidentiality and Integrity of Information Technology Systems*, 2010, in Madhuri, V. (Ed.), Hacking, Icfai University Press, p. 113]

“[A] proteção a direitos fundamentais conferida pelo artigo 10(1) da Lei Fundamental não se estende aos conteúdos ou circunstâncias de telecomunicações armazenadas no domínio controlado por uma das partes na comunicação depois de a transmissão ter sido completada, já que estas podem adotar as suas próprias precauções contra acesso a dados reservados. Quanto a estes dados, os riscos específicos da comunicação à distância, que a privacidade de telecomunicações pretende prevenir, já não se aplicam (...). Da mesma forma, a proteção concedida pela privacidade de telecomunicações não se aplica se uma autoridade estatal monitoriza o uso de um sistema de uma tecnologia de informação enquanto tal, ou realiza pesquisas no armazém de ficheiros media do sistema”

[v. Acórdão do Tribunal Federal Constitucional alemão de 27 de fevereiro de 2008 (1 BvR 370/07, 1 BvR 595/07)]

Isto não é dizer que nenhuma ação de infiltração no sistema local possa caracterizar uma intrusão na tutela das telecomunicações, mas apenas que se impõe distinguir os casos em que a sujeição ao poder público da mensagem é realizada por via da interceptação de um fluxo de transmissão de dados (comunicação) de todos os demais, em que fica apenas em causa a apreensão de elementos em situação de repouso. Através de programas maliciosos (*malware*) ou pela alteração manual de configurações da aplicação de webmail mediante acesso não-autorizado, por exemplo, é possível a *duplicação de ações de envio* a partir do terminal de mensagens, gerando um fluxo com destino a um recipiente indesejado pelo utilizador sempre que este envie uma mensagem. É também viável reproduzir *fluxos de extração*, remetendo furtivamente conteúdos para outro ponto da web, sob controlo de terceiro, sempre que exista *download* de mensagens pelo utilizador.

Nestas situações, estaremos, sem nenhuma dúvida, perante intrusões em telecomunicações, pese embora a ingerência seja realizada no dispositivo local. O novo fator que se introduz e que justifica a diferente forma de proteção constitucional reside na instrumentalização, de forma específica, de fluxos de transmissão de dados para realização do aposseamento da informação por terceiro à comunicação. O que dá causa à transferência de controlo sobre a informação é, em si



TRIBUNAL CONSTITUCIONAL

386
de

mesma, a tentativa do autor de comunicar com dado destinatário, razão por que existe plena justificação para que intervenha a especial proteção conferida pelo n.º 4, do artigo 34.º, da Constituição da República Portuguesa: esta surge, precisamente, quando o *ato de comunicação* se torna um risco singular para a privacidade, como, está bom de ver, sucede nestoutro grupo de situações.

Pela mesma ordem de motivos, a extração de informação mediante monitorização de fluxos executados por ISP (*Internet Service Providers*) será qualificável como ingerência em telecomunicações em qualquer ponto da sua estrutura. Como vimos, os ISP asseguram a conexão entre computadores (ou entre redes locais) e executam a transmissão de dados entre eles, caracterizando a prestação própria de um serviço de telecomunicação, utilizado por autores e recipientes, para que seja possível trocar dados entre dispositivos. A monitorização da informação em gestão pelos ISP constituirá, pois, a vigilância de atos de comunicação sob tutela do artigo 34.º, n.º 4, da Lei Fundamental.

A norma fiscalizada não respeita, porém, a qualquer situação congénere. A busca a equipamentos eletrónicos e outro hardware da empresa esgota-se enquanto pesquisa por registos documentais na forma de ficheiros informáticos em elementos do ativo imobilizado da entidade buscada, razão por que não invade o perímetro de defesa da sobredita norma constitucional.

Alguma doutrina, muito crítica da jurisprudência iniciada pelo Acórdão do TC n.º 91/2023, já veio a terreiro para explicitar isto mesmo:

"Se o operador que intermediou a comunicação à distância já não tem qualquer domínio sobre ela, uma possível quebra da confidencialidade dessa comunicação passada não lhe será imputável, não havendo razão para desencadear a proteção que o princípio da inviolabilidade das telecomunicações visa garantir. (...) [não se justifica a intervenção do direito ao sigilo das telecomunicações] se a devassa for levada a cabo através de uma ingerência realizada directamente em equipamentos eletrónicos à guarda do titular dos dados, sendo esses dados recolhidos desses dispositivos ou a partir deles, como é prática habitual entre nós. Ainda que se trate de dados que já foram uma telecomunicação e que permanecem expostos a uma situação de perigo de devassa não é pela exploração dessa vulnerabilidade que o Estado deles toma conhecimento e se apodera. Por esse motivo, não se fazendo sentir a razão de ser que funda o direito à autodeterminação comunicativa não há motivo para que os dados assim recolhidos beneficiem da sua proteção e para que as intromissões que neles sejam promovidas pelo Estado sejam qualificadas como intervenções restritivas nesse direito fundamental"

(v. NUNO BRANDÃO, *op. cit.*, pp. 227-228)

Pelo exposto percebemos também por que motivo não é útil a sinalização que o *interface* de webmail atribua a dada mensagem na listagem que exiba em *display* ao utilizador, incluindo a descrita na dimensão normativa da artigo 18.º, n.º 1, do RjdC, a cuja fiscalização aqui procedemos. Quer a



TRIBUNAL CONSTITUCIONAL

387
X

mensagem esteja catalogada como «*aberta/lida*», quer como «*fechada/não lida*», em qualquer um dos casos a apreensão realiza-se sobre ficheiros contidos no sistema local do utilizador e que estão sob seu controlo, sendo indiferente o grafismo escolhido ou o que exprima para quem dele faz uso.

Ferramentas de *software* destinadas ao tratamento de mensagens e sinais cujo significado, de resto, depende da forma como cada utilizador interprete o *display* do interface perante si, são, a todos os títulos, inúteis para a caracterização do objeto da apreensão ao abrigo do disposto no artigo 18.º, n.º 1, alínea c), do RJdC, ou para definir a extensão da respetiva proteção constitucional.

11.2. A fiscalização da norma constante do artigo 18.º, n.º 1, alínea c), do RJdC, tal como foi interpretada pelo Tribunal “*a quo*”, impõe ainda se avalie outra forma de pesquisa e apreensão de mensagens de correio eletrónico que se permite por este mesmo programa normativo (sobre o que agora veremos, v. *Electronic Evidence Guide*, V. 2.1., Conselho da Europa, Divisão de Cibercrime, Diretorado Geral dos Direitos Humanos e Estado de Direito, 2020, pp. 81 e ss e 126 e ss; *International Standards, Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence*, ISO/IEC 2012, *maxime*, pp. 12 e ss).

Imaginemos que, durante uma operação de busca, a AdC é informada pelo representante da entidade buscada, depois de interpelado, que não mantém arquivo de correspondência postal (física) na sede, que essa função foi objeto de *outsourcing*. Toda a correspondência da empresa é dirigida e recebida num armazém noutra localidade pelos colaboradores de uma outra empresa, com quem este serviço foi contratado: aí, as cartas são desenvolvidas e arquivadas numa divisão de arrumos pelos trabalhadores da fornecedora; também aí são entregues todas as cartas preparadas para envio, tendo em vista recolha pelos serviços postais e reprodução por fotocópia destinada a esse arquivo. Isto, à semelhança do que sucede com outras entidades, que noutras divisões do armazém instalam os respetivos acervos de correio. A empresa fornecedora mantém o edificado e respetiva segurança, mas a entidade buscada dispõe de chaves para acesso direto à sua divisão e ao seu arquivo, pelo que lhe é possível levantar documentação em qualquer altura, sem necessidade de autorização ou de intervenção de qualquer pessoa, tudo em função da sua melhor conveniência.

Como se concordará evidente, as «*instalações da empresa*» a que se reporta o artigo 18.º, n.º 1, alínea c), do RJdC, como espaço vulnerável a buscas não se cingem a edifícios que sejam *propriedade* da entidade visada, mas compreendem todos os que se integrem na sua estrutura de meios, por



TRIBUNAL CONSTITUCIONAL

deles extrair as respetivas utilidades funcionais, independentemente do título jurídico que lhe haja conferido essa posição material (v. g., arrendamento, comodato, *leasing*, cessão de exploração, ou outros negócios atípicos). Ninguém duvidará que, na situação colocada e ao abrigo desta norma, a busca poderá ser realizada também na divisão de armazém alocada ao arquivo da entidade buscada, tendo em vista a apreensão de todos os documentos que possuam relevo para a investigação.

Ora, já se adivinha, o *webmail account provider* disponibiliza um serviço análogo ao desta entidade conjecturada e os documentos em formato eletrónico que se encontrem nos seus servidores acham-se nas mesmas condições. O histórico completo de comunicações digitais realizadas pelo titular da conta não se encontrará, em princípio, nos aparelhos que utilize para aceder à web à data da busca, já que estes aparelhos são substituídos com frequência. A isto acresce que a preservação de arquivo em hardware (v. g., através de discos externos, pendrives, CDs/DVDs, etc.) é dispendiosa, importa riscos de perda de informação pela degradação dos equipamentos e não permite o acesso à informação de qualquer lugar. O propósito de manter uma conta webmail é, já tantas vezes o repetimos, manter toda essa informação acessível através da web a partir de qualquer terminal, dispensando aparelhagem local destinada a armazenamento.

Isto significa que, à semelhança desta situação hipotética, também as buscas realizadas ao abrigo do artigo 18.º, n.º 1, alínea c), do RJdC, poderão incluir a pesquisa e apreensão de ficheiros de correio eletrónico que não se encontrem nos dispositivos locais da entidade buscada, mas armazenados nos servidores da plataforma webmail que utilize, sem que se por isso se invada o espaço de defesa constitucional das telecomunicações. Desde que seja possível esse acesso através do terminal da empresa visada, porque daqui decorre, do ponto de vista técnico, a restrição da pesquisa ao seu arquivo de webmail em servidor, cujo acesso direto e *online* lhe está conferido pelo sistema, não se coloca neste âmbito qualquer forma de invasão da autodeterminação comunicativa.

Na verdade, a informação armazenada nos servidores do *webmail account provider* não se acha em trânsito, trata-se de ficheiros fixados em discos rígidos que *previamente* foram objeto de um fluxo de transmissão de dados (*download*) protocolado pelo SMTP, de forma idêntica ao que sucede em aparelhos do subscritor por protocolos POP ou IMAP. A apreensão de ficheiros será realizada a partir do sistema local da entidade buscada e implica a realização de um fluxo de extração, mas que não se caracteriza como um processo de comunicação a que as autoridades fossem alheias. Para todos os efeitos, trata-se de utilizar o canal de acesso a documentos de que a entidade buscada

389
X

TRIBUNAL CONSTITUCIONAL

dispõe (sem necessidade de envolvimento de terceiros), em nada se assemelhando a uma operação de intercetação de fluxos de dados enquanto circulam entre autor e destinatário (v. DUARTE R. NUNES, *Os Meios de obtenção de Prova previstos na Lei do Cybercrime*, Gestlegal, 2.ª Ed., 2021, pp. 156-157; D. SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Almedina, 2017, pp. 133 e 139-140).

Por outras palavras, a AdC utilizará os recursos que a empresa buscada utilizaria para aceder ao seu arquivo digital, ou, se recuperarmos o exemplo *supra* indicado, fará uso da *chave* e da *porta* de que a entidade dispõe para aceder ao depósito de correspondência postal em *outsourcing*, nada mais.

Por isso se diz que a extensão de operações de busca a pesquisas a sistemas informáticos não-locais por via “*de um acesso remoto (ou, se quisermos, um acesso online) (...) não se pode apelidar de um método de investigação semelhante a uma interceção de comunicações. (...) Nas buscas online recolhem-se dados informáticos existentes. Já gerados e que se encontram armazenados num sistema informático. O que cada vez mais é a realidade preponderante, sendo que, a curto prazo, pouco sobrará para os documentos físicos. (...) A busca a sistemas informáticos tanto pode ser [realizada] através de acesso a um dispositivo físico ou remotamente*” (v. T. CAIADO MILHEIRO, *Buscas Online*, in *Corrupção em Portugal*, Org. P. P. de ALBUQUERQUE, R. CARDOSO e SÓNIA MOURA, Univ. Católica Ed., 2021, p. 548-549).

Poder-se-á dizer que, não obstante o exposto, é possível que algumas das mensagens contidas em ficheiros gravados em servidores possam não ter sido ainda objeto de fluxo de extração pelo destinatário e, como tal, dir-se-ia, quanto a essas o processo comunicacional com origem no remetente não se completou [v., acórdão do TC alemão de 16 de junho de 2009 (2 BvR 902/06)]. Acresce que, achando-se a mensagem nas mãos de terceiro à comunicação, dir-se-ia sinalizada uma situação de perigo credora da defesa das telecomunicações (neste sentido, v. NUNO BRANDÃO, *op. cit.*, p. 228, muito embora conjecturando neste excerto, o A., um pedido de colaboração direto com a entidade gestora da plataforma pelas autoridades, que seria por isso subsumível ao artigo 18.º, n.º 1, alínea b), do RJdC, na redação que consideramos, não à norma ora fiscalizada; a doutrina expressa pelo A. na compreensão do problema, porém, imporia tratamento *a pari* na situação de que tratamos).

Em primeiro lugar, de assinalar que o primeiro argumento assenta numa conjectura: porque *pode* (ou não) existir uma mensagem ainda não extraída pelo destinatário, *tudo* o arquivo de webmail em servidor fica blindado pela defesa das comunicações, também os documentos que, nesta visão



TRIBUNAL CONSTITUCIONAL

das coisas, dela não beneficiariam. A *grave distensão* de uma norma de tutela reforçada francamente excepcional desde logo nos deve merecer uma pausa, sugerindo que algo não estará correto.

Em segundo lugar, impõe-se recordar o que antes dissemos: uma mensagem de e-mail, quando é enviada, não é dirigida ao pretendido destinatário do conteúdo, mas ao servidor com quem este acordou a instalação de conta de correio eletrónico. É este o destinatário do fluxo de comunicação com origem no remetente protocolado pelo SMPT e o ficheiro gerado integra-se por essa via na estrutura do *service provider*, constituindo seu ativo imaterial: porque assim é, não é correto afirmar-se que a mensagem se acha «em trânsito» para qualquer outro ponto de chegada.

Ilustrando o exposto com uma outra situação análoga, também fora do espaço web, é possível que uma pessoa dirija uma carta postal a outra, pedindo-lhe no escrito que o fotocopie e retenha uma cópia, mas que faça chegar o original a uma terceira pessoa, a quem se destina o conteúdo. No momento em que o destinatário se apossa do envelope e o abre, porém, é consensual entre doutrina e jurisprudência que cessa de imediato a tutela de comunicações (v., por todos, GERMANO MARQUES da SILVA e FERNANDO SÁ, *Constituição Portuguesa Anotada, Anotação ao artigo 34.º*, Tomo I, 2.ª edição, Coimbra Editora, 2010, p. 772). Um segundo envio de carta postal, agora da segunda pessoa para a terceira, será um segundo fluxo de comunicação, que receberá tutela autónoma. No interim, o escrito ou, a todo o tempo, a sua cópia, não serão mais do que *documentos*, como tal desprovidos da proteção conferida pelo artigo 34.º, n.º 4, da Lei Fundamental. Não é difícil encontrar o paralelismo que se coloca para com os ficheiros armazenados em servidor.

É de sublinhar, de outra parte, que a *situação de perigo* da mensagem ainda não extraída pelo utilizador é *exatamente a mesma* das que já tenham sido objeto de fluxo de extração: estão, todas elas, armazenadas nos servidores do *account provider* em idênticas condições de acesso por este último, por terceiros, ou por autoridades, sem assimetria entre elas que permitisse afirmar que existisse particular vulnerabilidade de umas, face a outras. Isto é assim porque a situação de risco colocada *não decorre de um fluxo de informação*, ao contrário do sugerido, mas na posição conferida a terceiro quando se lhe atribui a custódia de todo o histórico de correio eletrónico de uma entidade.

Recuperando o exposto sobre tecnologias de comunicação, nos sistemas de *messaging* em *peer-to-peer* os fluxos de informação são realizados *apenas* entre remetente e destinatário da mensagem, pois que o serviço não comprehende sistema de arquivo de mensagens em servidor. Porque não disponibilizam essa utilidade aos subscritores, o histórico de mensagens ficará



TRIBUNAL CONSTITUCIONAL

armazenado nos aparelhos utilizados ou será perdido. Nestas situações, bem se comprehende, não se coloca a possibilidade de realizar pesquisas num segundo sistema, já que este não fixa dados.

Resulta à evidência, pois, que é para desempenhar a função de *arquivo remoto* que se envia e grava a informação em servidores; este depósito é gerador de risco para a privacidade, mas que não se pode entender produto da função de telecomunicação também desempenhada pelo sistema, mas da valéncia de *arquivo*, autónoma e específica, que não se confunde com processos de comunicação.

De resto, alguns sistemas que operam *peer-to-peer* oferecem ao utilizador a possibilidade de, periodicamente, carregarem a informação fixada no seu aparelho para o servidor do *service provider*, garantindo que o descaminho ou destruição do dispositivo local não implicará perdas de dados. É a geração deste *arquivo*, subsequente à troca de mensagens entre remetente e destinatário e, bem assim, ao fluxo de *upload* para o servidor de toda a informação (arquivo que constitui uma externalidade face a todos eles), que conforma o acervo passível de exame pelas autoridades tendo em vista a apreensão, não envolvendo qualquer forma de intrusão nas comunicações predecessoras.

Também se impõe relembrar que a gestão do arquivo em servidor é, toda ela, realizada pelo utilizador com benefício de controlo e poderes de disposição característicos do domínio direto. Resulta ilógico que se confira a cobertura constitucional própria às telecomunicações aos dados em servidor quando, no contexto colocado, toda a informação é consultável, gerível e passível de todas as formas de gozo e de disposição pelo titular a todo o tempo, incluindo a faculdade de eliminação de mensagens eletrónicas e de dados anexos mediante comando de *delete*, por forma em tudo análoga àquela de que dispõe no seu sistema local quanto a dados aí armazenados e com idêntico grau de efetividade; isto, em *absoluta oposição* ao que sucede em sistemas de comunicação e que constitui o elemento legitimador da tutela reforçada: a transferência do domínio sobre a informação para terceiro, encarregue da sua deslocação do autor para o destinatário, com inerente *privacidade de gozo* e de *controlo* sobre a mensagem por ambos os intervenientes durante esse processo.

Foi a percepção desta peculiaridade do webmail que conduziu o Supremo Tribunal Federal alemão (06.10.2022, BGH, VII ZR 895/21) a entender que uma declaração negocial por mensagem eletrónica adquire eficácia e vincula o declarante perante o declaratário com a receção da mensagem no servidor do *account provider* deste último, ainda que este não proceda à sua extração e desconheça a sua existência. Um email posterior do mesmo declarante que revogue a declaração inicial não se considera recebido *contemporaneamente* com a primeira [única] forma de a destituir de caráter



TRIBUNAL CONSTITUCIONAL

35C
22

vinculativo à luz do Direito civil alemão – cfr. 130(1) BGB], ainda que ambas as mensagens hajam sido extraídas para o sistema local do declaratário no mesmo momento e pelo mesmo fluxo.

Foi perante o facto de o email depositado em servidor *se encontrar integrado na esfera de controlo do destinatário* (controlo nesta medida *partilhado* com o explorador da plataforma) que o Tribunal concluiu que a declaração inicial será vinculativa e irrevogável pelo ato declarativo subsequente: “*caso (...) o email esteja disponível para extração no servidor de webmail do destinatário (...) isto significa que o email ficou sob controlo do destinatário. (...) Não é necessário à acessibilidade que ele extraia e reconheça a existência do email. (...) O servidor de webmail usado pelo destinatário para receber mensagens de email deve (...) ser visto como sua área de controlo, para a qual declarações de vontade podem ser remetidas em forma eletrónica.*” (Ac. cit.).

O exposto torna-se mais evidente nas situações, que já assinalámos, em que o sistema webmail utilizado e os dispositivos utilizados, incluindo servidores, sejam privativos à empresa (ou empresas) visadas pelas buscas. Nessas situações, todas as operações características do correio eletrónico têm lugar em equipamentos das entidades envolvidas e toda a gravação de dados é realizada em dispositivos integrados nas suas estruturas, ainda que os servidores estejam fisicamente instalados fora de espaços administrativos ou de centros operacionais.

A utilização de servidores próprios constitui uma medida destinada a assegurar maior controlo sobre *arquivos de informação*, não maior privacidade na sua transferência, já que, quanto à realização de comunicações, nenhuma entidade estará dispensada de recorrer a *internet service providers*, com a inerente exposição dos dados *enquanto são transferidos* entre terminais e servidores – nesse espaço beneficiando, claro está, da tutela prevista para a autodeterminação comunicativa.

Está encontrada a distinção que interessa. Com certeza que a *criação* e a *existência* de um acervo histórico de documentação de mensagens recebidas e enviadas representa também, por si só, um risco para a privacidade e para a confidencialidade de informações de natureza empresarial; sem dúvida que esse risco é ampliado quando o arquivo esteja em equipamentos de terceiro, já que os dados ali ficam, “*digamos assim, à mão de semeiar*” (v. NUNO BRANDÃO, *op. cit.*, p. 224); e tanto mais será assim quando o utilizador não elimine mensagens recebidas ou enviadas com assiduidade: tudo isto, porém, é a contrapartida inerente aos benefícios que o sistema de webmail confere ao seu titular e consequência das suas decisões de gestão sobre o seu acervo de documentos eletrónicos.

Em qualquer dos casos, sempre foi consensual entre doutrina e jurisprudência que o artigo 34.º, n.º 4, da Constituição da República Portuguesa, não constitui norma de proteção de *informação*



TRIBUNAL CONSTITUCIONAL

armazenada, tanto menos quando se encontra à disposição do seu titular, mas apenas de *informação em trânsito* (comunicação) e porque se encontra fora da sua esfera de controlo e de gozo. Porque é assim, a norma do artigo 18.º, n.º 1, alínea c), do RjdC e as medidas de obtenção de prova que autoriza não se podem entender invadirem a proteção estabelecida pela norma constitucional.

11.3. Importa ainda deixar uma breve referência à informação qualificável como *metadados*, cuja sujeição ao poder público é coeva à apreensão de mensagens de correio eletrónico ao abrigo dos poderes conferidos à AdC pelo artigo 18.º, n.º 1, alínea c), do RjdC.

Na verdade, com os ficheiros digitais de mensagens localizados nos aparelhos eletrónicos da entidade buscada ou em servidores de que esta disponha de acesso direto encontrar-se-á, para além de conteúdos, um conjunto de informações referentes às circunstâncias *em que o ficheiro foi transmitido*, quer no que respeita aos sistemas de conexão à rede dos intervenientes (*dados de base*), quer quanto aos fluxos de transmissão de objetos enviados ou recebidos (data e hora das partidas e chegadas, IPs de emissores e receptores, volume de dados transferidos, etc. – *dados de tráfego*).

No que respeita aos dados de base, a jurisprudência constitucional vem afastando a sua cobertura pela tutela das comunicações quando não estejam associados e não sejam caracterizantes de um concreto fluxo de comunicação intersubjetiva (troca de informação entre duas pessoas), já que nas demais situações se reconduzem a “*dados escritos atinentes a uma relação contratual entre uma pessoa e uma empresa operadora de telecomunicações, referindo-se à identificação e morada do titular e ao próprio contrato de ligação à rede*” ou, noutras casas, a “*dados de localização a partir de um telefone ligado, mas em stand by, e/ou através do sistema de satélite GPS ou outro*” (v. Acórdão do TC n.º 464/2019; v. também, Acórdãos do TC n.ºs 486/2009, 403/2015 e, talvez de maior importância, 268/2022 e 800/2023).

Se do exposto resultaria tentador concluir que a autodeterminação comunicativa confere proteção a todos os metadados que não os compreendidos neste grupo, ou seja, que acobertaria os dados de base conexos com comunicações específicas e todos os dados de tráfego, certo é que não foi essa a posição assumida pelo Tribunal Constitucional nas duas ocasiões em que formulou juízo de constitucionalidade sobre as normas dos artigos 4.º e 9.º, da Lei n.º 32/2008, de 17 de julho, estatutivas de uma injunção de recolha generalizada e preservação desse tipo de meta-informação sobre empresas fornecedoras de ligação à internet. Com efeito, nessas ocasiões este parâmetro não



394
R

TRIBUNAL CONSTITUCIONAL

foi incluído nos fundamentos do juízo de constitucionalidade desse programa normativo, pese embora declarações de voto nesse sentido (v. Acórdãos do TC n.ºs 268/2022 e 800/2023).

Algum tempo antes, porém, o Acórdão do TC n.º 464/2019 firmou o entendimento que norma que autorizasse o acesso a dados de tráfego de comunicações por oficiais do SIS e SIES constituía ingerência no disposto no n.º 4, do artigo 34.º, da Constituição da República Portuguesa, renovando a jurisprudência primeiro patenteada no Acórdão do TC n.º 403/2015 com respeito a norma semelhante, mas mais abrangente quanto a categorias de informação (“*dados de tráfego, de localização ou outros dados conexos das comunicações*”). Este entendimento está também implícito aos fundamentos do Acórdão do TC n.º 486/2009, que concluiu que o acesso a dados de base e de tráfego relativos a chamadas por telemóveis se compreendia no âmbito de ingerência em comunicações que o disposto no artigo 187.º do Código de Processo Penal representava (como tal existindo norma capacitante sobre essa forma de intrusão em comunicações e, por isso, negando juízo de constitucionalidade sobre interpretação do preceito que permitisse a sua recolha).

No cômputo geral, parece que a jurisprudência do Tribunal Constitucional se vem orientando no sentido de que os *dados de base conexos a uma comunicação* e os *dados de tráfego* podem estar protegidos pela autodeterminação comunicativa, mas que a invasão proibida por este estatuto estará dependente de alguma forma especial de atividade envolvendo metadados (consentida ou promovida pela norma) cujos contornos, ao momento, não são ainda claros, já que não é seguro afirmar que variáveis estarão em causa (delas terá decorrido o juízo nos Acórdãos n.ºs 268/2022 e 800/2023). Seja como for, não é necessário realizar uma análise mais desenvolvida a qualquer um destes casos para procurar encontrar um critério jurisprudencial, já que os quadros normativos que nesses casos se colocaram eram substancialmente diferentes do que se nos depara *in casu*.

Nos Acórdãos citados, as normas fiscalizadas permitiam às autoridades o acesso a meta-informação por via da sua extração prévia de *uma comunicação em curso* pelas respetivas *operadoras*, que é dizer, pelas empresas que asseguram a ligação a rede de sistemas terminais (*internet ou rede telefónica*) executando os fluxos de transmissão de dados entre utilizadores, o que apelidámos *supra de Internet Service Providers ou ISP* (cfr. artigo 4.º, n.º 1, da Lei n.º 32/2008, de 17 de julho, artigo 10.º, n.º 1, da Lei Orgânica n.º 4/2017, de 25 de agosto e artigos 187.º, n.º 1 e 189.º, n.º 1, ambos do CP).

Constituía um atributo central a todos os modelos legais fiscalizados (pelo menos, tal como os compreendeu o Tribunal Constitucional, nos sobreditos casos) que a operação de aquisição da



TRIBUNAL CONSTITUCIONAL

informação se efetuasse pela *interpretação de fluxos de transmissão* de dados pela entidade que os executa (ISP) ao serviço e por conta do autor da comunicação, assim caracterizando a situação de vulneração da privacidade a que responde a autodeterminação comunicativa. Nuns casos, a exfiltração visava corresponder a pedido prévio de autoridades (artigo 10.º, n.º 1, da Lei Orgânica n.º 4/2017, de 25 de agosto e artigos 187.º, n.º 1 e 189.º, n.º 1, ambos do CP) e noutras impunha-se a permanente extração da informação pelos ISP e a sua preservação por certos períodos, tendo em vista satisfazer solicitações nesse hiato (artigo 6.º da Lei n.º 32/2008, de 17 de julho).

A norma sob sindicância, porém, não comprehende nada de vagamente semelhante.

No caso da pesquisa e apreensão de mensagens de correio eletrónico armazenadas em aparelhos locais ou em sistemas diretamente acessíveis através do terminal, a única meta-informação recolhida será a contida nos ficheiros pesquisados, resultante da aptidão destes últimos para conservar dados sobre a sua origem, destino e percurso, contextualizadores do conteúdo registado, isto à semelhança da generalidade dos documentos que hajam estado envolvidos em processos de comunicação. Embora esta informação possa permitir reconstruir o fluxo de trânsito por via dedutiva (ou seja, perceber quem enviou, quando enviou, o que enviou e que canal utilizou), ela não é obtida pela sua intercetação e é alheia ao trânsito de dados em si mesmo considerado, já que o documento apenas dele oferece testemunho ulterior, depois de concluído esse processo.

Uma vez mais recorrendo a um exemplo do «mundo analógico», por assim dizer, na análise de um arquivo de correio postal, atual ou centenário, encontrar-se-ão escritos-cartas com inscrição da data em que foram redigidos, indicações manuscritas de destinatário e de remetente (v. g., epígrafe e assinatura do subscritor), por vezes datação por selo de entrada aposto por serviços de secretariado do recipiente e rubrica de quem o recebeu, assim como outras indicações que não constituem *conteúdo da mensagem*, mas circunstâncias relativas à sua elaboração e trânsito (*metadados*).

O envelope que conteve a carta, usualmente unido ao escrito e com ele arquivado, por sua vez, exibirá os nomes e as moradas de caixa postal de destinatário e de remetente, bem como informações carimbadas identificativas da empresa postal que realizou o serviço de remessa e do ponto de recolha onde foi entregue (*dados de base*, conexos com uma comunicação específica). Através de selos, carimbos, distintivos autocolantes e inscrições manuscritas, o sobreescrito exibirá aposições dos serviços postais sobre a data de recebimento do objeto, a data em que foi transferido entre departamentos locais, quando seja o caso e, havendo devolução a remetente, o motivo da



TRIBUNAL CONSTITUCIONAL

falha na entrega e a data de remessa para restituição (*dados de tránsito*). Um aviso de receção anexo a uma cópia de um manuscrito enviado, de sua parte, documentará também a data em que a carta foi feita chegar ao destinatário (*dados de tránsito*) e reproduzirá elementos de um documento de identificação pessoal de quem o recebeu (*dados de base*, conexos com uma comunicação).

Todo estes são, em sentido próprio, *metadados do correio tradicional*, informações que explicitam e detalham o processo de comunicação em que o escrito esteve envolvido, mas que subsistem depois de este se concluir incorporados no documento em causa, e que, por este mesmo motivo, não deixarão de ser suas meras componentes, sem outra natureza atribuível.

Serve por dizer, da mesma forma que o confronto com qualquer uma destas informações aquando do apossamento por autoridades de correspondência em arquivo não tem por virtude converter a apreensão de um documento numa ingerência em sistemas de comunicação, também os metadados contidos num ficheiro apreendido na sequência de pesquisas realizadas em dispositivos eletrónicos não emprestam essa natureza à sua apreensão por autoridades. Todos os ficheiros fixados num sistema, quer tenham sido transferidos a partir de dispositivos locais ou criados no processador de um computador, retêm metadados, seja a respetiva data da criação/gravação, a data da última modificação, o programa de software que os gerou e por que foram modificados, a data do último acesso, a sua dimensão, a designação de perfil no sistema atribuída ao criador e muitas outras informações, potencialmente com grande relevância para uma investigação. Foi, por exemplo, pelo acesso a metadados de um ficheiro de texto criado pelo próprio – e que nunca esteve envolvido num processo de transmissão de dados, antes foi meramente fixado em diskette pelo autor – que o homicida norte-americano conhecido como “BTK” foi identificado como *Dennis Rader* e localizado em Park City, no Estado do Kansas.

Serve aqui, portanto, o que antes dissemos: porque o artigo 34.º, n.º 4, da Constituição da República Portuguesa, cinge o seu âmbito de tutela a *informações em trânsito* e, em exclusivo, enquanto estiverem em trânsito, alheando-se de depósitos de dados armazenados em suporte documental (digital), o disposto no artigo 18.º, n.º 1, alínea c), do RjdC, não invade aquele espaço de proteção.

11.4. Fechamos o presente título com uma análise sumária de algumas das consequências da proposta para delimitar a proteção das telecomunicações conferida pelo artigo 34.º, n.º 4, da Constituição da República Portuguesa, também no confronto com a jurisprudência recente.



TRIBUNAL CONSTITUCIONAL

397
R

11.4.1. A posição exposta sobre a tutela constitucional do sistema de comunicação *webmail* e de *messaging* análogos (*whatsapp*, *telegram*, *Messenger*, etc.) sumaria-se em dois itens (i) e (ii) *infra*.

Em primeiro lugar (i), o correio eletrónico e os sistemas de mensagens eletrónicas beneficiam da proteção conferida pelo artigo 34.º, n.º 4, da Constituição da República Portuguesa, quando realizam transferências de informação entre utilizadores. Estas trocas de informação são realizadas por um prestador externo (ISPs – *Internet Service Providers*: Vodafone, Meo-Altice, NOS, etc.) e permitem a comunicação à distância entre duas pessoas (intersubjetividade): como tal, não merece dúvidas que estão sob a especial proteção conferida pela autodeterminação comunicativa.

Qualquer quadro legal que consinta ações de intrusão nos sistemas de troca de informação realizados pela internet (v. g., captura e reprodução de conteúdos ou de dados periféricos – metadados – durante o processo de transferência entre computadores ou entre redes), terá por isso de observar as especiais garantias estabelecidas pelo artigo 34.º, n.º 4, da Lei Fundamental.

Já no que respeita a ficheiros resultantes dessa transferência de informação fixados em dispositivos eletrónicos (ii), estes *não beneficiam* da proteção conferida pela autodeterminação comunicativa. Trata-se de informação *armazenada*, não de um *processo communicativo*, pelo que nessas condições estão desprovidos da tutela reforçada garantida pela supracitada norma constitucional.

A busca e apreensão de ficheiros fixados em dispositivos eletrónicos (computadores, discos externos, pen drives, etc.) consentida pelo artigo 18.º, n.º 1, alínea c), do RjdC, realiza-se, única e exclusivamente, sobre dados informáticos colocados nestas condições, pelo que a norma não representa qualquer ingerência no direito à integridade das comunicações.

Não é relevante a quem pertence o dispositivo eletrónico onde o ficheiro está fixado, se ao receptor da mensagem, ao emissor ou a terceiro: desde que se trate de um ficheiro armazenado, não se verifica qualquer intrusão em telecomunicações. Por outro lado, desde que a entidade inspecionada disponha de acesso direto ao ficheiro (controlo), este fica compreendido no âmbito dos poderes de investigação e de reunião de prova conferidos pela norma fiscalizada à AdC. Isto significa que é possível, nestas condições, realizar a pesquisa e apreensão de ficheiros fixados em servidores em processos contraordenacionais por infrações ao Direito da concorrência.

É assim com o webmail, como é assim com o telefax, o telegrama ou qualquer outro meio de comunicação que liberte um suporte físico da mensagem duradouro: todos estes sistemas



398

TRIBUNAL CONSTITUCIONAL

beneficiam da tutela das comunicações durante o processo de transmissão de dados, mas não quando o suporte documental resultante desse processo (v. g., o papel impresso pela máquina telefax ou o boletim do telegrama) se acha arquivado, pertença o respetivo dossier e mobiliário de acondicionamento ao recetor ou a outra pessoa a quem haja confiado a sua guarda.

O artigo 18.º, n.º 1, alínea c), do RJDc, apenas permite a apreensão de ficheiros informáticos nesta segunda condição, resumindo-se a uma *operação clássica de busca e apreensão em empresa* que tem de peculiar ser realizada sobre aparelhos eletrónicos e com recurso a instrumentos informáticos. A norma não constitui qualquer forma de ingerência, pois, na autodeterminação comunicativa.

Posto isto, vejamos as consequências de outra forma de observar o problema, seja a proposta pelo Acórdão do TC n.º 91/2023.

11.4.2. Importa levar em conta que a atribuição da defesa das telecomunicações à correspondência eletrónica armazenada em sistemas de webmail não significaria, apenas, a sua subtração a processos contraordenacionais como meio de prova ou a proibição da sua apreensão em buscas. São conscientes e muito pertinentes as considerações que o Acórdão do TC n.º 91/2023 despende sobre a impossibilidade de realizar qualquer forma de fiscalização e repressão de práticas lesivas da concorrência sem acesso a mensagens de correio eletrónico armazenadas, mas esse não é o único efeito que daí decorre e talvez não seja, mesmo, o mais danoso e revolucionário.

Aquele entendimento significaria, também, que os mesmos elementos não poderiam ser sujeitos ao poder público em processos jurisdicionais não-penais por via de quaisquer outros atos de autoridade, já que também estes sinalizariam uma forma de intrusão nesse espaço de tutela.

Assim, a *requisição de documentos* em formato eletrónico em contas webmail, estejam estes na disponibilidade de sujeito processual ou de terceiro, fosse por iniciativa oficiosa do Tribunal ou a requerimento de uma das partes (artigos 429.º e 432.º do Código de Processo Civil), teria de ser entendida uma forma de ingerência em comunicações proibida pelo artigo 34.º, n.º 4, da Lei Fundamental, com certeza menos intrusiva que uma operação de busca, mas sem nenhuma dúvida atingindo a mesma (pretensa) reserva sobre mensagens eletrónicas. Num mundo orientado para a desmaterialização de documentos e em que a generalidade de trocas de informação e de formulação de declarações de vontade são realizadas por sistemas de webmail ou análogos, isso significaria proibir os Tribunais de acederem à documentação de boa parte do tráfego jurídico realizado, tanto



TRIBUNAL CONSTITUCIONAL

mais assim quando continua a vigorar o princípio sobre liberdade de forma de negócios (artigo 219.º do Código Civil): notas de encomenda, notas de débito ou de crédito, faturas, documentos de quitação, atos de interpelação, de denúncia, de resolução de contratos, atos de reclamação de defeitos, de reconhecimento de defeitos, moratórias, estipulações sobre prazos *ad hoc*, atos de confissão, tudo isto se declara, ou se recebe com valor declarativo, por mensagens de correio eletrónico, em detrimento dos veículos clássicos de formalização, *maxime* correio postal.

Também no sistema webmail estes documentos são preservados, com gozo de datação, ordenação e autenticidade garantidas pelo sistema; com benefício de acessibilidade facilitada e defendidos de olhos indiscretos pela privacidade inerente aos sistemas de informação; tudo isto, em detrimento do arquivamento em pastas, dossiers ou outras formas de arquivo corpóreo.

A própria geração de vínculos contratuais, pela convergência de vontades, a constituição em obrigação de indemnizar ou a indução do declarante em erro que atingirá a declaração negocial (v. g., pela veiculação de conteúdos injuriosos ou difamatórios; a transmissão de factos falsos ou criação de logros e ardil durante a fase pré-negocial) podem resultar do conteúdo de mensagens de webmail, que representará o único suporte de fontes de obrigações ou da viciação de negócios.

Se se concluir que o inacesso por autoridades públicas, incluindo Tribunais, a esta documentação constitui um imperativo constitucional, salvo processo criminais ou atos voluntários de quem controla o ficheiro digital e dele pode dispor, então teremos que nenhum direito privado poderá ser triunfantemente exercido no ambiente jurisdicional por quem não disponha de poderes de facto sobre o documento (ou documentos) que comprova(m) o fundamento da sua pretensão. Criar-se-á, enfim, um «mundo de clandestinidade» apenas franqueável por autoridades criminais.

Impõe-se assinalar, com a doutrina, que, levando em conta a intensidade da tutela em causa, “não se poderá deixar de ser especialmente rigoroso e tanto naquilo que se leva ao objeto da proibição, o mesmo é dizer, ao conteúdo normativo do princípio da autodeterminação comunicativa (...) sob pena de inviabilização de diversas importantes atividades investigatórias” (v. NUNO BRANDÃO, op. cit., p. 225). Isto será tanto mais assim quando o que se pretende integrar no âmbito de tutela não é, como vimos, caracterizável como comunicação, mas antes como conteúdos em formato eletrónico que foram comunicados.

Por fim, será também de levar em conta a que conduzirão diferentes formas de observar o problema no que respeita a certos procedimentos administrativos, *maxime* inspeções tributárias.

397
R

TRIBUNAL CONSTITUCIONAL

Assinalámos acima o advento e difusão, ao tempo presente, da *contabilidade digital ou colaborativa*, que constitui um produto tecnológico de estrutura semelhante ao webmail. Como acima dissemos, neste modelo toda a contabilidade de uma empresa é organizada e armazenada em servidores, que neste contexto (e outros) se apelida de *cloud*, recebendo *inputs* de informação e sendo consultável através de fluxos de envio e de extração, à inteira semelhança do webmail.

Constituindo uma ferramenta de partilha e troca de informação entre pessoas de uma mesma organização e caracterizando-se pela coordenação de fluxos de dados entre os dispositivos locais da empresa e do prestador do serviço eletrónico (*intersubjetividade*), estamos também perante um sistema de comunicação à distância, ainda que os conteúdos transferidos se cinjam a atos económicos privativos a uma mesma entidade: “é indiferente o conteúdo das missivas ou telecomunicações, não se exigindo que versem sobre coisas privadas ou íntimas nem que contendam com segredos. Pode tratar-se de matérias inteiramente anódinas, da troca de informações comerciais entre empresas ou mesmo da circulação de ofícios ou protocolos entre órgãos ou agentes da Administração Pública, em princípio expostos às regras da transparência” (v. M. COSTA ANDRADE, *Commentário Conimbricense...*, p. 754; Acórdão do TC n.º 91/2023).

Assim sendo, não será controverso que uma norma legal que capacite autoridades a exigirem de ISP a *interpretação e extração de informação* de fluxos de dados entre terminais de utilizadores e a *cloud* em sistemas de contabilidade colaborativa com destino a instrução probatória, invadirá o espaço de proteção do n.º 4, do artigo 34.º, da Constituição da República Portuguesa, subordinando-se às respetivas condições, designadamente no que tange reserva de processo-crime.

Pois bem, aqui chegados, impõe-se a saber se também a informação *armazenada* nos servidores do prestador do serviço, ou aquela que, extraída da *cloud*, esteja gravada em equipamentos eletrónicos da entidade utilizadora, beneficiaria da tutela constitucional conferida a comunicações, como, em confronto à posição que adotamos, se defende relativamente ao webmail. Atendendo à identidade de situações, será inevitável concluir que a jurisprudência recente responderia que sim.

Vejamos agora que os poderes conferidos às autoridades tributárias e aduaneiras pelo Regime Complementar do Procedimento da Inspeção Tributária e Aduaneira (RCPT) de pesquisa documentária para controlo da situação jurídico-tributária de particulares são semelhantes aos atribuídos à AdC pelo RJdC, talvez mesmo superiores, ao que acresce a introdução no âmbito dos poderes de fiscalização, *expressis verbis*, de faculdades de acesso a documentos e a sistemas eletrónicos destinados à documentação da atividade económica do sujeito passivo inspecionado.



TRIBUNAL CONSTITUCIONAL

No que aqui nos interessa, as autoridades tributárias podem proceder, no âmbito da inspeção, ao “*exame, requisição e reprodução de documentos, mesmo quando em suporte informático, em poder dos sujeitos passivos ou outros obrigados tributários, para consulta, apoio ou jnruão aos relatórios, processos ou autos*” (artigo 28.º, n.º 2, do RCPIT), com faculdade de “*examinar quaisquer elementos dos contribuintes que sejam suscetíveis de revelar a sua situação tributária, nomeadamente os relacionados com a sua atividade, ou de terceiros com quem mantinham relações económicas e solicitar ou efetuar, designadamente em suporte magnético, as cópias ou extratos considerados*” (artigo 29.º, n.º 1, alínea a), do RCPIT) e de “*copiar os dados em formato eletrónico dos registos e documentos relevantes para apuramento da situação tributária dos contribuintes ou efetuar uma imagem dos respetivos sistemas informáticos*” (artigo 29.º, n.º 1, alínea f), do RCPIT). Os «elementos relevantes» para estes efeitos compreendem todo o espólio documental das entidades, incluindo livros, registos contabilísticos e auxiliares, programas e suportes magnéticos, elementos de contabilidade analítica, documentos de suporte e outras formas de evidência contabilística, bem como todos os demais relacionados com a atividade com significado fiscal (artigo 29.º, n.º 2, alíneas a) a d), do RCPIT).

O procedimento de inspeção assenta no princípio de cooperação entre administração tributária e sujeito fiscalizado (artigos 5.º, 9.º, n.º 1 e 48.º e ss, do RCPIT), mas, em situações mais obscuras, pode não ser precedido de notificação prévia e, em caso de obstrução ao exercício dos poderes de fiscalização pelos inspecionados, pode ser requisitada força pública, designadamente para efetivação do acesso aos documentos relevantes (artigo 28.º, n.º 2, alínea h), do RCPIT), pelo que o procedimento de inspeção tributária está longe de estar desprovisto de dimensão coercitiva.

Ora, caso a empresa implemente um sistema de organização contabilística em *cloud*, como vai sendo tendência recente, a generalidade, senão a totalidade, destes elementos documentais estarão armazenados em formato eletrónico nos servidores do prestador do produto informático, ainda que se possam também encontrar certos fragmentos dispersos por aparelhos que hajam realizado extrações. A pretender-se que a informação nestas condições beneficie da tutela das comunicações, isso significará que toda a atividade de fiscalização dos serviços tributários de documentação contabilística fiscalmente relevante nos termos do RCPIT será proibida, em face da reserva de processo penal que se imporia ao abrigo do n.º 4, do artigo 34.º, da Lei Fundamental.

De resto, a Lei inclui nos elementos acessíveis à inspeção toda a documentação interna ou externa (à empresa) relativa às operações económicas e financeiras realizadas com terceiros (artigo 29.º, n.º 2, alínea e), do RCPIT), tendo em vista permitir a análise de lançamentos e respetiva



401
✓

TRIBUNAL CONSTITUCIONAL

evidência de forma contextualizada. Impõe também o acesso à “*correspondência recebida e expedida relacionada com a atividade*” (artigo 29.º, n.º 2, alínea g), do RCPT. Aos dias de hoje, como dissemos, estes documentos estarão, na sua generalidade, em ficheiros armazenados em servidores de *webmail account providers*, não arrumados em pastas ou dossiers manuseáveis nas instalações da empresa.

Parece, portanto, que a desmaterialização de documentos e a instalação da contabilidade em *cloud* teria por efeito deixar a empresa em situação de *absoluta invulnerabilidade* quanto a qualquer iniciativa da administração para controlar ou monitorizar a sua atividade económica com relevo fiscal, oferecendo evidentes perspetivas de impunidade (e oportunidades) para enviesamento de fatores de conexão, ocultação de rendimentos ou de ativos e quaisquer outras ações de fraude. Empresas mais modestas para quem o custo da contabilidade digital seja proibitivo, porém, continuarão expostas à ação de fiscalização das autoridades fiscais, como até aqui veio sucedendo.

Dissemos atrás que a integração na tutela das comunicações de mensagens webmail armazenadas representaria a criação de uma «*offshore de informação*» em território nacional ou um «*mundo de clandestinidade*». Esse fenómeno em ponto nenhum do tráfego jurídico será mais nítido do que no âmbito do Direito tributário: sem prejudicar o acesso do operador económico a informação contabilística (cuja gestão é até mais eficaz nestas condições) e inerente posição de gozo, os dados em *cloud* serão havidos como *perpetuamente em trânsito*, o que equivale a dizer que não se encontram em local *nenhum*, adquirindo uma «*propriedade quântica*» que os imunizaria de ações de fiscalização.

De notar que, neste domínio, como no âmbito do Direito processual privado, nem sequer a abertura da reserva de processo penal proposta pelo Acórdão n.º 91/2023 preveniria o resultado a que conduz esta posição, já que não tratamos de processos ou de procedimentos de índole sancionatória que, pelo entendimento contido no arresto, pudessem merecer tratamento diferente.

Embora o exposto já nos pareça o bastante, podemos ainda deixar impresso que esta forma de observar a questão importa também que se equacionasse até que ponto será compatível com a inviolabilidade das comunicações os poderes de fiscalização e de auditoria conferidos a entidades reguladoras (Banco de Portugal, Comissão do Mercado de Valores Mobiliários, Instituto de Seguros de Portugal, Entidade Reguladora do Setor Energético, etc.), já que a desmaterialização de acervos documentais, operacionais e contabilísticos, e a utilização de ferramentas de contabilidade em *cloud* serão realidades mundanas entre empresas desses setores. Também se terá de repensar o regime de transparência dos organismos administrativos e os direitos de acesso a documentos



TRIBUNAL CONSTITUCIONAL

402
R

conferidos aos cidadãos (Lei n.º 26/2016, de 22 de agosto, *maxime* artigos 12.º e ss), se arquivados em *cloud* ou se a base de dados resultar de transferência de informação entre sistemas, já que em ambos os casos estariam perante formas *a pari* de invasão da autodeterminação comunicativa.

Trata-se, portanto, e enfim, de uma *desfiguração* da proteção conferida pelo n.º 4, do artigo 34.º, da Constituição da República Portuguesa, que não é defensável alguma vez se tenha proposto conduzir a um efeito proibitivo com esta extensão e nestas condições, que criará situações de indefesa de particulares francamente lesivas do direito de acesso a tutela jurisdicional (direito a prova) e à efetivação de direitos (privados) (artigo 20.º, n.º 1, da Constituição da República Portuguesa), como conduzirá, pelo menos, a que se torne inviável qualquer perspetiva de assegurar receita tributária e equidade fiscal (artigo 103.º, n.º 1, da Constituição da República Portuguesa).

Finalizando a exposição, anotamos que a delimitação da proteção da autodeterminação comunicativa proposta não reside numa forma inovadora de compreender o artigo 34.º, n.º 4, da Constituição da República Portuguesa, em resposta às novas realidades colocadas por tecnologias de informação (pelo contrário, renovamos o entendimento firmado por doutrina e jurisprudência). A posição que adotamos cinge-se em não ver nele incluída norma que autorize a apreensão de informação armazenada em equipamentos de uma empresa ou em servidores de que disponha de acesso direto, isto com base no facto insofismável de que essa ação de sujeição ao poder público não se efetiva *enquanto*, nem *porque*, a informação se acha em trânsito. É este, sempre foi este, o atributo característico da ingerência em comunicações, o que, também aqui, se impõe reiterar.

Por tudo, resta concluir, enfim, que o artigo 18.º, n.º 1, alínea c), do RJDc, na interpretação normativa sindicada, não representa qualquer forma de ingerência na garantia de inviolabilidade das telecomunicações constante do artigo 34.º, n.º 4, da Constituição da República Portuguesa.

12. Correio Eletrónico, Estabelecimento, Privacidade e Autodeterminação Informacional (artigos 26.º, n.º 1, e 34.º, n.º 4, da Constituição da República Portuguesa)

12.1. O disposto no artigo 18.º, n.º 1, alínea c), do RJDc, na dimensão normativa sindicada, impõe ainda se considere a proteção conferida por outros dois direitos fundamentais integrados no elenco constitucional de direitos, liberdades e garantias, especificamente convocados pelos



TRIBUNAL CONSTITUCIONAL

recorrentes ao debate em alegações, sejam o direito à *privacidade* e o direito à *autodeterminação informacional* (artigos 26.º, n.º 1, e 35.º, n.º 4, ambos da Constituição da República Portuguesa).

A este respeito e lateralmente a ambas as matérias, impõe-se assinalar que a norma fiscalizada limita os poderes conferidos à AdC ao exame, busca e apreensão de mensagens de correio eletrónico (subsumíveis à noção de “*documentação*”, na dimensão normativa em causa) às “*instalações, terrenos ou meios de transporte de empresas ou de associações de empresas*”, como já dissemos.

Esta caracterização do sujeito passivo que é visado pelas operações de aquisição de prova e o recorte do seu objeto cinge a dimensão de ingerência decorrente da norma a *contexto empresarial*. As operações de busca e exame apenas podem invadir a estrutura de meios de uma empresa ou de uma associação de empresas e só podem ser sujeitos ao poder público documentos que constituam seus ativos imateriais. As mensagens de webmail subsumíveis à previsão da norma serão, pois, as que hajam sido criadas ou recebidas pelos seus colaboradores (incluindo corpos de gestão) no âmbito das atribuições que lhe estão confiadas na empresa ou em função dessa especial qualidade, que assim se considerarão componentes e parte integrante do seu estabelecimento. Trata-se, pois, de instrumentos da atividade económica desenvolvida ou de elementos diretamente relacionados com essa atividade, cujo privativo de governo e de disposição se inscreve na esfera da empresa.

Esta observação possui grande importância no caso *s/nb início*, já que, enquanto a tutela das comunicações constitui uma forma de defesa da privacidade da informação em *sentido formal*, os artigos 26.º, n.º 1, e 35.º, n.º 4, da Constituição da República Portuguesa, ocupam-se da sua proteção em função do seu *especial conteúdo* e inerente aptidão para impactar na personalidade.

12.2. A jurisprudência tem entendido (designadamente quando se debateu o sigilo bancário e respetiva projeção constitucional) que o artigo 26.º, n.º 1, da Constituição da República Portuguesa defende uma *dimensão de ordem económica* do direito à privacidade, muito embora o localize num espaço periférico e particularmente permissivo a cedências, quando em confronto com outros interesses jurídico-constitucionais. O reduzido âmbito de *garantia efetiva* do direito (Acórdão do TC n.º 442/2007) neste plano explica-se pela pobreza da conexão entre esse tipo de elementos e a personalidade da pessoa humana, que se avulta em valor jurídico defendido:



TRIBUNAL CONSTITUCIONAL

*“O direito à reserva da intimidade da vida privada e familiar (artigo 26.º, n.os 1 e 2, da Constituição da República Portuguesa) integra o catálogo de direitos, liberdades e garantias, estando dotado da especial eficácia que deriva do artigo 18.º da Constituição da República Portuguesa. É habitual desdobrar este direito fundamental em três dimensões: o direito à solidão, o direito ao anonimato e o direito à autodeterminação informativa. Este último, por sua vez, é entendido como “o direito de subtrair ao conhecimento público factos e comportamentos reveladores do modo de ser do sujeito na condução da sua vida privada” (v. Acórdãos do TC n.º 442/2007 e 517/2015), definindo um espaço de arbitrio conferido a cada pessoa para “decidir livremente quando e de que modo pode ser captada e posta a circular informação respeitante à sua vida privada e familiar” (*ibid.*) e é a dimensão que mais nos interessa no contexto colocado (em sentido parcialmente convergente, v. J. J. GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, Almedina, 2007, pp. 467-468). (...)”*

A grande dificuldade na compreensão deste direito, logo numa primeira abordagem, reside em distinguir, de entre o vasto espectro de informação relativa a uma pessoa, qual a que se inscreve no espaço de confidencialidade definido pelo seu perímetro defensivo e, dentro dele, em que medida se estabelecem graus de permeabilidade a exposição a publicidade entre categorias (v. J. J. GOMES CANOTILHO e VITAL MOREIRA, op. cit., p. 468). Se parece certo que a reserva de informação variará em função de estratos de natureza polarizada – entre a sua natureza íntima ou indiferenciada – é igualmente desafiante definir com segurança em que medida se pode entender que interesses jurídicos ou direitos justificariam limites ao direito e em função de que parâmetros.

(...) [O] balizamento entre parâmetros não pretende exprimir as condições para a admissibilidade de intrusões no direito à reserva da vida privada tendo por orientação um referente legitimador; mas, a montante desse problema, sinalizar o caráter complexo da delimitação da esfera de proteção conferida pelo direito e da intensidade da sua tutela. Este deverá definir, assim um espaço de proteção conjunto, mas estratificado, social e culturalmente adequado à vida contemporânea (v. J. J. GOMES CANOTILHO e VITAL MOREIRA, op. cit., p. 468), que constitua manifestação da pluralidade de vetores inerente ao contexto pessoal de quem dela beneficia (e de quem pode prejudicar) e adequada concretização jurídico-constitucional das variáveis, de segurança e interpessoais, inerentes às relações entre o indivíduo, terceiros e a própria comunidade jurídica. (...)

*De entre as múltiplas categorias de informação cujo direito à autodeterminação se coloca, a jurisprudência constitucional veio sinalizando «uma ‘esfera privada de ordem económica’ também merecedora de tutela» (acórdão do TC n.º 442/2007 citando ALBERTO LUISS, *Direito bancário*, Coimbra, 1985, p. 88; v. também acórdãos do TC n.os 278/95 e 517/2015), que compreenderá a reserva de informação sobre o património e sobre operações económico-financeiras (...)*

A privatividade da informação de índole patrimonial e económica não se pode admitir equiparável à informação íntima, já que necessariamente se entrelaça com interesses de terceiros e da ordem jurídica observada na sua globalidade: se, como dissemos, certas informações apenas sinalizam os interesses pessoais do indivíduo a que respeitam ou a curiosidade frívola de outros (v. g., o culto que professa, a sua orientação sexual, preferências de doutrina filosófica, sentimentos amorosos ou de ressentimento, etc.), o património e as operações que o envolvem lançam ramificações sobre a situação de terceiros e da própria ordem jurídica, (v. g.) impondo deveres gerais de abstenção e representando a garantia geral das obrigações de que beneficia o universo de credores do indivíduo, atuais e potenciais. Inclui-se neste universo os credores de pensão de alimentos, de trabalhadores por prestações remuneratórias e da posição ativa sobre créditos fiscais: todos estes direitos estão dotados de dimensões que em muito excedem, em termos de natureza, carga ética e valor jurídico, o vínculo obrigacional de mera fonte contratual.

Por outro lado, operações de transferência de capitais, especialmente fluxos destinados a países estrangeiros, a subscrição de produtos financeiros, ações de resgate e toda uma constelação de atos e negócios jurídicos semelhantes, podem representar perigos de ordem pública, seja de descapitalização da economia, de insuficiência ou de desorganização de setores económicos, ou de potenciação de mecanismos de branqueamento de capitais de origem ilícita ou criminosa; podem também caracterizar práticas de fraude, de burla, de abuso de confiança, de frustração de créditos, de insolvência dolosa ou de evasão fiscal; significa isto que operações patrimoniais impactam em interesses regulatórios públicos, em especial, e no governo económico do país na sua globalidade, bem como em certas áreas do Direito criminal.

Quando falamos de informação sobre o património (...) estamos, pois claro, num locus muito distante da estrita natureza individual, endógena e personalística, própria da intimidade, dos dados informativos relativos a uma pessoa.



405
X

TRIBUNAL CONSTITUCIONAL

(...) ainda que uma esfera de privacidade de ordem económica se possa entender acobertada pelo artigo 26.º, n.º 1, da Constituição da República Portuguesa, esta localizar-se-á num espaço altamente periférico do direito à autodeterminação informativa, resultando fragmentária quanto a objeto (de tal forma que não se afigura defensável um princípio geral de reserva sobre informação patrimonial) e particularmente permeável a fórmulas de intrusão quando em presença de interesses constitucionais (artigo 18.º, n.º 2, da Constituição da República Portuguesa)."
(v. Acórdão do TC n.º 679/2022 e, também, n.ºs 680/2022, 756/2022 e 177/2023)

No âmago desta questão coloca-se a extensão do direito à privacidade a *pessoas coletivas*, especialmente nos casos em que a respetiva estrutura jurídica não assente em substrato pessoal ou este seja pouco valorizado (v. g., sociedades de capitais e fundações), ou a outros veículos, ainda que desprovidos de personalidade jurídica, que se achem dotados de subjetividade suficiente para agirem no tráfego jurídico (v. g., fundos de investimento ou outros patrimónios coletivos). Será neste domínio que o caráter *empresarial* da informação será mais nítido, bem como a insipidez da sua associação com a pluridimensionalidade da personalidade humana que a privacidade tutela.

Também aqui, a questão é controversa, mas será seguro afirmar que, quando se reconheça existir tutela constitucional, se tratará de um espaço dotado de grande plasticidade e permeável a medidas legislativas que representem ingerências no exclusivo autogestionário da informação:

"o direito à reserva de privacidade reconhecido no artigo 26.º, n.º 1, da Constituição da República Portuguesa tem como perspetiva e objeto de observação o Ser Humano, na sua individualidade, intimidade e endogenia, pelo que, em princípio, dir-se-ia que as pessoas coletivas, ao menos quando se trate de entidades instrumentais ao desenvolvimento de uma atividade económica (maxime, sociedades comerciais), estariam excluídas do âmbito de tutela do direito. Estes entes coletivos são apenas uma forma de organização de interesses empresariais, achando-se por isso distantes, por sua própria natureza e pelos princípios ordenadores desse escopo jurídico, do núcleo de valores constitucional em que assenta o direito à reserva de intimidade da vida privada, razão por que a respetiva proteção resulta excluída (v. artigo 12.º, n.º 2, da Constituição da República Portuguesa).

O Tribunal Constitucional expressou já dividas sobre esta matéria, assinalando que a inclusão no espaço de defesa da privacidade "é problemática em relação às pessoas coletivas, muito particularmente as sociedades comerciais, pelo facto de não valerem (ou, pelo menos, de não valerem de igual modo), em relação a elas, as considerações fundamentadoras acima aduzidas, que se apoiam na possibilidade de acesso à esfera mais pessoal" da pessoa humana (v. Acórdão n.º 442/2007). Frontalmente contra, já se defendeu:

«Considero que a inclusão do sigilo bancário de que sejam titulares pessoas coletivas no âmbito de proteção do direito à reserva da intimidade da vida privada, consagrado no n.º 1 do artigo 26.º da Constituição, não será apenas problemática, como o acórdão concede (n.º 16.2, último parágrafo), mas é, mais radicalmente, de afastar. E, como só na medida em que constitui irrefracção deste direito à reserva da privacidade se me afigura possível dar garantia ao sigilo bancário no elenco dos direitos fundamentais, entendo que o legislador não está subordinado, no reconhecimento e conformação do sigilo bancário relativamente a pessoas coletivas (e entes equiparados), ao regime constitucional dos direitos, liberdades e garantias.

Efectivamente, os direitos fundamentais são primordialmente direitos de indivíduos, de pessoas singulares.
(...)



406
X

TRIBUNAL CONSTITUCIONAL

(...) o que pode justificar que aspectos do "segredo do ter" da pessoa, patentes na conta e outros dados da situação económica do titular em poder de uma instituição bancária, sejam assimilados ao "segredo do ser" protegido pela reserva da intimidade da vida privada é o que esses elementos podem revelar das escolhas ou contingências de vida do indivíduo, dos seus gostos e propensões, do seu perfil concreto enquanto ser humano, que cada um deve ser livre de resguardar do conhecimento e julgo moral de terceiros. Esta teleologia intrínseca surge eminentemente ligada à proteção da dignidade da pessoa humana, não sendo extensível a entes que apenas tem uma capacidade jurídica funcional, limitada pelo princípio da especialidade do fim que estatutariamente prosseguem, que não têm projecto de vida livremente determinado, pelo que o direito ao segredo bancário que contratual e legalmente se lhes reconheça não goza da proteção constitucional especificamente conferida pela inclusão do bem protegido pelo sigilo no âmbito do direito à reserva da intimidade da vida privada, consagrado no n.º 1 do artigo 26.º da Constituição».

(voto de vencido do Cons. Vitor Gomes ao Acórdão do TC n.º 442/2007)

Esta posição, porém, não é congruente com a aceitação de uma dimensão de ordem económica do direito à privacidade, que, ainda que volátil e permissiva a ingerências quando em presença de valores constitucionais, se reconhece contida no artigo 26.º, n.º 1, da Constituição da República Portuguesa, como acima assinalado. Não se perceberia que, de um lado, fosse reconhecida a uma pessoa privatividade sobre informação relativa a titularidade de bens e a atos e negócios de natureza económica, quando observada ou agindo singularmente, e, de outro, se lhe negasse qualquer forma de tutela constitucional quanto às mesmas informações quando se acbe associada a outras numa estrutura jurídica de organização de interesses, ou quando, agindo singularmente, se enroupe de uma fórmula jurídica de idêntica natureza (v. g., sociedades unipessoais).

Poder-se-ia contrapor que certas entidades coletivas – dotadas de personalidade jurídica, ou de subjetividade bastante para que lhes seja possível atuar no trânsito jurídico com autonomia: (v. g.) sociedades de capitais, fundos de investimento ou fiduciários, fundações e estabelecimentos estáveis, etc. – não possuem substrato pessoal tangível que permitisse caracterizar a titularidade do negócio e a prática de atos por pessoas, antes se reduzindo a formas de organização de acervos patrimoniais ou a fórmulas de investimento financeiro de caráter estrito, tornando ainda mais fantástica a sua equiparação, para efeitos de tutela, ao Ser Humano.

A nosso ver, o problema aqui está invertido: em último termo, qualquer uma destas entidades tem por atributo essencial a titularidade de bens e a realização de operações económicas por uma (ou mais) pessoa humana, por vezes apelidada de beneficiário efetivo (cfr. Lei n.º 89/2017, de 21 de agosto), que, de uma maneira ou de outra, será também a última responsável pela respetiva gestão; o exposto, porém, já se pode entender altamente ilustrativo da insipidez e da tibieza da informação económica para que a sua exposição possa impactar na integridade do indivíduo e se possa entender abarcada por um direito fundamental dirigido à tutela da confidencialidade sobre a vida pessoal e familiar; quando distilada para o seu estado purificado, como é o caso quando a encontramos associada a uma estrutura jurídica de interesses e de investimento, obtemos prova de que a informação económica pouco ou nada revela sobre os conteúdos humanos do indivíduo a que respeita e que se acobertam pelo artigo 26.º, n.º 1, da Constituição da República Portuguesa.

Assim, se se pode admitir que as entidades coletivas beneficiem de privacidade e exclusividade gestionária sobre a sua informação pessoal (...) a sua natureza exclusivamente económica e a sua estrita contextualização nesse âmbito colocará a tutela num espaço ainda mais periférico do espectro de defesa definido pelo artigo 26.º, n.º 1, da Constituição da República Portuguesa, resultando tanto mais permeável a ingerências fundadas em valores constitucionais (artigo 18.º, n.º 2, da Constituição da República Portuguesa)."

(v. Acórdão do TC n.º 679/2022 e, também, n.ºs 680/2022, 756/2022 e 177/2023)

Daqui resulta, portanto, que, ainda que não de forma comparável à proteção conferida a pessoas singulares, o arquivo de correio eletrónico de uma empresa será credor de proteção pela privacidade, conferindo o respetivo exclusivo de gestão e de disposição à titular. Uma ingerência



TRIBUNAL CONSTITUCIONAL

407
X

de autoridade pública em qualquer um desses elementos exprime também tensão com a *liberdade de empresa* (artigo 61.º, n.º 1, da Constituição da República Portuguesa), enquanto garantia de desenvolvimento de uma atividade económica liberta de interferências estaduais (v. J. GOMES CANOTILHO e VITAL MOREIRA, *op. cit.*, p. 546) e a convergência de ambos define um corpo normativo dirigido de forma específica à defesa da “*eficácia e racionalidade do funcionamento do estabelecimento segundo o critério e os interesses do legítimo titular*”, al adquirindo relevo “*a tutela da reserva e do segredo (...) contra a devassa e a espionagem da concorrência*” (v. M. COSTA ANDRADE, *Commentário Conibrianus...*, p. 718), também na dimensão colocada pelo artigo 18.º, n.º 1, alínea c), do RjdC.

Sobre o objeto desta proteção, cabe sublinhar que “*a inviolabilidade das instalações das empresas visa proteger, muito particularmente, as estratégias industriais e comerciais das empresas em relação ao mercado e aos poderes públicos*”, *maxime* os seus “*segredos de negócio*” (M. P. ANTUNES, *op. loc. Cit.*, p. 108) e será relativamente a esta tipologia de elementos informacionais, potencialmente integrados em mensagens arquivadas ou reveláveis pela quebra da sua confidencialidade, que os poderes de busca e apreensão da AdC conferidos pela norma fiscalizada materializam uma medida de intrusão.

Uma última nota para assinalar que a tutela da privacidade, no plano em causa, não resguarda a posição do *remetente* de uma mensagem em arquivo, atendendo a que, com o envio, este perde o controlo sobre a informação, cedendo-a a entidade terceira e, assim, precludindo qualquer expectativa de que fosse gerida de acordo com a sua vontade (fosse o caso da preservação de reserva ou de confidencialidade): porque nos achamos em contexto profissional e empresarial, fora do espaço de defesa da informação íntima ou personalística, endógena ao indivíduo, não existe cobertura constitucional nesta dimensão, tal como não existe nos casos em que essa informação seja transmitida de outra forma a terceiros (em diálogo, por carta, por telefone, pela utilização de páginas públicas em redes sociais ou por qualquer outro meio de comunicação à distância).

Serve por dizer, e em suma, o artigo 18.º, n.º 1, alínea c), do RjdC, coloca em causa o direito constitucional (resultante do direito à privacidade) de autodeterminação informativa sobre dados de ordem económica que, em convergência com a liberdade de empresa, concretizam uma garantia de integridade e de reserva da empresa-objeto (artigos 26.º, n.º 1, e 61.º, n.º 1, ambos da Constituição da República Portuguesa). Este espaço de tutela constitucional, porém, não desempenha uma função especialmente relevante de proteção da pessoa humana, pelo que o



TRIBUNAL CONSTITUCIONAL

âmbito de garantia efetiva será muito mais estreito que o conferido à reserva da vida íntima, caracterizando-se como um perímetro defensivo tributário de interesses de ordem económica.

Importará, pois, avaliar o programa sob sindicância de acordo com estes parâmetros.

12.3. No que respeita ao direito à *autodeterminação informacional* (artigo 35.º, n.º 4, da Constituição da República Portuguesa) e na medida em que constitui uma garantia autónoma (v. J. GOMES CANOTILHO e VITAL MOREIRA, *op. cit.*, p. 51 e M. P. RIBEIRO DE FARIA *in Constituição Portuguesa Anotada*, coord. J. MIRANDA e R. MEDEIROS, Univ. Católica Ed., 2017, p. 569), este tem por finalidade “*evitar intromissões abusivas na vida privada das pessoas através da recolha e tratamento de dados pessoais informatizados*”, mas numa perspetiva mais abrangente quanto à natureza da informação, já que acoberta toda a que seja referenciável a uma pessoa humana ou que permita identificá-la. O alargamento da garantia pretende assegurar “*que a pessoa não é usada como fonte de informação para terceiros contra a sua vontade, podendo além disso controlar a informação que é fornecida e os termos e abrangência em que ela é tratada*” (v. M. P. RIBEIRO DE FARIA, pp. 569-570), ainda que não se inscreva na sua intimidade, que é dizer, no âmbito de tutela que é próprio à proteção dos elementos da vida privada.

A autonomização desta forma de tutela dos dados pessoais decorre da tendência para a dispersão e difusão da informação pessoal contida em ficheiros eletrónicos em ambiente digital, que rapidamente é convertida em mercadoria transacionável por operadores do setor. Isto significará que nem apenas a informação característica do núcleo individual de um Ser humano se compreende no objeto de proteção, mas também os dados relativos à sua situação económico-financeira, que naturalmente possuem utilidade e valor na elaboração de perfis ou de hábitos de consumo (v. g.), já que diretamente o referenciam (nesse sentido, são «dados pessoais»).

O exposto não prejudica a afirmação, porém, que se trata de um âmbito de proteção diretamente ligado à defesa da personalidade, o que, de resto, resulta textualmente do preceito (“*É proibido o acesso a dados pessoais de terceiros*”), razão por que organizações de meios ou instrumentos de investimento, possuam ou não personalidade jurídica, não beneficiam da proteção conferida pela norma: “*Sendo um direito eminentemente pessoal, também não faz sentido, como se viu, distendê-lo às pessoas coletivas (art. 12.º-2), com a possível exceção do n.º 1, com as devidas adaptações. De resto, o preceito tem a ver essencialmente com «dados pessoais» (n.ºs 2, 3, 4, 6 e 7), que não têm aplicação a pessoas coletivas.*” (v. J. GOMES CANOTILHO e VITAL MOREIRA, *op. cit.*, p. 558). Assim sendo, estamos já em posição de concluir



TRIBUNAL CONSTITUCIONAL

409
R

que a defesa realizada nestes autos sobre a privatividade de mensagens eletrónicas e exclusivo autogestionário da empresa titular ao abrigo da autodeterminação informacional não tem mérito.

Já se afigura inegável, porém, que mensagens constantes dos arquivos da empresa visada pela investigação possuirão informações desta natureza relativas a terceiros, ou seja, que o correio eletrónico armazenado em aparelhos locais da entidade buscada ou em servidores conterá dados referenciáveis a uma pessoa (incluindo administradores e trabalhadores) e que, nesse pressuposto, estarão a coberto da autodeterminação informacional. Inclui-se aqui não apenas o *conteúdo* das mensagens, mas também *metadados* dos ficheiros que as suportam, já que também por via deles é possível conhecer o perfil de um indivíduo e representar atributos a ele característicos (v., Acórdãos do TC n.ºs 687/2021, 268/2022 e 800/2023). Esta forma de tutela subsiste ao fluxo de comunicação, seja quem for que controle a informação, por isso estendendo proteção aos bancos de dados de arquivos webmail empresariais (v. J. GOMES CANOTILHO e VITAL MOREIRA, *op. cit.*, p. 558).

No entanto, impõe-se levar em conta que se toda a informação referenciável a um indivíduo estará protegida pela autodeterminação informacional, a garantia efetiva deste direito não será insensível à natureza da informação que esteja em causa. No caso em mãos, tratamos de contas de webmail de caráter empresarial e os dados em causa, sendo assim, não serão passíveis de referenciar os atributos mais identificadores e reservados de alguém, mas essencialmente os *factos económicos* em que esteve envolvido. Por outro lado, porque a pesquisa e apreensão de mensagens se encontra vinculada à instrução probatória de procedimentos contraordenacionais, temos que a lesão se caracteriza por um caráter cirúrgico e condicionado, já que, em função de objeto e formas de utilização, esta não é associável aos riscos específicos a que a norma constitucional oferece resposta.

A autodeterminação informacional “põe em relevo que o perigo da informática para a esfera privada resulta, sobretudo, da perda de controlo dessas informações [pessoais], que podem vir a ser adisfrutivamente utilizadas, e com grande rapidez, por um grande número de pessoas e entidades, para fins que o interessado não conhece e em relação aos quais não tem qualquer possibilidade de intervenção”. (v. J. GOMES CANOTILHO e VITAL MOREIRA, *op. cit.*, p. 558.). A norma responde, pois, essencialmente aos riscos inerentes à recolha, processamento e difusão da informação no ambiente digital, que é dizer, ao “alargamento das possibilidades de recolha e de armazenamento de dados relativos ao cidadão individual” perante “a facilidade e a velocidade de acesso e de cruzamento de todos esses dados” (v. M. P. RIBEIRO DE FARIA *op. cit.*, p. 571). Temos então, por um lado, a aptidão do formato digital para reter volumes massivos de dados de



4910
X

TRIBUNAL CONSTITUCIONAL

natureza pessoal, associada à valência de replicação ilimitada e, por outro, a voracidade de agentes económicos cujo modelo de negócio assenta na monetarização desta categoria de informação.

A concorrência destes fatores conduz à dispersão de informação referenciável a pessoas por uma rede em que cada ponto de chegada multiplica as linhas de expansão pré-existentes, descrevendo uma linha de progressão exponencial até infinito do potencial de difusão dos dados. Daqui decorre o inerente “*risco de uma recolha injustificada de dados suscetível de constituir por si só uma intrusão ilegítima na vida privada das pessoas e uma compressão das suas liberdades (não tanto pela sua natureza, como pela desnecessidade ou natureza infundada dessa recolha), como o uso e divulgação sem limites desses dados pode gerar designaldades de tratamento e riscos de exclusão.*” (v. M. P. RIBEIRO DE FARIA *op. cit.*, p. 571).

São, portanto, os atributos da tecnologia digital para acumulação de informação, a proliferação de pontos de extração e a disponibilidade de uma rede de comunicações global, incontrolada (e incontrolável) que, associada à eficiência e velocidade dos circuitos de trânsito de dados, corporizam o perigo específico para a integridade moral da pessoa humana a que responde a norma do n.º 4, do artigo 35.º, da Constituição da República Portuguesa, restitutiva do exclusivo autogestionário dessa informação ao seu titular e obstativa do seu acesso e *broadcasting* por terceiros.

Pois bem, afigura-se bastante evidente que uma diligéncia de busca e de apreensão de mensagens webmail no âmbito de um processo contraordenacional com recurso a ferramentas eletrónicas não sinaliza este perigo de nenhuma forma importante, pelo menos não mais que a generalidade das diligências instrutórias e das operações de obtenção de prova.

Desde logo, a utilização de conteúdos pelas autoridades é legalmente vinculada e cinge-se às necessidades probatórias do processo, não se destinando a replicação e não se enquadrando nos circuitos de dispersão de dados: a informação apreendida não será cedida, tanto menos colocada à disposição de um universo indiferenciado de sujeitos no espaço web ou em qualquer outro, antes constituirá componente de prova num processo específico, beneficiando do resguardo proporcionado por normas de competência e de titularidade. Em segundo lugar, a finalidade a que o objeto da pesquisa fica adstrito representa a depuração de todos os dados que não interessem ao processo, o que, por seu turno, implicará a preservação da reserva e seu âmbito de eficácia sobre a generalidade dos dados examinados, resguardando os seus titulares legítimos da sua exposição.

O instituto do artigo 18.º, n.º 1, alínea c), do RJdC, não é mais, em essência, que a *adaptação para a tecnologia digital* de uma operação de busca e apreensão em instalações de empresa de

411
L

TRIBUNAL CONSTITUCIONAL

documentos físicos constantes de arquivos, distinguindo-se pela introdução de diferentes recursos (*software* de pesquisa) e pela natureza informática do objeto (ficheiros digitais), não pela amplitude do impacto na reserva de informação que representa para as pessoas visadas. A informação acedida pelas autoridades será *rigorosamente a mesma* que numa busca tradicional: não se observa, mesmo em tese, maior potencial para a exposição de dados pessoais da que decorreria do acesso a um arquivo de correspondência tradicional instalado em mobiliário e do manuseamento de pastas e dossiers contendo missivas e envelopes percorrendo anos ou décadas de atividade da empresa.

Dir-se-á, em oposição ao exposto, que o acesso constitui uma intromissão mais intensa em face da aptidão incomparável das bases digitais para acumularem dados e que a sua circulação via webmail é mais profícua em informação do que a correspondência tradicional alguma vez foi.

Assinala-se uma vez mais que o artigo 18.º, n.º 1, alínea c), do RJDc, se confina ao acesso aos *arquivos digitais de uma empresa ou de uma associação de empresas*, razão por que a ingerência estará confinada aos elementos relacionados com as respetivas atividades, à inteira semelhança do que sucederia com arquivos corpóreos. Não há razão para presumir que uma empresa reterá mais informação em formato eletrónico sobre terceiros (pessoas singulares) do que aquela que reteria em suporte de papel, já que o que orienta e motiva a organização de arquivo é a *utilidade* que a informação representa para a gestão enquanto *instrumento económico*, não qualquer outro fator.

É, de resto, francamente capcioso que se pretenda associar um meio de reunião de prova desta natureza e limitado pelo descrito escopo à generalização de práticas predatórias sobre dados que se observa no espaço web, estas assentes na pobre sofisticação dos utilizadores, no oceano de informação disponível e na sua convertibilidade em mercadoria transacionável nesses círculos, situação tanto mais distinta quando aí impõe a ausência ou insuficiência de parâmetros de regulamentação: a informação que é alvo de pesquisa e apreensão será mais, ou menos, abundante, em função do que seja a dimensão da atividade da empresa e o uso que faça de correspondência eletrónica, à semelhança, *mutatis mutandis*, do que sucederia quanto a registos de atividade corpóreos.

Embora, como vimos, responda aos perigos específicos inerentes às tecnologias de informação (v. epígrafe do artigo 34.º da Constituição da República Portuguesa), é de assinalar que a autodeterminação informacional não está limitada ao suporte eletrónico, distendendo-se também à contida em documentos corpóreos ("*ficheiros manuais*" – artigo 35.º, n.º 7, da Constituição da República Portuguesa; v. J. GOMES CANOTILHO e VITAL MOREIRA, *op. cit.*, p. 557). Acresce que



4r2
K

TRIBUNAL CONSTITUCIONAL

este direito fundamental está consagrado na Lei Fundamental desde a reforma de 1982 (artigo 35.º, n.º 2, da Constituição da República Portuguesa, na redação conferida pela Lei n.º 1/82, de 30 de setembro): desde então e até à data de hoje, porém, não se conhece doutrina ou jurisprudência que haja caracterizado a requisição ou apreensão por autoridades de documentos em suporte de papel contendo dados pessoais (em processos administrativos, fiscais, judiciais ou quaisquer outros), ou buscas tendentes a localizá-los, como fórmula de tutura, ou de extraordinária lesão, desta garantia.

Por tudo, resulta seguro concluir que a norma do artigo 18.º, n.º 1, alínea c), do RJdC, na interpretação questionada, se conforma uma ingerência no direito conferido pelo n.º 4, do artigo 35.º, da Lei Fundamental, pois que importa a pesquisa e acesso por autoridades públicas a bases de dados compreendidos no seu âmbito de tutela, caracteriza-se pelo grau moderado e condicionado, que partilha com a generalidade dos meios de obtenção de prova admitidos em Direito.

12.4. Sobre a Necessidade de Autorização Judicial prévia

12.4.1. Na interpretação normativa sindicada, a realização da operação de busca e apreensão de mensagens eletrónicas é realizada pela AdC sob autorização de Magistrado do Ministério Público, dispensando autorização prévia ou validação judicial. O Acórdão do TC n.º 91/2023 entendeu que esta ação para reunião de prova dependeria de autorização prévia por Juiz em observância da reserva jurisdicional contida no n.º 4, do artigo 32.º, da Constituição da República Portuguesa, adotando a jurisprudência firmada pelo Acórdão n.º 687/2021 e concluindo por juízo positivo de inconstitucionalidade material com esse fundamento. Essa posição é também defendida pelos recorrentes nestes autos.

Ora, em primeiro lugar, ambos os Acórdãos (como os recorrentes) sinalizam uma intrusão na tutela das comunicações (artigo 34.º, n.º 4, da Constituição da República Portuguesa), o que, como já vimos, não é a forma adequada de observar norma que capacite a AdC a realizar operações de busca e apreensão de mensagens armazenadas em sistemas informáticos, sejam eles locais ou diretamente acessíveis a partir de sistemas locais (desde que não importem a intercetação de fluxos de transmissão de dados entre sistemas), como sucede pelo artigo 18.º, n.º 1, alínea c), do RJdC.

Em segundo lugar, o Acórdão do TC n.º 687/2021 censurou uma norma de *processo criminal* (Lei n.º 109/2009, de 15 de setembro, a Lei do Cibercrime), como tal subordinada a um regime

413
K

TRIBUNAL CONSTITUCIONAL

constitucional particularmente sensível quanto a garantias de defesa (artigo 32.º da Constituição da República Portuguesa) e que não é diretamente transponível para outros ramos do Direito punitivo, seja o caso da Lei processual das contraordenações (v. Acórdãos do TC n.ºs 573/98, 189/01, 659/2006, 73/2007, 313/2007, 632/2009, 95/2008, 552/2008, 589/2008, 355/2012, 612/2014, 143/2016, 508/2016 e 459/2022), como também já tivemos oportunidade de sublinhar antes.

Vendo melhor, o quadro de garantias de processo criminal ocupa-se em reforçar a proteção da pessoa visada contra a perspetiva de condenação em processo-crime, levando em conta a violência das lesões que pode importar na sua esfera pessoal (*maxime*, prisão – cfr. artigo 27.º, n.ºs 2 e 3, alíneas b) e h), da Constituição da República Portuguesa) e o seu estatuto maximizado de direitos e de garantias caracteriza o devido *due process of law*. Não estamos perante, pois, um *regime geral das intrusões na privacidade, na liberdade empresarial e na autodeterminação informatacional* – ou em quaisquer outros direitos, liberdades ou garantias –, que pudesse ser generalizado: a aplicação da jurisprudência do Acórdão do TC n.º 687/2021 à norma sindicada deslocaliza a solução aí encontrada dos fundamentos materiais de que se socorre, já que, no Acórdão do TC n.º 91/2023, como no caso *sub iudicio*, não se debate a adjetivação de uma pretensão punitiva de natureza penal.

De maior importância, sobre a jurisprudência firmada por aquele arresto, se se aceita e aplaude que “*a intervenção judicial constitui uma garantia adicional de ponderação dos direitos e liberdades atingidos no decurso da investigação criminal*” (Acórdão do TC n.º 687/2021), a afirmação que *qualquer forma* de intrusão em direitos fundamentais em processo-crime apenas dispensa autorização por Juiz a título de exceção, devendo cingir-se a “*situações pontuais e definidas com rigor, em que não constitua um meio excessivo para prosseguir interesses particularmente relevantes de investigação criminal*”, designadamente “*atuações preventivas on canteiros, em que haja particular urgência ou perigo na demora no que toca à conservação de elementos probatórios, e desde que se assegure uma posterior validação judicial da atuação das autoridades competentes*” ou situações análogas (*ibidem*), é, a nosso ver, francamente excessiva.

Isto, desde logo, porque não será fácil encontrar *uma única* medida de obtenção ou de produção de prova em inquérito que não conforme nenhum tipo de ingerência num direito fundamental (de estrutura defensiva), ainda que moderada ou pouco expressiva, seja (v. g.) a convocação obrigatória e sujeição a interrogatório de testemunhas, de assistente ou de arguido (o direito a *estar só*, coevo à reserva da vida privada), a requisição ou apreensão de objetos e de documentos (o direito ao património, o direito à autodeterminação informativa e informacional),

2/4
X



TRIBUNAL CONSTITUCIONAL

ou uma diligência de reconhecimento (o direito à imagem e o direito à não autoinculpação) (cfr. artigos 26.º, n.º 1, 32.º, n.º 2, 35.º, n.º 4 e 62.º, n.º 1, todos da Constituição da República Portuguesa).

Colocar na dependência de autorização pelo juiz de instrução a prática de *todo e qualquer* ato desta natureza significaria uma compressão excessiva dos poderes do Ministério Público, importando a sua equiparação a uma qualquer força de polícia com competências em matéria penal e aproximando o inquérito do modelo de investigação presidida por Juiz. Esta solução representa a abrogação das atribuições constitucionais do Ministério Público, a quem incumbe o *exercício autónomo* da ação penal (artigo 219.º, n.º 1, da Constituição da República Portuguesa), de que deriva competência para iniciativa de inquérito e, por inerência, poderes de direção da investigação.

Acresce ainda que estes poderes se entendem garantia e consequência da efetiva separação orgânico-subjetiva entre órgão acusador e os titulares de funções jurisdicionais em matéria criminal (Juízes), emprestando alcance prático ao princípio do acusatório (artigo 32.º, n.º 5, da Constituição da República Portuguesa – v. J. GOMES CANOTILHO e VITAL MOREIRA, *op. cit.*, p. 522):

“É através desta Magistratura [o Ministério Público] que se logra obter: a separação entre a entidade que há-de presidir à instrução preparatória (bojo, inquérito) e à acusação e aquela a quem há-de caber a decisão, e com a qual se visa conseguir a necessária objectividade e imparcialidade do julgamento; a possibilidade de uma instrução liberta de quaisquer pré-julgados (...) e finalmente que a acusação, determinando a vinculação temática do juiz pela exata delimitação dos seus poderes cognitivos e da extensão do caso julgado, represente uma importante garantia de defesa do arguido e dos seus direitos fundamentais.”

(J. FIGUEIREDO DIAS, *Direito Processual Penal, Clássicos Jurídicos*, Coimbra, 2004, p. 362)

Por outra parte, veja-se que, nos casos em que exige autorização judicial, a Lei Fundamental, ao impô-la, especifica certas formas de lesão nos direitos, caracterizando intrusões particularmente violentas no âmbito de tutela e que tendencialmente se traduzem na sua *nullificação*, dessa forma delimitando a reserva de Juiz a um mínimo, que circunscreve a situações peculiares e muito graves.

Assim sucede na defesa do *domicílio* (artigo 35.º, n.º 2, da Lei Fundamental), cuja reserva judicial se cinge a ações de *entrada forçada*, não outras ingerências. Pense-se (v. g.) na interdição imposta a residentes de uma habitação, depois de um acesso consentido e fora de quadro de urgência, de transitarem por um dos quartos tendo em vista recolha de prova pela polícia científica. Também aqui, estamos perante uma intrusão no perímetro de defesa do domicílio, mas que não se caracteriza por *invasão* (*entrada forçada*), sendo por isso desnecessária autorização judicial prévia.



415
R

TRIBUNAL CONSTITUCIONAL

É este também o caso de intrusões na *liberdade ambulatória* (artigos 27.º, n.ºs 2 e 3, alíneas c) a b) e c) a h), 28.º e 30.º, n.º 2), em que apenas a *privacidade* (ainda que parcial) depende de intervenção judicial, mas não outro tipo de restrições (v. Acórdãos do TC n.ºs 464/2022 e 466/2022); no *direito à permanência em território nacional* (artigo 33.º, n.ºs 2 e 7), em que se limita à expulsão ou extradição do território; na *liberdade de filiação*, que condiciona a reserva judicial à separação entre pais e filhos (artigo 36.º, n.º 6); na *liberdade associativa* (artigo 46.º, n.º 2), em que se limita a exigência de intervenção judicial à *dissolução* de pessoas coletivas, aliviando desse requisito quaisquer outros atos restritivos; e na *liberdade de empresa* (artigos 62.º, n.º 1 e 86.º, n.º 2), em que é imposta apenas quando o Estado pretenda intervir numa entidade privada, alterando a sua organização de recursos ou de governo, permitindo até exceções à obrigatoriedade de autorização judicial nesses casos.

Parece-nos muito insatisfatória, pois, a interpretação desta moldura constitucional que converta uma *regra de exceção* reservada para as lesões mais graves num grupo limitado de direitos fundamentais, em *regra de princípio* aplicável a todos eles e a qualquer forma de ingerência.

É dizer, a subordinação de ações de busca e apreensão de documentos em formato eletrónico (mensagens de webmail) integradas numa estrutura empresarial a autorização prévia por Juiz dependeria da *reformulação* do texto constitucional pelo intérprete, introduzindo, não apenas normas especiais que impusessem a intervenção judicial sobre ingerências nos valores jurídicos que se colocam, mas, ainda e também, caracterizando certo tipo de ações particularmente ofensivas desses direitos a que aquela disciplina de obtenção de prova se pudesse dizer subsumível.

Tratar-se-ia, a nosso ver, de um processo hermenêutico que não nos é, de todo, consentido.

Mais se diga, se os Acórdãos do TC n.ºs 687/2021 e 91/2023 se afirmam a si mesmos tributários do Acórdão do TC n.º 7/1987 e da jurisprudência constitucional que se sedimentou desde então, é de assinalar que este arresto fiscalizou, entre o mais, um quadro legal que autorizava *revistas e buscas não domiciliárias* sob autorização do Ministério Público (sem intervenção judicial).

O arresto concluiu que a Lei Fundamental não se opunha à desnecessidade de intervenção de juiz em resultado da articulação da tutela da privacidade com o âmbito de proibições constitucionais a prova em processo penal constante (hoje) do n.º 8, do artigo 32.º, da Constituição:

"O n.º 6 do artigo 32º da Constituição só considera nulas, no que aqui importa, as provas obtidas mediante abusiva intrusão na vida privada. Ora, sendo as revistas e buscas não domiciliárias - no âmbito, é claro, do inquérito - autorizadas ou ordenadas pelo Ministério Público - que é "autoridade judiciária" nos termos da alínea b) do nº 1 do

416
X

TRIBUNAL CONSTITUCIONAL

artigo 1º do Código - e especificando-se nos nºs 1 e 2 do artigo 174.º os casos em que elas são admitidas, não se vê que estejamos em presença de uma intromissão abusiva na vida privada. E o mesmo parece poder dizer-se, embora aí se dispense a autorização previa do Ministério Público, em relação aos casos previstos no n.º 4 do artigo 174.º, face as exigências feitas nas próprias alíneas desse número e, no caso da alínea a), ainda no nº 5 do mesmo artigo.”
(Acórdão do TC n.º 7/1987)

Este excerto do aresto possui mesmo especial importância, já que por aqui fica claro o excesso do entendimento adotado no Acórdão do TC n.º 687/2021. Esta jurisprudência introduziu novas proibições de prova com fonte constitucional (todas as que sejam obtidas com ingerência num direito fundamental, se não autorizadas por Juiz), em desrespeito pelo n.º 8, do artigo 32.º da Constituição da República Portuguesa. Embora esta norma atinja de nulidade os *elementos de prova*, por isso tendo por campo privilegiado a aplicação direta a atos processuais concretos (artigo 18.º, n.º 1, da Constituição da República Portuguesa), por ela se estabelece a proibição e recenseia o vício com relação ao *meio* por que haja sido obtida (“*obtidas mediante*”). Existem, portanto, certas atividades que são proibidas às autoridades em investigação penal, razão por que a norma define condicionantes à iniciativa legislativa quanto a modelos legais de aquisição de prova criminal.

Isto é assim, mas caso se entenda que a Lei Fundamental exige que *toda e qualquer* intrusão em direitos fundamentais operada por meios de obtenção de prova estará sujeita a autorização judicial, isso equivaleria a uma nova (e extensa) proibição sobre prova e sobre meios de obtenção de prova com fonte constitucional, representando uma distensão abrogante do catálogo definido no artigo 32.º, n.º 8, do diploma (“*tortura, coação, ofensa de integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio ou nas telecomunicações*”). Na verdade, enquanto a norma cinge o vício de nulidade que estatui a prova obtida mediante intromissão *abusiva na vida privada, no domicílio ou nas telecomunicações* – o que incluirá os casos de intrusão nestes direitos sem autorização judicial, quando seja constitucionalmente obrigatória – o Acórdão do TC n.º 687/2021 estendeu esta lógica à intromissão em *qualquer* direito fundamental, que se haverá como abusiva *sempre* que não exista autorização judicial, já que a entende necessária em *todos* os casos (salvo situações de urgência).

Trata-se de uma expansão imensa da nulidade de fonte constitucional de meios de prova, já que não é defensável que ações de reunião de elementos probatórios como as exemplificadas *supra* (inquirição de testemunha, apreensão de objetos ou diligências de reconhecimento) pudessem ser equiparáveis às situações extremas de lesão da personalidade de particulares a que se reporta o artigo 32.º, n.º 8, da Lei Fundamental, em que pontifica a “*tortura*”.



4/18
d

TRIBUNAL CONSTITUCIONAL

Toda a questão transporta consigo a dificuldade de compreender a reserva de competência exclusiva a Juiz (indelegável noutras entidades) sobre os atos de “*toda a instrução*” que envolvam direitos fundamentais, *ex n.º 4, do artigo 32.º, da Constituição da República Portuguesa*. O Acórdão do TC n.º 687/2021 (e, com ele, também o aresto n.º 91/2023) parece daqui extrair a regra de que qualquer ato de inquérito estará subordinado a autorização judicial quando envolva intromissões nesta categoria de direitos, sem qualquer outra variável a isso obstativa, daí concluindo pela inconstitucionalidade de qualquer meio de recolha de prova neles ingerente que a dispense.

Não é fácil perceber a que se reporta o termo “*instrução*” presente na norma e a doutrina dá nota disso mesmo (v. J. GOMES CANOTILHO e VITAL MOREIRA, *op. cit.* pp. 520-521 e GERMANO MARQUES DA SILVA e H. SALINAS, *in Constituição Portuguesa Anotada*, coord. J. MIRANDA e R. MEDEIROS, Univ. Católica Ed., 2017, pp. 528-529), mas se se concluir que inclui a fase de inquérito e respetivas operações de obtenção de prova, como pretende aquela parte da jurisprudência, isso significará que *não basta* autorização judicial para a prática desses atos: a norma atribui competências a Juiz *exclusivas e indelegáveis*, o que significa que as diligências teriam de ser por ele realizadas ou, ao menos, por ele *presididas*, com inerentes poderes de apreciação de conveniência e oportunidade.

Isto significaria que toda a recolha de prova em inquérito teria de ser realizada (ou, no mínimo, presidida) por Juiz, já que, como vimos, a generalidades dessas operações corporizam algum tipo de ingerência em direitos defensivos. Esta solução, como parece evidente e acima adiantámos, representaria uma invasão das atribuições de *exercício autónomo da ação penal* conferidas ao Ministério Público, confrontando o seu estatuto constitucional e descharacterizando o princípio do acusatório (artigos 219.º, n.º 1 e 32.º, n.º 5, ambos da Constituição da República Portuguesa).

A forma de compreender a norma preservando e com ela conciliando o estatuto constitucional do Ministério Público e a estrutura acusatória do processo-crime, será entender “*a instrução*” referida no n.º 4, do artigo 32.º, da Constituição da República Portuguesa, como a fase de controlo jurisdicional do inquérito (*maxime*, da decisão final), esta também uma garantia de defesa tributária do princípio do acusatório (v. J. GOMES CANOTILHO e VITAL MOREIRA, *op. cit.* p. 522), hoje regulada nos artigos 286.º a 310.º do CPP (neste sentido, v. GERMANO MARQUES DA SILVA e H. SALINAS, *op. cit.*, p. 529). A norma imporá que, durante este estádio, o processo transite para titularidade por Juiz, a quem será admitido delegar certos atos, mas não quando contendam com direitos fundamentais, seja exemplo operações de produção ou de reunião de prova (o juiz não



418
L

TRIBUNAL CONSTITUCIONAL

poderá, v. g., delegar nas polícias a inquirição de uma testemunha ou no Ministério Público a presidência de uma diligência pericial – é este o regime consagrado no artigo 290.º, n.º 2, do CPP).

Inscrita nas competências jurisdicionais ficará também a autorização ou validação de atos de *inquérito* que disso dependam, mas, tratando-se de uma competência que não resulta do n.º 4, do artigo 32.º, da Lei Fundamental, isso decorrerá de normas ou de regimes normativos que exprimam a respetiva obrigatoriedade, dispersos pelo texto constitucional, à semelhança das normas que conferem ao Juiz competência *decisória* em sentido próprio durante a investigação (v. g., a aplicação de prisão preventiva ou de outras medidas de coação ou a detenção para comparência a ato de inquérito; artigos 28.º, n.º 1 e 27.º, n.º 3, alínea f), ambos da Constituição da República Portuguesa).

Será esse o caso da realização de buscas através de *invasão* de domicílio (artigo 34.º, n.º 2, da Constituição da República Portuguesa). De sua parte, porque a autodeterminação comunicativa partilha com o domicílio o estatuto de inviolabilidade (cfr. artigo 34.º, n.º 1, da Constituição da República Portuguesa) e de invalidação constitucional de elementos probatórios resultantes de intrusões no seu âmbito de defesa (cfr. artigo 32.º, n.º 8, da Constituição da República Portuguesa), impõe-se igual disciplina quanto a meios de obtenção de prova que constituam *invasão* de processos comunicativos (v. g., escutas telefónicas e outros meios de interceptação de comunicações): também estes, pois, reclamarão por autorização judicial prévia para que não se entendam *abusivos* (a consagração expressa no artigo 34.º, n.º 4, da Lei Fundamental, sendo assim, seria redundante).

Diferentemente, a privacidade apenas partilhará o regime de autorização judicial obrigatório quando constitua intromissão na *vida privada* em sentido próprio, ou seja, quando represente um ataque ao espaço de defesa mais intenso do direito a privacidade. Na verdade, apenas aí se encontra um registo *personalístico* da informação – com inerente aptidão para lesar a dignidade humana e a integridade moral do indivíduo – equiparável ao objeto de tutela do domicílio e da comunicação (ambos, de resto, irradiações especiais dessa esfera central do direito a privacidade; v. J. GOMES CANOTILHO e VITAL MOREIRA, *op. cit.* pp. 543-546 e 551; A. R. FIDALGO, *Autorização Judicial e Legalidade nas Buscas domiciliárias*, in *Prova Criminal e Direito de Defesa*, Coord. T. PIZARRO BELEZA e F. L. da COSTA PINTO, Almedina, 2010, pp. 162-165), permitindo por isso compreender o tratamento paritário constante do artigo 32.º, n.º 8, da Constituição da República Portuguesa. Esta assimilação dependerá ainda de um grau de lesão suficiente no bem jurídico que justifique a equiparação conceptual à tipificação das demais intrusões abarcadas na norma, excluindo ingerências pouco

419
R

TRIBUNAL CONSTITUCIONAL

significativas e que se possam dizer absorvidas pela efetivação de outro valor constitucional (será este o caso, v. g., da intrusão no *direito a estar só*, inscrito na defesa da reserva da vida privada e familiar prevista no artigo 26.º, n.º 1, da Lei Fundamental, que a sujeição a interrogatório importa).

Sendo assim, ficará também excluída da solução a perimetria exterior do âmbito de tutela da privacidade, onde se localiza a proteção de informação económica, *maxime* empresarial.

Neste mesmo sentido, se a defesa constitucional da empresa-objeto é realizada pela associação de direitos integrados no elenco de direitos, liberdades e garantias (direito à privacidade de ordem económica e autodeterminação informacional) a um direito dotado de dimensão defensiva de força jurídica equiparada (artigo 17.º da Constituição da República Portuguesa) (a liberdade de empresa), o Acórdão do TC n.º 7/1987 nisso não divisou fundamento para concluir pela necessidade de autorização judicial para operações de busca a estabelecimento. O argumento central reside, como vimos, no facto de nada no texto constitucional o impor, conquanto a ingerência não implica a quebra do direito a reserva da *vida privada* na sua dimensão pessoal e íntima.

De resto, desde 1987 que o regime do processo penal de buscas em estabelecimento dispensa autorização por Juiz (cfr. artigos 174.º, n.os 2 e 3, 176.º e 177.º, n.º 1, todos do CPP), sem que doutrina ou jurisprudência venham questionando a conformidade constitucional desta solução. Seria francamente ousado afirmar que, desde 1987 e até à data presente, todas as diligências de busca em empresas (e outros espaços não-domiciliários) destinadas à recolha de informação relevante para inquéritos criminais, designadamente em suporte documental, foram realizadas (e a prova delas obtida valorada em juízo) em violação da Constituição da República, já que todas elas importaram alguma medida de lesão na privacidade de ordem económica, na autodeterminação informacional e na liberdade de empresa, todos eles parte do elenco de direitos fundamentais.

A jurisprudência do Acórdão n.º 7/1987, que sem nenhuma dúvida aplaudimos, foi reiterada, pelo menos, nos Acórdãos n.os 67/97 (este, com relação a uma diligência de busca a uma *garagem*, também espaço não-domiciliário), 593/2008 e 596/2008 (este, remetendo para o segundo). O mesmo entendimento está também implícito no Acórdão do TC n.º 452/89, que deixou na dependência da qualificação de «*caravanas*» como «*domicílio*» a conclusão que alcançou sobre a necessidade de autorização judicial para realização de ações de busca por polícia nas primeiras.

Aproximando a exposição a que nos dedicamos do caso *sub iudice*, os arrestos n.os 593/2008 e 596/2008 ocuparam-se, precisamente, da conformidade constitucional dos poderes de *busca em*

420
e

TRIBUNAL CONSTITUCIONAL

estabelecimento conferidos à AdC pelo regime da concorrência, sob autorização do Ministério Público e sem autorização judicial. Citarmos do primeiro:

“A alegação põe em confronto directo o disposto no n.º 2 daquele preceito com o direito à inviolabilidade do domicílio (artigo 34.º, n.º 1, da CRP) e as condições legitimantes da sua restrição, fixadas no n.º 2 do mesmo artigo. Na verdade, a norma questionada faz depender a realização das diligências previstas na alínea c) do n.º 1 do artigo 17.º de “despacho da autoridade judiciária” que as autorize, ao passo que, nos termos constitucionais, “a entrada no domicílio dos cidadãos contra a sua vontade só pode ser ordenada pela autoridade judicial competente, nos casos e segundo as formas previstas na lei” (artigo 34.º, n.º 2).

A apreciação do eventual desrespeito desta disposição requer, como questão prévia, a definição rigorosa do objecto da inviolabilidade do domicílio. O que deve entender-se, para este efeito, por domicílio?

Não é fácil a resposta, até porque o conceito técnico de domicílio, compreendido como a “residência habitual” (artigo 80.º do Código Civil), é aqui imprestável, por demasiado restritivo, atentos o sentido e a função da tutela constitucional. Seguro é apenas que, no âmbito do artigo 34.º da CRP, o conceito vem dotado de maior amplitude, abarcando, sem margem para dúvidas, qualquer local de habitação, seja ela principal, secundária, ocasional, em edifício ou em instalações móveis. Mas já não é consensual a extensão da protecção ao domicílio profissional (em sentido afirmativo), GOMES CANOTILHO/VITAL MOREIRA, Constituição Portuguesa anotada, I, 4.ª ed., Coimbra, 2007, 540; contra, PAULO PINTO DE ALBUQUERQUE, Comentário do Código de Processo Penal, Lisboa, 2007, 478-479).

Mas, quando se extravasa da esfera domiciliária das pessoas físicas, entrando no campo de actividade das pessoas colectivas, afigura-se que saímos também para fora do âmbito normativo de protecção da norma constitucional, pois deixai a sua razão de ser.

Como expressam os primeiros Autores a que fizemos referência (ob. cit., 541):

«Já quanto às pessoas colectivas, a protecção que é devida às respectivas instalações (designadamente quanto à respectiva sede) contra devassas externas não decorre directamente da protecção do domicílio, de cuja justificação não compartilha, como se vín acima, mas sim do âmbito de protecção do direito de propriedade e de outros direitos que possam ser afectados, como a liberdade de empresa, no caso das empresas (...).»

Essa conclusão decorre do substrato e das conexões valorativas do direito à inviolabilidade do domicílio, ainda um direito à liberdade da pessoa pois está relacionado, tal como o direito à inviolabilidade de correspondência, com o direito à inviolabilidade pessoal, (esfera privada espacial, previsto no art. 26.º), considerando-se o domicílio como projeção espacial da pessoa (...).

O bem protegido com a inviolabilidade do domicílio e o êxito de valor que lhe vai associado têm a ver com a subtração aos olhares e ao acesso dos outros da esfera espacial onde se desenvola a vivência doméstica e familiar da pessoa, onde ela, no recato de um espaço vedado a estranhos, pode exprimir livremente o seu mais autêntico modo de ser e de agir. Dando conta desta identificação do domínio protegido com a esfera da intimidade doente humano, afirmou-se no Acórdão n.º 67/97:

«Parece incontrovertido que o conceito constitucional de domicílio deve ser dimensionado e moldado a partir da observância do respeito pela dignidade da pessoa humana, na sua vertente de reserva da intimidade da vida familiar – como tal conjugado com o disposto no n.º 1 do artigo 26.º da CR – assim acantelando um núcleo íntimo onde ninguém deverá penetrar sem consentimento do próprio titular do direito.»

Não se ignora que, nos termos do n.º 2 do artigo 12.º da CRP, as pessoas colectivas podem ser titulares de direitos fundamentais, desde que compatíveis com a sua natureza. E não custa reconhecer que o direito à privacidade não é incompatível, em absoluto, com a natureza própria das pessoas colectivas, pelo que a titularidade desse direito não lhes pode, a priori, e em todas dimensões, ser negada.

Mas, como acentua JORGE MIRANDA, reportando-se, em geral, à titularidade “colectiva” de direitos fundamentais, “dai não se segue que a sua aplicabilidade nesse domínio se vá operar exactamente nos mesmos termos e com a mesma amplitude com que decorre relativamente às pessoas singulares” (JORGE MIRANDA/RUI

426
R

TRIBUNAL CONSTITUCIONAL

MEDEIROS, Constituição Portuguesa anotada, I, Coimbra, 2005, 113). É esta uma orientação firme, tanto da doutrina (cfr., também, GOMES CANOTILHO/VITAL MOREIRA, ob. cit., 331, e VIEIRA DE ANDRADE, Os direitos fundamentais na Constituição Portuguesa de 1976, 3.ª ed., Coimbra, 2007, 126-127), como da jurisprudência (cfr. os Acórdãos n.ºs 198/85 e 24/98).

A susceptibilidade, em princípio, de extensão da tutela da privacidade às pessoas colectivas, não implica, pois, que ela actue, nesse campo, em igual medida e com a mesma extensão com que se afirma na esfera da titularidade individual. Dessa tutela estarão excluídas, forçosamente, as dimensões nucleares da intimidade privada, que pressupõem a personalidade física.

É o que acontece com a inviolabilidade do domicílio, uma manifestação particular e qualificada da tutela da intimidade da vida privada, dirigida, como vimos, à realização da personalidade individual e ao resguardo da dignidade da pessoa humana.

E, não estando em causa uma invasão do domicílio, a autorização prévia do Ministério Público para as buscas é o bastante para excluir, sem margem para dúvida, estarmos perante uma "abusiva intrusão na vida privada" (cfr., nesse sentido, o Acórdão n.º 192/2001, citando o Acórdão n.º 7/87).

É neste ponto, na exigência de despacho da autoridade judiciária autorizativo da realização das diligências de busca "nas instalações das empresas", que a lei da concorrência se afasta decisivamente da lei francesa, em relação à qual foi proferido, em 16 de Abril de 2002, o acórdão do Tribunal Europeu dos Direitos do Homem, no *Affaire Colas*, invocado pela recorrente em defesa da sua tese.

Como resulta da transcrição, no ponto 22, da legislação aplicável ao caso, os agentes da direção geral do comércio interior e dos preços tinham "livre acesso às instalações que não constituam a habitação do comerciante", sem qualquer controlo de uma entidade judiciária independente. Em face desses dados normativos, o tribunal concluiu que a legislação e a prática francesas não ofereciam "garantias adequadas e suficientes contra os abusos" (ponto 48), como o exigia a tutela do domicílio, consagrada no artigo 8.º da CEDH.

Não é essa, como se viu, a situação normativa vigente entre nós, em que a salvaguarda da privacidade das pessoas colectivas está acantelada, na justa medida, pela necessidade de autorização do Ministério Público, entidade a quem cabe, nos termos constitucionais, "defender a legalidade democrática" (artigo 219.º, n.º 1, da CRP).

Pode, pois, concluir-se que a interpretação normativa questionada não viola o disposto nos artigos 34.º, n.º 1, 2, 3 e 4, e 32.º, n.º 8, da CRP."

(Acórdão do TC n.º 503/2008)

Ainda que não se tenha pronunciado sobre o *objeto* da pesquisa de forma particular, parece evidente que o *objetivo* indissociável do instituto de obtenção de prova fiscalizado – a reunião de informação documental apta a servir como prova de práticas anticoncorrenciais, já num contexto histórico de desmaterialização de documentos e de utilização de serviços web – não se poderá entender ignorado pelo Tribunal quando formulou este entendimento. Temos por feliz o contraponto que esta jurisprudência ofereceu para com a tutela do domicílio, convocando uma exigência constitucional expressa de intervenção judicial (artigo 34.º, n.º 2, da Constituição da República Portuguesa) que não existe com relação a muitos outros direitos fundamentais de estrutura defensiva (seja os aqui colocados), daí decorrendo a necessidade de diferente tratamento.

O acervo de correspondência eletrónica preservado por uma empresa é, a todos os títulos, um ativo imaterial por esta titulado e essa base de dados constitui componente do seu



TRIBUNAL CONSTITUCIONAL

estabelecimento, pelo que não existe fundamento para que se diga que beneficia de maior proteção do que aquela que à empresa-objeto é conferida (v. Acórdão do TEDH, *Delta Pekáni v. República Checa*, de 2 de janeiro de 2015). Assim, a efetivação de uma operação de busca e apreensão de documentação digital nestas condições não imporá maiores exigências que a autorização por Magistrado do Ministério Público, cuja vinculação a critérios de legalidade (artigo 219.º, n.º 1, da Constituição da República Portuguesa) assegurará a conexão entre a ingerência e o referente legitimador, tal como defendido nos Acórdãos n.ºs 7/1987, 67/97, 593/2008 e 596/2008, jurisprudência que renovamos.

12.4.2. O que vai exposto não pretende exprimir que não poderão existir outros casos em que se concluirá pela necessidade de autorização judicial para certos atos de inquérito criminal (ou para a validação de atos) ou de ações de investigação no âmbito contraordenacional, que não os que destacámos *supra*, mas apenas que a obrigatoriedade dependerá que se surpreenda uma situação de lesão em valores constitucionais *a pari* face às previsões da Lei Fundamental que especialmente formulam essa exigência. Esse nunca será o caso, como já tantas vezes repetimos, da proteção conferida a informação de conteúdo económico, que se caracteriza por uma garantia efetiva insípida e permeável a ingerências perante outros interesses normativos do catálogo constitucional.

Por outro lado, o exposto também não pretende afirmar que *nenhum* controlo jurisdicional existirá sobre os meios de obtenção de prova que importem intrusão na defesa da privatividade de ordem económica e da integridade do estabelecimento em processos de investigação por autoridades públicas. Apenas significa que esse controlo será *posterior* à efetivação da operação de recolha de prova e no âmbito do controlo da respetiva validade, seja pela ulterior sujeição do processo a titularidade jurisdicional (artigo 32.º, n.º 4, da Constituição da República Portuguesa; v. g., artigos 290.º, n.º 1 e 286.º, n.º 1, 310.º, n.º 2, 311.º, n.º 1, 338.º, n.º 1 e 368.º, n.º 1, todos do CPP e artigo 59.º do RGC), seja por via de instrumentos de impugnação autónomos e específicos ao meio de obtenção de prova [v. g., artigo 55.º, n.º 1, do Regime Geral das Contraordenações (RGC)].

O controlo *ex post facto* da legalidade do ato de recolha de prova compreenderá as condições em que foi autorizada, incluindo observância de requisitos legais e justificação material, bem como a forma como foi executada, abarcando todas as matérias de facto e de Direito que importem e em que naturalmente se inclui juízo de conformidade do ato para com direitos, liberdades e garantias (cfr. artigo 18.º n.º 1, da Constituição da República Portuguesa). A invalidação do meio de prova

423
X

TRIBUNAL CONSTITUCIONAL

em função de qualquer irregularidade no procedimento de obtenção, por seu turno, reconstituirá a situação de instrução probatória do processo, dele expurgando os elementos abrangidos pelo vício.

Este é, de resto, o *standard* da jurisprudência do Tribunal Europeu dos Direitos do Homem (TEDH) sobre garantias de controlo judicial sobre operações de busca e apreensão em edifícios privados (incluindo residências): aquelas entendem-se infringir o artigo 8.º da Convenção Europeia dos Direitos do Homem (CEDH) *apenas* quando a Lei não garanta a *possibilidade* de a pessoa visada suscitar controlo judicial *subsequente*, não necessariamente *prévio* à diligência que efetiva a intrusão:

"O Tribunal sublinha neste contexto que operações de busca e apreensão representam uma séria ingerência nos direitos conferidos pelo artigo 8.º, no caso concreto no escritório de um advogado e na sua correspondência e que, em consequência, terão de estar baseadas numa Lei particularmente precisa. É essencial que existam regras claras e detalhadas sobre esta matéria, estabelecendo salvaguardas contra a possibilidade de abuso ou arbitrariedade (...)"

Sobre o caso dos autos, o Tribunal reitera o entendimento de «Sallinen e outras» (citado supra, § 89), de que não existe supervisão independente ou supervisão judicial na concessão do mandado de busca, uma vez que a decisão de autorizar a diligência é tomada pelas próprias polícias (...)"

*O Tribunal nota que a ausência de mandado judicial prévio pode ser contrabalançada pela disponibilidade de uma revisão judicial *ex post facto*. (...) No entanto, no caso presente, o queixoso não dispunha de acesso efetivo, a posteriori, a Tribunal para que fossem revistas a legalidade e a justificação do mandado de busca."*

(Ac. TEDH de 15 de fevereiro de 2011, *Heino v. Finlândia*)

"No que respeita, em particular, a buscas de edifícios (de habitação) e apreensões, o Tribunal tem entendido de forma consistente que os Estados contratantes podem considerar necessário recorrer a este tipo de medidas tendo em vista obterem prova tangível de cartas infrações. (...)"

*Relativamente a medidas preventivas de abusos existentes na legislação russa, o Tribunal observa que, na ausência de exigência de autorização judicial prévia, as autoridades de investigação dispunham de discreção não-controlada para aferirem da necessidade e o âmbito da busca e apreensão. (...) No caso presente, porém, a ausência de mandado judicial prévio foi, em certa medida, compensada pela disponibilidade de revisão judicial *ex post facto*. O queixoso podia dirigir e, na verdade, dirigiu, uma queixa a Tribunal, que foi chamado a rever tanto a legalidade como a justificação para o mandado de busca. A eficácia desta revisão, porém, será tida em conta na análise a que procederemos agora da ingerência."*

(Ac. do TEDH de 7 de junho de 2007, *Smirnov v. Russia*)

"À data dos factos (...) a polícia poderia realizar uma busca sem autorização prévia nos casos em que a diligência pudesse ser prejudicial [aos objetivos da diligência]. Ela tinha competência para apreciar, isolada, a oportunidade de uma busca e o respetivo âmbito. (...)"

Por outro lado, o Tribunal nota que à data dos factos o queixoso não beneficiava de uma via efetiva de impugnação para obter o controlo a posteriori, por um Juiz, da legalidade e a justificação da busca em questão. (...)"

Considerando o exposto, o Tribunal considera que as disposições legais em vigor à data dos factos não estabeleceram garantias suficiente que evitassem que as autoridades não pudessem empreender medidas arbitrárias e atentatórias do direito do queixoso à reserva do seu domicílio. Assim sendo, existiu violação do artigo 8.º da Convenção."

(Ac. do TEDH de 30 de setembro de 2008, *İşildaş v. Turquia*)

429
8



TRIBUNAL CONSTITUCIONAL

"De acordo com o Direito interno em vigor à data dos factos, o procurador decidia por si só proceder à busca domiciliária e poderia realizá-la sem obter mandado, tanto menos mandado judicial. O Tribunal observa que se tratou de uma lesão grave ao direito dos dois primeiros requerentes à reserva do seu domicílio, deixando à disposição do procurador que, como já aqui se julgou, ainda que se trate de um magistrado do ministério público, não observa as exigências de independência face ao poder executivo (v., entre outros, Dumitru Popescu, *supra citado*, § 71). Por outro lado, se, na ausência de mandado judicial prévio, a busca em causa não foi sujeita a nenhum controlo a priori, o Tribunal faz ver que à época dos factos os dois queixosos não dispunham de uma via de impugnação efetiva para que obtivessem a revisão e controlo, a posteriori e por um Juiz, da legalidade e do bem-sucedido da busca em questão. Assim sendo, realizada na ausência de mandado (prévio) e formalizado por via oral, sem testemunhas ou outros espectadores, a busca realizada pelo procurador não respeitou as garantias mínimas que as disposições legais impunham às autoridades encarregues do inquérito penal e não foi sujeito ao controlo por autoridades judiciais." (Acórdão do TEDH de 1 abril de 2008, *Varga v. Roménia*)

Em especial sobre diligências de busca e apreensão em empresas no âmbito de processos por infrações à concorrência, entendeu o TEDH:

"(...) nas matérias que concernem à proteção de pessoas contra atentados arbitrários pelo poder público aos direitos garantias pelo artigo 8.º (o Tribunal) já teve oportunidade de fazer ver que a ausência de um mandado de busca (judicial) pode ser compensado por um controlo judiciário efetivo e realizado *ex post facto* (v. *Heino, supra citado*, § 45; *Smirnov, supra citado*, § 45 *in fine*). (...)"

De acordo com o Direito interno, o simples facto de ter sido instaurado um procedimento administrativo contra a sociedade queixosa conferia à Autoridade da Concorrência o direito de proceder à inspeção (do estabelecimento comercial). Esta não foi objeto de autorização prévia por Juiz, que poderia ter circunscrito o seu âmbito ou monitorizar a forma como foi realizada. (...)

No entanto, o Tribunal já teve a ocasião de firmar, nestas situações, a ausência de um mandado de busca pode ser contrabalançado por um controlo judiciário *ex post facto* sobre a legalidade e necessidade desta medida de instrução (v. *Heino, supra citado*, § 45; *Gutsanovi, supra citado*, § 222). Isto importa, porém, que o controlo seja eficaz nas circunstâncias colocadas pela matéria em causa (*Smirnov v. Rússia*, n.º 71362/01 § 45, *in fine*, 7 de junho de 2007). Na prática, isto implica que os interessados possam obter um controlo jurisdicional efetivo, na prática por via do exercício de um direito, da medida questionada e da forma como foi realizada; nos casos em que uma operação julgada irregular tenha sido já consumada, o recurso ou recursos legais disponíveis devem permitir à interessada obter a reconstituição da situação criada pela lesão"

(Acórdão do TEDH de 2 de janeiro de 2015, *Delta Pékarni v. República Checa*)

O Tribunal de Justiça da União Europeia (TJUE) assimila essencialmente a jurisprudência do TEDH em matéria de direitos fundamentais (v. Acórdão do TJUE de 15 de outubro de 2020, *Casino Guichard Perrachon*, 249/17 §§ 53 e 73), designadamente no que respeita às garantias conferidas pelo artigo 7.º da Carta de Direitos Fundamentais da União Europeia (CDFUE), congénere ao artigo 8.º da CEDH. Sobre o controlo judicial de ações de busca e apreensão em empresas no âmbito de processos por infrações à concorrência, entendeu o TJUE, oferecendo continuidade ao exposto:

8/25
A

TRIBUNAL CONSTITUCIONAL

"quanto ao argumento invocado pela Deutsche Bahn segundo o qual o Tribunal Geral cometeu um erro de direito ao basear-se, no n.º 66 do acórdão recorrido, nos acórdãos do TEDH, Harju c. Finlândia e Heino c. Finlândia, já referidos, há que constatar que, nesses acórdãos, o TEDH afirmou expressamente que a falta de mandado judicial prévio pode ser compensada por uma fiscalização jurisdicional a posteriori eficaz de todas as questões de direito e de facto. (...) o TEDH considera que a existência de uma fiscalização jurisdicional a posteriori permite compensar a falta de um mandado judicial prévio e constitui, portanto, uma garantia fundamental para assegurar a compatibilidade da medida de inspeção em causa com o artigo 8.º da CEDH (v., desigualmente, TEDH, acórdão Delta Pekáry a. s. c. República Checa, n.º 97/11, §§ 83, 87 e 92, de 2 de outubro de 2014).

É precisamente o que se verifica no âmbito do sistema aplicado na União Europeia, uma vez que o artigo 20.º, n.º 8, do Regulamento n.º 1/2003 indica expressamente que o controlo da legalidade da decisão da Comissão se encontra reservado exclusivamente ao Tribunal de Justiça.

A fiscalização prevista pelos Tratados implica que o juiz da União exerce, com base nos elementos de prova invocados pelo recorrente em apoio dos fundamentos invocados, uma fiscalização completa, ou seja, que incide quer sobre questões de direito quer sobre questões de facto (v., neste sentido, acórdãos Chalkor/Comissão, C-386/10 P, EU:C:2011:815, n.º 62, e CB/Comissão, C-67/13 P, EU:C:2014:2204, n.º 44).

Daqui se conclui que o Tribunal Geral teve razão em considerar que o direito fundamental à inviolabilidade do domicílio, conforme protegido pelo artigo 8.º da CEDH, não foi violado devido à falta de mandado judicial prévio." (Acórdão do TJUE de 18 de junho de 2015, C-583/13 P, Deutsche Bahn AG e outros v. Comissão Europeia, §§ 26 e 32-35)

"(...) há que constatar, como faz a Comissão, que resulta destes acórdãos que o que é visado é realmente a intensidade da fiscalização e não o momento em que esta é exercida. A fiscalização deve ser exercida sobre a totalidade dos elementos de facto e de direito e permitir que a situação seja adequadamente sanada na hipótese de já ter ocorrido uma operação considerada irregular (TEDH, acórdão Société Canal Plus e o. c. França, n.º 59, supra, n.º 36).

Em segundo lugar, é possível interpor recurso da decisão de inspeção ao abrigo do artigo 263.º TFUE. Por conseguinte, a falta de uma fiscalização completa exercida ex ante por uma autoridade nacional, a qual emitiria um mandado, em todo o caso, não releva, ao contrário do que alegam as requerentes. O artigo 20.º, n.º 4, do Regulamento n.º 1/2003 prevê tal fiscalização pelo juiz da União e impõe que tal seja mencionado na decisão que ordena a sujeição a uma inspeção nas instalações da empresa. No caso em apreço, a Comissão respeitou esta formalidade quando da adoção da primeira, segunda e terceira decisões de inspeção e as recorrentes sabiam que podiam interpor um recurso que lhes permitia contestar a necessidade da inspeção, como atestam os presentes processos.

Em terceiro lugar, não se pode seriamente contestar o facto de o Tribunal Geral poder exercer uma fiscalização dos factos e não funcionar, como alegam as recorrentes, unicamente como um tribunal de cassação". Com efeito, o juiz da União, pronunciando-se sobre um recurso de anulação de uma decisão de inspeção interposto ao abrigo do artigo 263.º TFUE, exerce uma fiscalização tanto de direito como de facto e tem o poder de apreciar as provas e de anular a decisão impugnada. Resulta da jurisprudência que, no quadro da sua fiscalização das decisões de inspeção, o juiz da União pode ser levado a certificar-se da existência de indícios suficientemente sérios que permitam suspeitar de uma infracção às regras da concorrência por parte das empresas em causa. (v. acórdão Roquette Frère, n.º 80, supra, n.os 54 e 55 e jurisprudência referida). Por outro lado, resulta destas considerações que o segundo argumento das recorrentes (v. n.º 105, supra), segundo o qual a alegada ausência de fiscalização judicial completa das decisões de inspeção após o início das referidas inspeções viola o artigo 6.º, n.º 1, da CEDH, deve ser julgado improcedente.

Em quarto lugar, há que salientar que, como a Comissão corretamente recorda, a eventual anulação da decisão de inspeção ou ainda a constatação da existência de uma irregularidade no desenvolver das medidas executadas pelos agentes mandatados implicam a impossibilidade de a instituição utilizar as informações colhidas durante as operações controvertidas num processo de infração (acórdão Roquette Frères, n.º 80, supra, n.º 49).

Por conseguinte, há que julgar integralmente improcedente o segundo fundamento."

(Acórdão do TJUE de 6 de setembro de 2013, T-289/11, T-290/11 e T-521/11, Deutsche Bahn AG v. Comissão Europeia, §§ 108-114)

426
L

TRIBUNAL CONSTITUCIONAL

Esta jurisprudência europeia, consistente e reiterada, deve merecer-nos uma pausa, já que a norma fiscalizada consagra um sistema de *redundância* quanto a controlo judicial: *antes* do ato de obtenção de prova, mediante autorização pelo Ministério Público – entidade integrada no aparelho judicial e com garantias de independência face ao poder executivo e à autoridade administrativa que realiza a busca e requer a autorização – e *depois*, pela sua sindicabilidade judicial.

Este modelo representa, sem nenhuma dúvida, um reforço sensível de garantias face às exigências da jurisprudência europeia sobre a matéria colocada, que entende suficiente o controlo judicial posterior à operação. Por outra parte, um sistema de *díplo controlo judicial* (defendido pelo Acórdão do TC n.º 687/2021), se não se pode dizer proibido pelo Direito da União, quando se lhe confira caráter *necessário* representará oposição à jurisprudência do TEDH e do TJUE, prejudicando a coerência e a uniformidade desta categoria de sistemas processuais no espaço da União.

É dizer, o modelo de controlo judicial *ex post facto* das operações de busca e apreensão em empresas e de autorização *precedente* por magistrado do Ministério Público, constitui um arquétipo adequado de defesa de particulares como, bem assim, do mercado concorrencial europeu, ao mesmo tempo que orienta o processo de convergência entre o Direito interno e o Direito da União.

Em suma, são quatro as razões por que concluímos pela desnecessidade de autorização judicial prévia para operações de busca e apreensão em empresas de mensagens eletrónicas ou outros documentos digitais ao abrigo do artigo 18.º, n.º 1, alínea c), do RjdC: (i) porque não está em causa qualquer ingerência na autodeterminação comunicativa; (ii) porque a norma fiscalizada não se integra no ordenamento processual do crime e, como tal, não se encontra sujeita à observância do respetivo regime especial de garantias (artigo 32.º da Constituição da República Portuguesa); (iii) porque a Lei Fundamental não impõe que esse tipo de ingerências na privacidade sejam subordinadas a autorização ou validação por Juiz, mesmo no domínio criminal, como não existe exigência nesse sentido sobre intrusões na liberdade de empresa ou na autodeterminação informacional (cfr. artigos 61.º e 35.º, n.º 4, ambos da Constituição da República Portuguesa); (iv) porque os controlos garantidos pela Lei, pelo Ministério Público antes da ingerência e a sindicância jurisdicional, depois, concretiza e excede os *standards* de Direito europeu sobre defesa da privacidade de ordem económica, alinhando o ordenamento com a jurisprudência europeia.

427
ok

TRIBUNAL CONSTITUCIONAL

Concluímos, por tudo, que não será por não impor autorização prévia por Juiz que a norma do artigo 18.º, n.º 1, alínea c), do RJdC, será entendida materialmente inconstitucional.

12.5. Levando em conta que o artigo 18.º, n.º 1, do RJdC, corporiza uma fórmula de intrusão no direito à privacidade, associado à liberdade de empresa (artigos 26.º, n.º 1 e 61.º, n.º 1, ambos da Constituição da República Portuguesa) e no direito à autodeterminação informacional (artigo 35.º, n.º 4, da Constituição da República Portuguesa), cabe agora aferir se a norma sob sindicância constitui uma intrusão proporcional nos respetivos estatutos defensivos (artigo 18.º, n.º 2, da Constituição da República Portuguesa). Impõe-se saber, enfim, se a norma configura uma medida *necessária e apta* à realização da função de garantia da efetividade de uma pretensão punitiva estadual em matéria de ilícito de mera ordenação que seja passível de se arvorar em referente legitimador e se representa um *ganho líquido* na realização dos valores constitucionais observados no seu conjunto, face às medidas de lesão que importa.

Pois bem, se, quanto à dimensão de ingerência que a norma desempenha nos direitos fundamentais colocados o *supra* exposto parece suficiente, sobre o valor jurídico que suporta a intrusão e de cuja tutela a norma é instrumento – a livre concorrência em mercados –, interessa chamar à colação o expedido no Acórdão do TC n.º 91/2023:

“O direito da concorrência, nacional e europeu, destina-se a garantir a integridade do funcionamento dos mercados. As respetivas normas protegem os consumidores e as empresas de práticas comerciais concertadas que tenham por finalidade ou efeito impedir, restringir ou falsear o livre desenvolvimento dos mercados, assegurando aos primeiros reais «possibilidades de escolha» e franqueando às segundas o ingresso num circuito livre de «obstáculos» gerados por quem dele beneficia, de modo a permitir-lhes criar riqueza e empregos» (Considerando 1 da Diretiva ECN+).

Trata-se, assim, de um conjunto de normas que se inscrevem, por um lado, na incumbência prioritária do Estado fixada na alínea f) do artigo 81.º da Constituição, que o vincula a «[a]ssegurar o funcionamento eficiente dos mercados, de modo a garantir a equilibrada concorrência entre as empresas, a contrariar as formas de organização monopolistas e a reprimir os abusos de posição dominante e outras práticas lesivas do interesse geral», e se reconduzem, por outro, ao direito fundamental dos consumidores «à proteção [...] dos seus interesses económicos», consagrado no n.º 1 do artigo 60.º da Lei Fundamental, constituindo um dos principais eixos da tutela a estes constitucionalmente devida contra práticas comerciais manipuladoras e abusivas, designadamente aquelas que «mantêm os preços de produtos e serviços artificialmente elevados» (Considerando 1 da Diretiva ECN+).

Dispõe o bem jurídico tutelado pelo direito sancionatório da concorrência de inequívoco assento jurídico-constitucional — protegê-lo constitui mesmo, como vimos, um dever prioritário do Estado —, não há dúvida de que nos encontramos em matéria que a Constituição permite que o legislador situe no (ou aíque no) domínio do direito penal, substantivo e adjetivo. Do ponto de vista da Constituição — aquele que aqui releva —, o controlo do chamado «poder de mercado» constitui um valor da «máxima relevância jurídica» (expressão utilizada no Acórdão n.º 377/2015), cuja proteção o legislador se encontra por isso legitimado a prosseguir através da ameaça de sanções



TRIBUNAL CONSTITUCIONAL

punitivas, que são «aquelas que em geral maiores sacrifícios impõem aos direitos fundamentais» (Acórdão n.º 99/2002).»

Subscrevemos estas considerações e podemos acrescentar o seguinte. A distorção da concorrência e o bloqueio de mecanismos concorrenciais adquire especial relevância no atual contexto português, face à transição verificada nas últimas décadas entre um modelo de governo económico assente na titularidade estadual de empresas em espaços-chave da economia (o que por vezes se apelida de *capitalismo monopolista de Estado*) para um modelo regulatório, liberal e institucional, assente no controlo de fatores de produção, total ou predominantemente, por privados, que se arvoram em governantes da economia. O Estado, neste modelo, é relegado para funções de *monitorização e policiamento* dos mercados, não de agente interventor, cingindo as suas atribuições a assegurar a liberdade dos operadores e a proteger a estrutura económica contra fatores que perturbem os seus equilíbrios autogestionários. Mesmo o desempenho desta função, que se pretende neutral e assética, fica diferido para entidades independentes aos órgãos de soberania, tendo em vista deixar à margem qualquer tentação de intervenção estadual nos mercados.

Esta transição resultou de uma estratégia abrangente de privatizações iniciada em 1995 (pela devolução total de estruturas públicas a investidores privados, por vezes deixando ao Estado participações residuais) e atravessou o *Programa de Assistência Económica e Financeira* (PAEF), que expandiu esta orientação política e consagrou vínculos específicos a esse respeito. Incluíram-se no processo a generalidade das empresas nacionais instaladas em setores estratégicos, sejam (v. g.) *energia* (EDP, REN e GALP), *comunicações* (PT e CTT) e *transportes* (TAP e Aeroportos de Portugal).

A perda do poder estadual de intervenção direta na economia através de unidades empresariais significa a rendição aos mecanismos de concorrência do *quase-exclusivo* de otimização dos circuitos económicos nacionais, pelo que do seu nível de desempenho operativo dependerá a evolução e a expansão da economia portuguesa, predicando toda a sua capacidade para gerar, reter e distribuir riqueza. A atividade de uma ou mais empresas (ou de associações de empresas) de dado setor *contra o mercado* (contra clientes, contra fornecedores), seja mediante concertação, abuso de posição dominante ou outras práticas de infração à concorrência, representa a desconstrução deste paradigma: dispensa a moderação de preço ou a qualificação da prestação como fatores de maximização de lucros e fecha os mercados à iniciativa de novos operadores; por isso, alavanca fenómenos inflacionistas artificiais, desincentiva a inovação, promove imobilismo e, em último



TRIBUNAL CONSTITUCIONAL

termo, deixa o setor refém do infrator. No limite, estaremos perante operações de drenagem de recursos da economia orientadas para a acumulação de riqueza num grupo restrito de pessoas ou entidades, promovendo fluxos de saída do território e a descapitalização da economia; este fenómeno dificulta e encarece o acesso a capitais de financiamento por operadores nos mercados nacionais, desequilibra a balança de pagamentos, insufla desigualdades e paralisa o crescimento.

Merecem particular destaque de entre as condutas restritivas da concorrência as classificadas como *cartelização «hard core»*, que é dizer, as práticas de *concertação de preços, distribuição de mercados, limitação da oferta e concertação de licitações em concursos públicos*, que a OCDE destacou em 2018 como as mais “*clamorosas violações de Direito da concorrência. Elas lesam consumidores em muitos países através da elevação de preços e limitando a oferta, assim tornando mercadorias e serviços completamente indisponíveis para alguns compradores e desnecessariamente dispendiosos para outros.*” (OCDE, *Recomendação do Conselho sobre Ação Efetiva contra «Cartéis hard core»*, OECD/LEGAL/0294). A distorção que realizam dos mercados cria “*supremacia de mercado, desperdício e ineficiência em países onde os mercados poderiam ser, de outra forma, competitivos e deixá-los especialmente dependentes de cooperação*” (*ibidem*). O estudo de práticas antitrust nos Estados Unidos sugere que o custo anual dessas atividades para consumidores e contribuintes ascende a largos milhares de milhões de dólares, pesando em particular sobre os primeiros. Um único caso, referente a um cartel transnacional do setor de suplementos alimentares, conduziu a que “*ao longo de quase uma década, todos os consumidores americanos, qualquer pessoa que haja tomado vitaminas, bebido um copo de leite ou comido uma taça de cereais, haja pago em excesso para que os infratores colhessem centenas de milhões de dólares em receitas adicionais*” (v. B.. K. PAYNE, *White-Collar Crime*, Sage Publications, Inc., 2017, p. 224). Foi a elevada danosidade do fenómeno que levou o Conselho da OCDE a recomendar em 2018 a aprovação de quadros legais aptos a reprimir e dissuadir a cartelização, incluindo “*procedimentos de enforcement*”, designadamente por “*instituições dotadas de poderes para detectarem e remediar carteis hard-core, incluindo poderes para obter documentos e informações*” (OCDE, *Recomendações...*, sublinhado nosso). A norma fiscalizada responde a este objetivo, como temos vindo a assinalar.

Por outro lado, a doutrina vem defendendo que não é apenas o particular valor do bem jurídico tutelado ou a violência do impacto antijurídico que merece especiais considerações quando se consideram práticas restritivas da concorrência, seja o caso dos cartéis, mas também a percepção “*de que os participantes nestas práticas restritivas da concorrência têm a consciência da ilegalidade da sua conduta e, ainda assim, persistem na sua atuação, desafiando diretamente a lei e os seus aplicadores*”, demonstrando uma

42
2

TRIBUNAL CONSTITUCIONAL

"atitude de indiferença ou mesmo de voluntária e expressa contraditoriedade com a lei, aliada a atos materiais de dissimulação dos acordos, decisões e práticas concertadas em causa" (v. F. NEVERSA LOUREIRO, *op. cit.*, p. 201). Vários autores sinalizam mesmo o ambiente empresarial como tendente a promover, em certas condições, a aceitação ou tolerância por *"atos pouco éticos ou mesmo ilícitos praticados pelos seus funcionários ou agentes quando tais comportamentos geram uma vantagem para a própria empresa"* (v. F. NEVERSA LOUREIRO, *op. cit.*, pp. 217). De mais específico, o estudo do fenómeno delinquencial em empresas sugere a *"existência de uma natureza e de uma estrutura próprias das organizações económicas que, aliadas a fatores sociais, económicos e culturais específicos do meio em que aquelas estão inseridas, ajudam a promover uma atitude de aceitação do risco e de flexibilização ética que faz com que a prática de atos ilegais e, mesmo, criminosos, se torne um ato banal e não censurado"* (v. F. NEVERSA LOUREIRO, *op. cit.*, p. 219; mantém atualidade a exposição de E. SUTHERLAND sobre *associação diferencial e desorganização social* como fatores de contexto de práticas empresariais ilícitas – *in White Collar Crime*, Yale Univ. Press, pp. 227-264).

O exposto permite concluir que no domínio colocado encontramos, não apenas um grau expressivo de anti-juridicidade, mas também de *grave censurabilidade* sobre as práticas reprovadas e tipificadas pela legislação antitrust, ambos associados a indicadores de contexto com importante potencial criminógeno, também neste conjunto de pressupostos se impondo avaliar as medidas de reunião de prova destinadas a servir a instrução de processos pelas respetivas infrações.

Se daqui resulta demonstrado, à saciedade, que a tutela do Direito da concorrência será apta a legitimar uma ingerência nos direitos fundamentais colocados, sobre a *adequação e necessidade* da solução do artigo 18.º, n.º 1, alínea c), do RJdC, para a sua efetivação quando confere poderes à AdC para realizar operações de pesquisa e apreensão de mensagens eletrónicas, podemos recorrer ao que dispõe o Acórdão do TC n.º 91/2023, uma vez mais, que nesta parte subscrevemos:

"a disponibilização do meio de obtenção de prova que a norma sindicada facilita à AdC inscreve-se no propósito, enfatizado e reforçado pela Diretiva ECN+, de dotar a autoridade nacional da concorrência de instrumentos eficazes para a recolha de elementos de prova das infrações cometidas através de práticas anticoncorrenciais, cuja impunidade, como ali se diz, impedirá as empresas de concorrerem com base nos seus méritos" (Considerando 6) e penalizará severamente os consumidores, tendo em conta que, «[n]uma economia de mercado, um dos principais instrumentos de defesa dos interesses económicos [destes] são as instituições de defesa da concorrência, sancionando-se, designadamente as práticas restritivas da concorrência e os abusos de posição dominante» (Gomes Canotilho/Vital Moreira, Constituição da República Portuguesa Anotada, I Vol., Coimbra, Coimbra Editora, 2014, p. 782).
Para a realização desta finalidade, a possibilidade de acesso, através de busca e apreensão em sistemas informáticos, a comunicações eletrónicas enviadas e recebidas no âmbito do correio eletrónico profissional de uma empresa ou dos seus representantes constitui uma medida idónea e necessária. Idónea porque as práticas anticoncorrenciais proibidas



TRIBUNAL CONSTITUCIONAL

431
Q.

— em particular as que se traduzem em acordos entre empresas concorrentes tendo por objeto a fixação dos preços, a atribuição de quotas de produção ou de venda, o controlo da distribuição ou do desenvolvimento técnico e a repartição dos mercados — resultam precisamente de trocas de informação e comunicações entre as partes envolvidas, através das quais são forjados os esquemas de manipulação e falseamento do livre desenvolvimento dos mercados. Necessária porque, atendendo ao que acabou de dizer-se, não são facilmente configuráveis, em abstrato, outros meios de obtenção de prova, menos onerosos e tão ou mais eficazes, para o combate às práticas que põem em causa a criação e o funcionamento de um mercado concorrencial mais aberto e mais justo (Directiva ECN+, Considerando 1), internamente e na União. Na verdade, «a informalidade que caracteriza as práticas restritivas mais graves — os cartéis — pode mesmo implicar que não possam considerar-se asseguradas as condições mínimas para a investigação tendente ao exercício dos poderes sancionatórios» sem a previsão de um regime de busca e apreensão de mensagens de correio eletrónico (neste sentido, referindo-se aos “danos colaterais” para a defesa da concorrência gerados pelo entendimento restritivo dos poderes da AdC que resultou das alterações introduzidas ao Código de Processo Penal pela Lei n.º 48/2007, de 29 de agosto, que equiparam, como atrás se viu, a recolha de prova em meio digital a escutas telefónicas, v. Miguel Moura e Silva, “As práticas restritivas...”, cit., p. 24). Conforme alertou o Conselho Superior da Magistratura em parecer datado de 23 de fevereiro de 2012, emitido durante o procedimento legislativo que culminou na aprovação da Lei n.º 19/2012, «[...] mensagens de correio eletrónico são um dos raros meios de prova disponíveis para a prova dos cartéis, abstraindo dos requerimentos de clemência. Nesta conformidade, a falta de norma deixará a AdC com a mesma dificuldade com que já hoje se depara nas suas buscas, aliás contra a corrente dos poderes das suas congéneres europeias e da própria Comissão Europeia [...]”

Já fizemos ver: quando se debatem medidas de obtenção de prova para a instrução de processos punitivos de condutas restritivas da concorrência caracterizadas pela concertação ou implementação de certas fórmulas de atividade empresarial, será necessário que as autoridades possam aceder aos seus registos de comunicações, particularmente das realizadas por corpos de governação e administrativos, já que constituem instrumentos e veículos da atividade infracional; com o advento do mundo digital, o formato eletrónico será o suporte mais frequente (senão exclusivo) dessa documentação, impondo a criação de norma legal que capacite as autoridades a procederem à sua localização e apreensão como condição mínima de efetividade da ação punitiva.

Como se disse, estas práticas caracterizam-se por *dissimulação* e pela natureza *confidencial e furtiva*, também porque a sua exposição representa perdas muito importantes de capital de prestígio pelas entidades infratoras (*maxime*, perante público consumidor, mas também sobre outros agentes económicos, cujas condições operacionais sejam afetadas pela prática). Nesse pressuposto, será indissociável à investigação e repressão de condutas anticoncorrenciais a presença e oposição de uma contraforça exercida pelos investigados de resistências às tentativas de adquirir notícia e prova sobre a prática implementada, traduzida em procedimentos dirigida a dificultar a deteção.

Se é frequente associar as tecnologias de informação a perdas de privacidade, não é menos verdade que trouxeram (em particular, o webmail e outros instrumentos análogos) também



TRIBUNAL CONSTITUCIONAL

455
T

excelentes oportunidades para ocultação de condutas antijurídicas, ao mesmo tempo que facilitam a comunicação entre infratores, promovendo a sua associação e viabilizando a sua organização de recursos. Instrumentos informáticos permitem dispensar reuniões presenciais ou diálogos pessoais para definir ou projetar práticas complexas (diminuindo o risco de aparência e a visibilidade de atos preparatórios e executórios da infração), bem como prescindir de registos manuscritos para memória e exequibilidade do accordado. Se cartas com facilidade percorrem muitas mãos e são colocadas sob muitos olhares até chegarem ao destinatário (v. g., estafetas, colaboradores administrativos e de secretariado), à semelhança de agendas, blocos de notas e apontamentos escritos de um executivo, não é assim com o webmail. Na descrição de um gabinete, atrás do ecran de um *laptop* ou manuseando um *smartphone* é possível preparar e executar o mais danoso dos accordos de cartel sem suscitar a atenção de olhos espantados. Isto significa a redução dos vestígios a mínimos sem paralelo noutros contextos históricos, confinados a espaços controlados e a dispositivos defendidos por modernos programas informáticos contra intrusões.

De resto, a compreensão da política económica de uma empresa depende da análise de circulares e instruções de órgãos de cúpula para quadros intermédios e subordinados em centros operacionais e também aqui o formato digital é um veículo e instrumento de registo incontornável.

Por outro lado, pedidos graciosos de colaboração, incluindo atos de interpelação e de requisição de documentos, serão, obviamente, inúteis para estes efeitos, ou, pelo menos, de eficácia muito condicionada. Isto, não apenas quando se considere a sobredita resistência à investigação coeva a este tipo de práticas e de agentes, mas também porque as operações imporão que se realize uma penosa tarefa de pesquisa em vastos acervos documentais tendo em vista a localização dos elementos com valor para a comprovação da prática infracional. Não é equacionável, seria talvez mesmo ingênuo, imaginar que uma empresa investigada participaria na sua própria culpabilização nesta medida, mobilizando recursos humanos e materiais para recolha de prova e é até duvidoso que fosse permitido exigir-lhe este tipo de atividade ao serviço da sua autoinculpação.

Sendo assim, temos que os poderes de pesquisa e apreensão de mensagens eletrónicas conferidos à AdC pelo artigo 18.º, n.º 1, alínea c), do RJDc, são *adequados e imprescindíveis* à defesa da concorrência, entendida esta como o interesse normativo legitimador da ingerência.

Aqui chegados, e por fim, não é difícil concluir de todo o exposto que o sacrifício moderado que a norma importa para os direitos fundamentais perturbados tem por contrapartida um ganho



435

TRIBUNAL CONSTITUCIONAL

superlativo, já que estamos perante a *síntese* fórmula apta a emprestar um mínimo de efetividade ao controlo e repressão de práticas anticoncorrenciais, com a pluralidade de impactos danosos que representam. Diríamos mesmo que a consagração deste tipo de medidas processuais é indissociável do novo modelo económico liberal, observado de forma global e integrada e em função da forma como se relaciona e convive com o sistema político-constitucional democrático instituído.

A doutrina assinala também que a política que vem sendo implementada de privatização e liberalização, *maxime* no âmbito do PAEF, teve “*o objetivo de diminuição da presença do Estado na economia e tinha como contrapartida criar os meios e mecanismos para que houvesse uma regulação forte e independente do poder político. Esta regulação abrangia desde logo o regulador transversal que é a AdC, o qual na prática assume preponderância em resultado de um conjunto de fatores*” (M. ROSADO DA FONSECA, *As Diligências de Busca e Apreensão em Processos sancionatórios*, in *Novos Estudos de Compliance e Direito Penal*, 2020, Almedina, p. 467), por isso impondo-se manter “*presente esta dialéctica entre os dois objetivos de política económica para, por um lado, se apreender o contexto do reforço dos poderes sancionatórios da AdC e dos reguladores abrangidos pela Lei-Quadro e, por outro e numa perspetiva de futuro, ter presentes os pressupostos subjacentes à opção estratégica, assente na independência e reforço dos poderes dos reguladores [que suportam o] (...) âmbito dos poderes de investigação.*” (*ibidem*).

Ainda em reforço do exposto e citando VITAL MOREIRA (a propósito da jurisprudência constitucional sobre apreensão de correio eletrónico em processos criminais, mas, a nosso ver, transponível, *mutatis mutandis*, para a controvérsia aqui colocada, face ao contexto das infrações), “*o excesso de garantismo processual desequilibra o necessário compromisso entre a eficácia punitiva do processo penal e as liberdades individuais, podendo pôr em risco a obrigação punitiva do Estado e gerar a descrença social nas instituições penais, um dos alimentos preferidos do populismo político*” (causa-nossa.blogspot.com/2021/09).

In casu, ações intrusivas efetivadas ao abrigo da norma-objeto serão pontuais e localizadas, cingir-se-ão a estruturas com dimensão que lhes permita impactarem nos equilíbrios concorrenciais – como tal em número muito reduzido de entre o universo empresarial, cingidas a mercados em que exista concentração de operadores –, e a sua realização dependerá de aquisição de notícia da infração e de razoável acervo indiciário, já que as operações estarão subordinadas a autorização pelo Ministério Público. A autonomia deste organismo, dissociado da entidade administrativa a quem incumbe a iniciativa (a AdC) e a sua vinculação estrita a critérios de legalidade (artigo 219.º,

434
L

TRIBUNAL CONSTITUCIONAL

n.ºs 1 e 2, da Constituição da República Portuguesa), é garantia da conexão entre a ação intrusiva e o referente legitimador, excluindo ações persecutórias, frívolas ou desproporcionais.

O controlo jurisdicional subsequente sobre a validade do meio de prova (também em função da forma como foi obtida) e a apreciação das condições da sua autorização e de execução da medida no terreno – para o que a entidade visada dispõe de meio de impugnação específico e intercalar (artigo 55.º, n.º 1, do RGC) e que se compreenderá também no objeto do julgamento –, constitui uma segunda salvaguarda contra qualquer forma de instrumentalização ou de abuso.

Em suma, a defesa da concorrência, de que a norma do artigo 18.º, n.º 1, alínea c), do RJdC, constitui condição de eficácia mínima, pretende garantir a abertura dos mercados e os seus processos de equilíbrio entre agentes (consumidores incluídos), promovendo a melhor eficiência dos circuitos económicos na função de geração, retenção e distribuição da riqueza ao repelir práticas parasitárias ou predatórias altamente censuráveis que colocam em risco o desempenho daquela função. A norma oferece efetividade, pois, à *liberdade de iniciativa económica e de empresa* (artigo 61.º, n.º 1, da Constituição da República Portuguesa), à *defesa do consumidor* (artigo 60.º, n.º 1, da Constituição da República Portuguesa) e é condição de *tarifas essenciais do Estado*, especialmente no plano económico (artigos 9.º, alínea d) e 80.º, alínea c), ambos da Constituição da República Portuguesa). A norma não tem por contrapartida mais que uma lesão moderada no exclusivo gestionário sobre informação de caráter económico, assim sem invadir espaços sensíveis da tutela da pessoa humana e está envolvida por um quadro jurídico-processual de garantias de defesa efetivo.

À guisa de remate, em face de todo o exposto, resta-nos concluir que a norma do artigo 18.º, n.º 1, alínea c), do RJdC, interpretada no sentido de *permitir a Autoridade da Concorrência, em processo contraordenacional, o exame, recolha e apreensão de mensagens de correio eletrónico assinaladas no sistema informático como «abertas» ou «lidas», sem necessidade de autorização judicial prévia, bastando a que tenha sido concedida pelo Ministério Público*, não enferma de qualquer vício de inconstitucionalidade material.

13. Por decaírem no presente recurso, os recorrentes são responsáveis pelo pagamento de custas nos termos do artigo 84.º, n.º 2, da LTC. Ponderados os critérios constantes do artigo 9.º, n.º 1, do Decreto-Lei n.º 303/98, de 7 de outubro, a prática do Tribunal em casos semelhantes e a moldura abstrata aplicável prevista no artigo 6.º, n.º 1 do mesmo diploma, afigura-se adequado e proporcional fixar a taxa de justiça em 30 unidades de conta para cada um deles.

435
/2

TRIBUNAL CONSTITUCIONAL

*

III. Decisão

Nestes termos e com estes fundamentos, decide-se:

- a) Não julgar constitucional o disposto no artigo 18.º, n.º 1, alínea c), da Lei n.º 19/2012, de 8 de maio (na redação original, anterior à conferida pela Lei n.º 17/2022, de 17 de agosto), quando interpretado:
 - i) - No sentido de que “é possível, em processo de contraordenação da concorrência, examinar, recolher e apreender mensagens de correio eletrónico”;
 - ii) - No sentido de admitir a “possibilidade de exame, recolha e/ou apreensão de mensagens de correio eletrónico abertas ou didas”;
 - iii) - No sentido de “admitir o exame, recolha e apreensão de mensagens de correio eletrónico em processo de contraordenação da concorrência sem despacho judicial prévio”;
- b) Negar provimento aos recursos interpostos por Somafel – Engenharia e Obras Rodoviárias, SA e por Paulo Alfredo Carvalho Serradas.

*

Custas pelos recorrentes, que, ponderados os critérios aplicáveis, se fixa em 30 UC para cada um deles (artigo 84.º, n.º 2, da LTC e artigos 6.º, n.º 1 e 9.º, n.º 1, ambos do Decreto-Lei n.º 303/98 de 7 de outubro).

Lisboa, 04 de julho de 2024

O relator, que também junta declaração, *António José da Ascenção Ramos*, que participou na sessão por meios telemáticos, atesta o voto de vencido do Senhor Conselheiro *José Eduardo Figueiredo Dias*, das Senhoras

*KSB
R*



TRIBUNAL CONSTITUCIONAL

Conselheiras *Dora Lucas Neto* e *Mariana Canotilho* e do Senhor Conselheiro Vice-Presidente *Gonçalo de Almeida Ribeiro*, conforme declarações de voto anexas.

Assinado por: **ANTÓNIO JOSÉ DA ASCENSÃO**

RAMOS

Num. de identificação: 04386182

Data: 2024.07.04 14:26:59+01'00'

Certificado por: **Diário da República**

Atributos certificados: Juiz Conselheiro - Tribunal

Constitucional



CARTÃO DE CIDADÃO

• • •



TRIBUNAL CONSTITUCIONAL

Processo n.º 1104/2022

DECLARAÇÃO DE VOTO

1. Em complemento ao que vai exposto no acórdão, sustenta ainda a minha posição o que seguidamente exponho, que a maioria entendeu ser de excluir do texto do arresto.

Como consta da decisão, assumo a posição que os sistemas de comunicações eletrónicas (emails, sistemas de *cloud*, mensagens eletrónicas, etc.) beneficiam da proteção conferida pelo artigo 34.º, n.º 4, da CRP nos processos de transferência de dados que executam (tanto conteúdos, como metadados), ou seja, o sistema webmail (e qualquer outro sistema de mensagens eletrónicas) beneficia daquela especial proteção constitucional quando realiza processos comunicativos, à semelhança de qualquer outro meio de comunicação.

Já não beneficiam dessa forma de tutela, porém, os ficheiros de dados criados por esses sistemas que se encontrem armazenados em aparelhos eletrónicos. Nessas situações, as mensagens e demais dados contidos nos ficheiros beneficiam da proteção proporcionada por outros direitos fundamentais, o que, quando colocados no âmbito do fenômeno empresarial, permite quadros legais que confirmaram poderes à AdC para a busca e apreensão sob autorização de Magistrado do Ministério Público em processos por infrações à concorrência, desde que garantido (como está) instituto de sindicância jurisdicional subsequente das operações de pesquisa e recolha de prova.

Abordarei agora duas matérias que são, a meu ver, centrais para o problema que aqui se coloca, a primeira das quais (*infra* (2)) respeitante às consequências a contraluz do Direito europeu associadas à qualificação de ficheiros armazenados em dispositivos eletrónicos como *comunicações*, sujeitando por isso a norma fiscalizada ao crivo do artigo 34.º, n.º 4, da CRP; a segunda (*infra* (3)), sobre a (des)necessidade de autorização jurisdicional para a realização de buscas a ficheiros informáticos contendo mensagens ao abrigo do artigo 18.º, n.º 1, alínea c), do RJdC, defendida pelo Acórdão do TC n.º 91/2023 e pelos Conselheiros «vencidos», também no confronto com normas e princípios de Direito europeu.

Introduzirei na presente declaração a recente (20 de junho de 2024) pronúncia da Advogada-Geral junto do Tribunal de Justiça da União Europeia nos Procs. C-258/23, 259/23 e C-260/23 (*IMI – Imagens Médicas Integradas, SA et al.*), decorrentes do acionamento de reenvio



TRIBUNAL CONSTITUCIONAL

prejudicial pelo Tribunal da Concorrência, Regulação e Supervisão a respeito da admissibilidade da apreensão de correio eletrónico ao abrigo do artigo 18.º, n.º 1, alínea c), do RJdC, perante o disposto nos artigos 7.º, 51.º, n.os 2 e 3, da Carta de Direitos Fundamentais da União Europeia (CDFUE) e no artigo 6.º da Diretiva (UE) 2019/1 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018 (Diretiva ECN+).

É certo que não se trata de um precedente prudencial, nem sequer de uma decisão jurisdicional, mas a tomada de posição da Advogada-Geral não deixa de aportar contributos importantes para o objeto deste processo de fiscalização, como adiante se notará.

2. A propósito da primeira questão, sejamos claros. Caso, em oposição ao presente acórdão, se aceite que a apreensão de ficheiros informáticos contendo mensagens armazenados em dispositivos eletrónicos constituem ingerência em telecomunicações, existem apenas duas possibilidades: ou se acede à abertura da reserva de processo penal das comunicações constante do artigo 34.º, n.º 4, da CRP nos termos propostos pelo Acórdão do TC n.º 91/2023, admitindo meios de obtenção de prova intrusivos em processos comunicativos no âmbito da investigação de contraordenações; ou o artigo 34.º, n.º 4, da CRP, é incompatível com a Diretiva ECN+, transposta entre nós pela Lei n.º 17/2022, de 17 de agosto, que, entre outros, alterou o artigo 18.º do RJdC, ora fiscalizado.

Se a referida reconstrução da reserva de processo criminal se afigura extremamente insatisfatória e está tratada no texto do acórdão pela forma que propus à secção e que formou maioria entre os Conselheiros subscritores, impõe-se ver mais de perto o conflito que se suscita entre Direito constitucional e Direito europeu a que agora me refiro.

A Diretiva ECN+ ocupou-se de garantir a implementação pelos Estados-membros de um estatuto legal de investigação e instrução probatória apto a sinalizar e reprimir atividades anticoncorrenciais no espaço da União. Aqui se inclui a obrigatoriedade de os Estados conferirem às autoridades nacionais da concorrência (ANC) poderes de acesso e de valoração como prova de *todos os registos de comunicações* das entidades inspecionadas, incluindo webmail e sistemas de *messaging* análogos (cfr. artigo 6.º, n.º 1, alíneas a), b) e c), da Diretiva ECN+):

"Para ser eficaz, a competência das autoridades administrativas nacionais da concorrência para realizar inspeções deverá permitir-lhes ter acesso a informações acessíveis à empresa ou associação de empresas ou à pessoa sujeita a inspeção e relacionadas com a empresa ou associação de empresas investigada. Deverá assim incluir necessariamente a competência para pesquisar documentos, ficheiros ou dados em dispositivos não previamente identificados com precisão. Sem uma tal competência, seria impossível obter as informações necessárias à investigação nos casos em que as empresas ou associação de empresas assumissem uma atitude de obstrução ou se recusassem a cooperar. A



439

TRIBUNAL CONSTITUCIONAL

competência para examinar livros ou outros documentos deverá ser extensiva a todas as formas de correspondência, incluindo mensagens electrónicas, independentemente de parecerem não ter sido lidas ou de terem sido apagadas.” (§ 32 da Diretiva ECN+)

“As ANC deverão dispor de competência efectiva para exigir que as empresas ou associações de empresas lhes fornecam as informações necessárias para detetar infrações aos artigos 101.º e 102.º do TFUE. Para tal, as ANC deverão poder exigir a divulgação de informações que lhes permitam investigar potenciais infrações. Tal deverá incluir o direito de exigir informações em qualquer formato digital, incluindo mensagens de correio electrónico ou de um sistema de mensagens instantâneas, independentemente do local em que estejam armazenadas, nomeadamente em nuvens e servidores, desde que a empresa ou associação de empresas destinatária do pedido de informações tenhacesso às mesmas.” (§ 35 da Diretiva ECN+)

“A prova é um elemento importante para a aplicação dos artigos 101.º e 102.º do TFUE. As ANC deverão poder ter em consideração os elementos de prova relevantes, independentemente de serem escritos, orais, em formato electrónico ou gravados. (...) as ANC deverão poder considerar as mensagens electrónicas como prova relevante, independentemente de estas mensagens parecerem não ter sido lidas ou de terem sido apagadas.” (§ 73 da Diretiva ECN+)

A Diretiva ECN+ determina a necessidade de implementar quadros legais internos que confiram às ANC dos Estados-membros acesso ao universo de elementos que documentem comunicações com relevo para a investigação de práticas anticoncorrenciais, bem como a possibilidade de os utilizarem como meios de prova. Adota a este título um conceito amplo de *documento* e inclui qualquer forma de suporte de informação, também (*expressis verbis*) mensagens de webmail e de *instant messaging* (“*documentos, ficheiros ou dados em dispositivos*”, “*mensagens de correio electrónico ou de um sistema de mensagens instantâneas*”, “*elementos de prova relevantes, independentemente de serem escritos, orais, em formato electrónico ou gravados*” – §§ 32, 35 e 73 da Diretiva ECN+ e cfr. artigo 6.º, n.º 1, alíneas a), b) e c), do mesmo diploma).

Um elemento de importância cardinal reside no critério adotado pela Diretiva para entender mensagens electrónicas passíveis de apreensão em processos dirigidos à repressão de práticas anticoncorrenciais. Este reside na sua mera *acessibilidade* pela entidade inspecionada (cfr. artigo 6.º, n.º 1, alíneas a), b) (*maxime, in fine: “quaisquer informações acessíveis à entidade inspecionada”*) e c), da Diretiva ECN+), sem necessidade de associação a quaisquer outros requisitos (fossem ações do utilizador ou local de armazenamento), assim opondo-se frontalmente ao paradigma do Acórdão n.º 91/2023. Ao mesmo tempo que adota como objeto da apreensão um ficheiro *«em repouso»* (isto é, fixado em sistema e não em trânsito), a norma faz depender o poder de apreensão da faculdade de acesso a informação pela empresa visada: desde que esta possa aceder à mensagem por recursos próprios, ela será também acessível pelas autoridades, seja qual for o local onde se encontre (“*independentemente do local em que estejam armazenadas, nomeadamente em nuvens e servidores, desde que a*



TRIBUNAL CONSTITUCIONAL

440/2023

"empresa ou associação de empresas destinatária do pedido de informações tenha acesso às mesmas." – § 35 da Diretiva ECN+).

Isto significa que o *locus* da mensagem identificado pelo Acórdão do TC n.º 91/2023 é tido por elemento caracterizador da mensagem como *comunicação* («*caixa de correio eletrónica virtual*» para o Acórdão do TC n.º 91/2023), não poderá impedir, a contraluz da Diretiva ECN+, a AdC de aceder e apreender ficheiros ou mensagens para efeitos de instrução probatória de processos por infrações ao Direito *antitrust*, já que nesse *locus* ela é acessível pela empresa investigada.

Pois bem, dotando a mensagem nestas condições da tutela que resulta do artigo 34.º, n.ºs 1 e 4, da CRP e inerente sujeição a reserva de processo criminal, a natureza contraordenacional dos processos por infração a concorrência não permitiria à AdC aceder ou apreender esses dados, como proibiria a sua utilização subsequente como prova, atingindo diretamente o conteúdo da Diretiva ECN+, de transposição injuntiva para o Direito interno.

Podemos acrescentar que, mesmo que se entendesse que *apenas* as mensagens *fechadas* (assinaladas como não-lidas) na «*caixa postal virtual*» constituíssem *comunicações* – por isso apenas este grupo beneficiando da proteção constitucional conferida às comunicações e inerente reserva de processo criminal –, ainda assim se imporia concluir por um encurtamento inadmissível dos poderes das ANC a contra-luz da sobredita Diretiva ECN+.

Também este entendimento, repelido pelo Acórdão do TC n.º 91/2023 por se mostrar uma forma *insuficiente* de proteção do segredo das comunicações, oferece uma proteção *excessiva* a mensagens eletrónicas perante a fonte de Direito europeu. Isto é assim porque *também* as mensagens *fechadas* são *acessíveis* pelo particular, sem diferença assinalável face às «*abertas*», e porque o diploma expressamente impõe que *todas* as mensagens eletrónicas nessas condições sejam passíveis de apreensão e utilizáveis no plano probatório («*A competência para examinar livros ou outros documentos deverá ser extensiva a todas as formas de correspondência, incluindo mensagens eletrónicas, independentemente de parecerem não ter sido lidas ou de terem sido apagadas.*» – § 32 da Diretiva ECN+, sublinhado nosso; cfr. artigo 6.º, n.º 1, alíneas a), b) e c), do mesmo diploma).

O Tribunal Constitucional tem vindo a sublinhar de forma enfática a primazia do Direito europeu (primário ou derivado) e a sua prevalência perante fontes de Direito interno (Acórdãos do TC n.ºs 422/2020, 268/2022, 198/2023 e 800/2023), pelo que encontramos aqui, como se disse, uma violenta colisão entre o Direito europeu e o (pretendido) estatuto constitucional.

A meu ver, este conflito é apenas aparente e decorre da compreensão incorreta do instituto fiscalizado: se os textos dos artigos 7.º da CDFUE e 8.º da CEDH não individualizam as comunicações como objeto de tutela reforçada, face à privacidade, ao contrário do que sucede com



445
1/2

TRIBUNAL CONSTITUCIONAL

o n.º 4, do artigo 34.º, da CRP, na verdade o Direito constitucional não oferece maior grau de defesa do que aquela que é conferida pelo Direito europeu na matéria que tratamos. O problema reside em insistir-se em qualificar como «comunicação» aquilo que não tem essa natureza, corrompendo o âmbito de tutela do artigo 34.º, n.º 4, da CRP. O artigo 18.º, n.º 1, alínea c), do RjdC (na redação sindicada, nas precedentes e na atualmente em vigor) limita-se a permitir a pesquisa e apreensão de *dados armazenados em dispositivos eletrónicos*, não a interferência em processos de comunicação intersubjetiva. Jamais se defendeu, com base na Diretiva ECN+, de qualquer outro ato normativo de Direito Europeu ou de qualquer norma de Direito interno, que a Comissão Europeia, as ANC ou a AdC portuguesa dispusessem de poderes para realizar intercessões em comunicações, fossem «escutas» telefónicas ou em aparelhos informáticos quando trocam informação pela internet: *in casu*, a norma sindicada ocupa-se apenas em conferir autoridade para *buscas a empresas* para obtenção de documentos em formato digital, nada mais.

Recusando distender a autodeterminação comunicativa a ficheiros armazenados em dispositivos eletrónicos, a posição adotada no presente acórdão, pois, desvia a tutela constitucional das telecomunicações da rota de colisão com a Diretiva ECN+ em que a colocou a doutrina do Acórdão do TC n.º 91/2023, antes converge com o disposto neste ato normativo de Direito europeu, depondo pela preservação do estatuto constitucional.

Sem deixar de assinalar – uma vez mais – que o artigo 18.º, n.º 1, alínea c), do RjdC, não capacita a AdC a realizar ingerências em processos comunicativos, o presente acórdão elege um critério semelhante ao da Diretiva para a apreensão de documentos eletrónicos contendo mensagens, excluindo do espectro defensivo definido pelo artigo 34.º, n.º 4, da CRP a apreensão pela AdC de ficheiros de dados *armazenados* nos dispositivos da entidade visada ou em servidor remoto (quanto a este último, desde que a empresa possa aceder-lhe diretamente). Estes poderes são exteriores à reserva de processo penal e, por inerência, a solução legal não incorre em vício de inconstitucionalidade material.

Serve por dizer, o entendimento proposto aconselha-se, não apenas por todo o exposto, mas também em face da primazia do Direito europeu e do inerente princípio de interpretação do Direito interno (também do Direito constitucional) em conformidade com ele, que, em respeito pelos princípios estruturantes do Estado de Direito (sobre o alcance deste princípio e os poderes cognitivos do Tribunal Constitucional, v. Acórdão do TC n.º 422/2020), tem vindo a ser sublinhado de forma muito enfática pela jurisprudência deste Tribunal:



Q4C
L

TRIBUNAL CONSTITUCIONAL

“(...) O princípio da interpretação conforme — nascido na década de 70 do século XX a propósito da obrigação de os tribunais nacionais alcançarem, através da interpretação do direito nacional, o efeito útil de directivas insuscetíveis de produzir efeito direto (cfr., entre muitas outras, Acórdãos do TJUE Mazzalai, de 20.05.1976, proc. 111/75, e Von Colson, de 10.04.1984, proc. 14/83; Marleasing, de 13.11.1990, proc. 106/89) — foi sendo reconstruído a um cânones geral de interpretação do direito nacional (de todo o direito nacional) de modo a atingir a plena eficácia do direito da União Europeia. Determina tal princípio que os tribunais nacionais, ao aplicar o direito interno, são obrigados a interpretá-lo, na medida do possível, à luz do direito europeu: «Esta obrigação de interpretação conforme do direito nacional é inerente ao sistema do Tratado FUE, na medida em que permite aos órgãos judiciais nacionais assegurar, no âmbito das suas competências, a plena eficácia do direito da União quando decidem dos litígios que lhes são submetidos» (Acórdão do TJUE de 24.01.2012, Maribel Dominguez, proc. C-282/10).

Assim, os tribunais dos Estados-Membros, na fixação do sentido das normas de direito nacional, estão vinculados ao efeito útil do direito europeu e devem, dentro da margem permitida pelas regras interpretativas internas, escolher a exegese que melhor se acomode às normas europeias. No fundo, no seio da obrigação de as autoridades nacionais tomarem as medidas que garantam a efetividade do direito da União, «uma dessas medidas consiste precisamente na obrigação de os tribunais, e as restantes autoridades nacionais, interpretarem a lei nacional em conformidade com o direito da União» (cfr. SOFLA OLIVEIRA PAIS, “Princípio da interpretação conforme”, Princípios Fundamentais de Direito da União Europeia, 3.º Edição, Almedina, 2016, p. 96). Trata-se, pois, de uma garantia de eficácia do direito europeu plenamente recebida pelo disposto no n.º 4 do artigo 8.º da Constituição.”

(Acórdão do TC n.º 268/2022)

Contra o exposto, poder-se-á dizer (também em linha com o Acórdão do TC n.º 91/2023), que a Diretiva ECN+ entrou em vigor apenas em 3 de fevereiro de 2019 (cfr. artigo 36.º do diploma), achando-se desprovida de efeito direto na ordem jurídica interna e com data máxima de transposição para 4 de fevereiro de 2021. Por esse motivo e porque as ações de busca e apreensão realizadas na causa principal ao abrigo do artigo 18.º, n.º 1, alínea c), do RjdC, foram realizadas entre os dias 12 e 24 de julho de 2017, a disciplina estabelecida por aquela Diretiva não participa no juízo de validade firmado pela jurisdição sobre os atos de obtenção de prova em causa. Pode dizer-se, enfim, que a Diretiva ECN+ não influiu na interpretação do parâmetro constitucional a cujo crivo se sujeita a norma fiscalizada, já que esta foi aplicada antes de este ato normativo de Direito europeu ter adquirido vigência.

No entanto, já se afigura inegável que considerar que mensagens eletrónicas armazenadas em aparelhos locais ou servidores está acobertada pelo artigo 34.º, n.º 4, da CRP deflagra um conflito direto e imediato entre a Diretiva ECN+ e a CRP, quando a norma se aplique a operações realizadas *depois* de 3 de fevereiro de 2019; permite também ter por inevitável, como dissemos, juízo de reprovação constitucional sobre as alterações introduzidas no preceito pela Lei n.º 17/2022, de 17 de agosto, que transpôs a Diretiva. Não é legítimo descurar este facto e o que implica para a ordem jurídica portuguesa (e europeia).



TRIBUNAL CONSTITUCIONAL

Por outra parte e porventura com maior importância, será também de sublinhar que os poderes de busca e apreensão de documentos em formato eletrónico em causa *não surgiram* no ordenamento europeu em 3 de fevereiro de 2019 pela Diretiva ECN+, ao contrário do que parece sugerir o Acórdão do TC n.º 91/2023. Estes poderes foram conferidos à Comissão no âmbito de investigação a infrações contra a concorrência pelo Regulamento (CE) n.º 1/2003 de 16 de dezembro de 2002 (cfr. artigo 20.º, n.ºs 1 e 2, alíneas a), b) e c) e 4) e são pelo menos desde então uma componente da ordem jurídica europeia.

Na “*Nota explicativa relativa às inspeções da Comissão, em conformidade com o artigo 20.º, n.º 4, do Regulamento n.º 1/2003 do Conselho*”, a Comissão Europeia (DG da Concorrência) detalhou o âmbito das inspeções e dos poderes conferidos aos inspetores na execução de buscas e apreensão em instalações por infrações à concorrência nos seguintes termos:

“9. Os inspetores têm o direito de examinar os livros e outros registos relacionados com a atividade, independentemente do seu suporte, e de tirar ou obter sob qualquer forma cópias ou extractos de tais livros ou registos. Tal inclui, igualmente, o exame de informações eletrónicas e a sua cópia, em suporte eletrónico ou papel.

10. Os inspetores podem pesquisar o ambiente informático (por exemplo, servidores, computadores de secretária, computadores portáteis, tablets ou outros dispositivos móveis) e todos os suportes de armazenamento de dados (por exemplo, CD-ROM, DVD, chaves USB, discos rígidos externos, bandas magnéticas de salvaguarda e os serviços de computação em nuvem) da empresa. Esta disposição aplica-se também aos dispositivos e meios de comunicação privados que são utilizados para fins profissionais (*Bring Your Own Device - BYOD*) quando são encontrados nas instalações. Para o efeito, os inspetores podem não só utilizar qualquer ferramenta de pesquisa integrada (palavra-chave), como também recorrer ao seu próprio software e/ou hardware específico (ferramentas de informática forense). Estas ferramentas de informática forense permitem à Comissão copiar, pesquisar e recuperar dados, respeitando simultaneamente a integridade dos sistemas e dos dados da empresa.”

Está bom de ver, a atribuição a autoridades públicas de poderes de pesquisa e apreensão de ficheiros armazenados em sistemas informáticos de empresas no âmbito de infrações à concorrência era já uma componente normativa do Direito europeu antes da Diretiva ECN+, integrada que estava na moldura do Regulamento (CE) n.º 1/2003.

Um putativo conflito entre o artigo 34.º, n.º 4, da CRP, e a atribuição destes poderes a entidades públicas por quadros de Direito europeu, pois, *precede* a Diretiva ECN+, não surgiu com ela. A Diretiva não introduziu qualquer novidade sobre o *âmbito* das operações admitidas pelo Direito europeu, pois que a Comissão beneficiava já de poderes de exame de aparelhos aptos à fixação de informação da empresa investigada e todos aqueles a que esta possuisse acesso direto, incluindo “servidores” e “serviços de computação em nuvem”, permitindo o exame por “ferramentas de informática forense” de cópia, pesquisa e recuperação de dados, incluindo ficheiros resultantes de processos prévios de transferência de dados entre sistemas.



444
R

TRIBUNAL CONSTITUCIONAL

A menos que se pretenda defender que o artigo 34.º, n.º 4, da CRP, impede a eficácia do Regulamento (CE) n.º 1/2003, na ordem jurídica portuguesa e oferece obstáculo a que a Comissão desenvolva este tipo de atividades investigatórias na jurisdição nacional ao abrigo do Regulamento (CE) n.º 1/2003, não é defensável que a interpretação conferida ao artigo 18.º, n.º 1, alínea c), do RjdC, pelo Tribunal “*a quo*” seja proibida pela Lei Fundamental.

Por outro lado, o Regulamento (CE) n.º 1/2003 de 16 de dezembro de 2002 veio implementar um modelo difuso de fiscalização e repressão da atividade anticoncorrencial no espaço da União, implementando uma rede de entidades nacionais da concorrência e devolvendo-lhes competência nesse âmbito, em cooperação entre si e com a Comissão (artigos 5.º, 11.º e 22.º). Os poderes de inquérito e de inspeção relativos a infrações à concorrência estabelecidos no diploma incluindo quanto a pesquisas e apreensões de dados, respeitavam apenas ao organismo europeu (artigo 20.º), como acima dissemos, o que significa que continuou a deferir-se para o Direito interno a definição dos recursos ao dispor das ANCs para o desempenho da sua missão e respetivas condições processuais (v., sobre o assunto, C. Potocnik-Manzouri, *The ECN+ Directive: An Example of Decentralised Cooperation to Enforce Competition Law*, in European Papers, Vol. 6, 2021, n.º 2, pp. 990-993).

No entanto, a Comissão ocupou-se de imediato em procurar obter convergência entre jurisdições a este respeito. Foi então criada ao abrigo do Regulamento (CE) n.º 1/2003 a *Rede Europeia da Concorrência* [European Competition Network (ECN)] e formuladas recomendações sobre o catálogo de poderes a conferir às ANCs pelos Estados membros, particularmente no domínio de inspeções a empresas e de poderes de apreensão de ficheiros informáticos, também os que contenham mensagens eletrónicas.

Na *ECN Recommendation on Investigative Powers, Enforcement Measures and Sanctions in the Context of Inspections and Requests for Information*, a ECN recomendou aos Estados que assegurassem por quadros legais de Direito interno de que seria possível às ANCIs “*entrar nas instalações [de empresas] e examinar livros e outros registos relacionados com a empresa, independentemente do meio em que estejam armazenados* [i. e., incluindo ficheiros digitais], “*efetuar cópias ou extratos de livros e de outros registos relacionados com o negócio, independentemente do meio em que estejam armazenados* [i. e., incluindo ficheiros digitais] e/ou apreender documentos originais durante as inspeções” e, com maior importância, “*recolher prova digital e/ou forense*” (B. Inspeção de Instalações de Empresas, II. Recomendações ECN).

Especificamente sobre a questão colocada nestes autos, a *ECN Recommendation on the Power to collect digital Evidence, including by forensic Means* recomendou aos Estados o seguinte:



TRIBUNAL CONSTITUCIONAL

442
X

"1. Todas as Autoridades devem dispor de poderes efetivos e eficazes de recolha de prova digital, incluindo prova obtida por ferramentas forenses, através de inspeções a empresas (...) Para esse fim, as Autoridades devem ter o poder de recolher toda a informação em formato digital relacionada com a(s) empresa(s) sob investigação, independentemente do meio em que esteja armazenada e da evolução tecnológica do aparelho de gravação. As Autoridades devem ter também poderes para realizar informação digital pela realização de cópias, incluindo imagens forenses dos dados e/ou pela apreensão dos aparelhos de gravação.

2. O poder de recolha de prova digital, incluindo prova obtida através de instrumentos forenses, como definido pela Recomendação 1, deve incluir o direito de aceder à informação que seja acessível à pessoa investigada cujas instalações estão a ser inspecionadas e que esteja relacionada com a(s) empresa(s) sob investigação."

(sublinhado nosso)

Foi no desenvolvimento destes instrumentos de *soft law* que a Diretiva ECN+ veio a surgir, especificando as atividades e poderes admitidos às ANC's, designadamente no que tange a apreensão de correio eletrónico arquivado e instrumentos forenses passíveis de serem utilizados, com o inerente dever de transposição pelos Estados (artigo 288.º, § 3, do TFUE).

No entanto, também por aqui resulta evidente que a Diretiva não introduziu qualquer novidade sobre o âmbito das operações admitidas a entidades reguladoras da concorrência pelo Direito europeu, antes limitou-se a estabelecer a vinculação estrita dos Estados membros a conformarem a sua Lei ordinária para com aquele no que tange os poderes conferidos às ANC's: a Comissão beneficiava já de poderes de exame dos aparelhos eletrónicos aptos à fixação de informação da empresa e todos aqueles a que esta possuisse acesso direto, incluindo "servidores" e "serviços de computação em nuvem", permitindo o exame por "ferramentas de informática forense" de cópia, pesquisa e recuperação de dados ao abrigo do Regulamento (CE) n.º 1/2003, este dotado de eficácia direta (cfr. artigo 288.º, § 2, do TFUE).

A Diretiva veio apenas assegurar-se que toda a rede de ANC's dispusesse das mesmas prerrogativas ao abrigo do Direito interno dos Estados membros.

Em *IMI – Imagens Médicas Integradas, SA et al.*, a Advogada-Geral junto do TJUE fez ver isto mesmo, sustentando com base na jurisprudência do Tribunal firmada a propósito dos poderes da comissão ao abrigo do Regulamento (CE) n.º 1/2003, a compatibilidade com o Direito da União dos poderes conferidos à AdC pela Lei portuguesa (e pela Diretiva ECN+):

"as ingerências no exercício dos direitos consagrados no artigo 7.º da Carta [privacidade e comunicações] que decorrem das inspeções e das apreensões efetuadas pelas autoridades nacionais de concorrência quando aplicam, em conformidade com o artigo 3.º, n.º 1, e com o artigo 5.º do Regulamento (CE) n.º 1/2003, os artigos 101.º e 102.º TFUE, têm por finalidade detetar práticas contrárias a essas disposições. Ora, o Tribunal de Justiça já teve ocasião de afirmar [Nordzucker and Others, 22 de junho de 2022] que os artigos 101.º e 102.º TFUE são disposições de ordem pública que proíbem respetivamente os acordos e os abusos de posição dominante e que tem por finalidade, indispensável ao funcionamento do mercado interno, garantir que a concorrência não seja falseada nesse mercado. (...) como salienta a corretamente a Comissão, no ambiente digital atual, a correspondência electrónica constitui uma das principais formas através das quais as empresas atuam. Assim, as diferentes formas em que esta correspondência

446
L



TRIBUNAL CONSTITUCIONAL

se declina, como as mensagens de correio eletrónico trocadas através de caixas de correio profissionais, tornaram-se elementos de prova frequentemente insubstituíveis para detetar práticas anticoncorrenciais. Resulta, além disso, da jurisprudência do Tribunal de Justiça que a revista e a apreensão de mensagens de correio eletrónico pela Comissão no exercício dos poderes que o artigo 20.º do Regulamento n.º 1/2003 lhe confere são admissíveis, desde que sejam juntas ao processo as mensagens de correio eletrónico pertinentes. Do mesmo modo, resulta da jurisprudência do TEDH que tais medidas não são a priori excluídas no quadro de processos administrativos, quando a ingérvia no direito ao respeito pela correspondência é proporcional à importância do objetivo legítimo prosseguido. Atendendo às considerações expostas, considero que o artigo 7.º da Carta não se opõe à revista e à apreensão, por uma autoridade nacional da concorrência, de mensagens de correio eletrónico trocadas através da caixa de correio interna de uma empresa sujeita a uma inspeção nas suas instalações profissionais ou comerciais no quadro de um inquérito por infração às regras da concorrência, desde que essas mensagens sejam pertinentes para o objeto da inspeção.”

(sublinhado nosso)

Levando em conta todo o exposto, impõe-se concluir que, porque o Regulamento (CE) n.º 1/2003, entrou em vigor em 24 de janeiro de 2003 e tornou-se aplicável em 1 de maio de 2004 (cfr. artigo 45.º), desde essa data se impõe interpretar o artigo 34.º, n.º 4, da CRP, em conformidade com o ato normativo de Direito europeu: se é evidente que o que se consentia à Comissão, não seria proibido às autoridades nacionais, não existe óbice em interpretar o artigo 18.º, n.º 1, alínea c), do RJdC, como conferindo à AdC os poderes conferidos pelo Regulamento (CE) n.º 1/2003 à Comissão, mesmo antes da aprovação da Diretiva ECN+, do inicio da sua vigência, ou do esgotamento do prazo para a sua transposição. A harmonia e a continuidade entre o Direito Europeu e o Direito Constitucional aconselham esta leitura da autodeterminação comunicativa, excluindo a *distensão* desta forma de tutela a ficheiros *armazenados* que contenham mensagens eletrónicas.

De assinalar também que a compaginação destes poderes de investigação com direitos fundamentais *nunca foi controversa* para os Tribunais europeus, desde que respeitadas as garantias de processo, *a pari* com outros métodos de inquérito intrusivos na privacidade de empresas ou de pessoas singulares com elas relacionadas (v. g., Acórdãos do TEDH de 2 de janeiro de 2015, *Delta Pekární v. Republika Česká; Vinci Construction e GMT v. França*, de 2 de abril de 2015; Acórdãos do TJUE *Nexans France v. Comissão Europeia*, de 14 de novembro de 2012; neste caso, porém, cabe assinalar que se debatia a sujeição da entidade privada ao acesso a documentos digitais pela Comissão no âmbito de investigação a infrações a concorrência, incluindo webmail, e as condições de recurso desses atos; e *Nexans France v. Comissão Europeia*, de 12 de julho de 2018; v.. M. P. ANTUNES, *op. cit.*, 176, 2023, p. 116).

Em *Nexans France v. Comissão Europeia* (12 de julho de 2018), o TJUE apreciou a licitude da apreensão de emails apreendidos em instalações e mais tarde examinados nas instalações da Comissão (§§ 52-64), nos seguintes termos:



447
a

TRIBUNAL CONSTITUCIONAL

"No presente caso, a prática de realizar uma imagem-cópia do disco rígido de um computador ou uma cópia dos dados armazenados num aparelho de armazenamento digital toma lugar no contexto de uma operação de FIT, que os oficiais da Comissão utilizam durante as inspeções. (...) a tecnologia envolve a utilização de software específico para pesquisar o disco rígido de um computador ou qualquer outro dispositivo de armazenamento de dados em busca de informação relevante para a matéria que é objeto da inspeção através de palavras-chave.

A pesquisa impõe uma fase preliminar apelidada de indexação, durante a qual o software coloca todas as letras e palavras no disco rígido de um computador ou outro dispositivo de armazenamento de dados sob inspeção num catálogo. A duração da indexação depende do tamanho do dispositivo de armazenamento de dados em questão, mas geralmente toma tempo considerável. Nessa situação, os oficiais da Comissão geralmente realizam uma cópia da informação contida no dispositivo de armazenamento inspecionado para indexar os dados fixados. No caso de um disco rígido de um computador, esta cópia toma a forma de uma imagem-cópia. Esta imagem-cópia torna possível obter uma verdadeira cópia do disco rígido inspecionado, contendo toda a data no disco rígido no preciso momento em que a cópia foi realizada, incluindo ficheiros que, em aparência, tenham sido apagados.

A este respeito, há que dizer que (i) (...) a cópia dos dados fixados no dispositivo de armazenamento de uma empresa inspecionada é realizada para o propósito de indexação e que (ii) a indexação tem por escopo possibilitar a busca pelos documentos relevantes para a investigação, subsumindo esta operação de cópia ao âmbito dos poderes conferidos à Comissão pelo artigo 20(2) b) e c) do Regulamento n.º 1/2003.

Ao contrário do alegado pelo Autor, não decorre do artigo 20(2) b) e c) do Regulamento n.º 1/2003 que o poder da Comissão de obter cópias ou extratos dos livros ou registos relacionados com o negócio da empresa inspecionada esteja limitado aos livros e registos relacionados com o negócio que já vistoriou.

Por outro lado, deve ser observado que tal interpretação poderia minar a efetividade do artigo 20(2) b) do Regulamento, na medida que, em certas circunstâncias, o exame de livros e registos relacionados com o negócio ou empresa inspecionada pode necessitar de cópias de tais livros ou registos de negócio antecipadamente, ou de ser simplificado, como no presente caso, através da realização da cópia.

Em consequência, dado que a realização da imagem-cópia do disco rígido do computador do Sr. M. e cópias de conjuntos de emails encontrados nesse computador e no computador do Sr. R. constituem parte do processo através do qual os oficiais da Comissão realizaram o FIT, cujo propósito era procurar informação relevante para a investigação, a operação compreende-se no âmbito do artigo 20(2) b) e c) do Regulamento n.º 1/2003.

(...) com respeito ao argumento do Autor de que os oficiais da Comissão não dispunham de poderes para pesquisar informação relevante para a investigação contida na imagem-cópia do disco rígido do computador do Sr. J. e nas cópias dos conjuntos de emails encontrados nesse computador e no computador do Sr. R. nas instalações da Comissão, deve sublinhar-se que, ao contrário do alegado pelo Autor, o artigo 20(2) b) do Regulamento n.º 1/2003 não determina que o exame de livros e registos relacionados com a empresa ou estabelecimento inspecionados tenha de ser realizado inteiramente nas instalações destas, no caso de, como é o que está colocado, não ser possível concluir essa inspeção no período de tempo inicialmente estimado. Apenas exige que a Comissão ofereça, aquando do exame dos documentos nas suas instalações, as mesmas garantias à empresa inspecionada que lhe estavam impostas na realização do exame no local da empresa. (...)

Perante o antes exposto, impõe-se concluir que, durante a inspeção, a Comissão não ultrapassou os poderes conferidos pelo artigo 20(2) do Regulamento n.º 1/2003. A pretensão do Autor terá de ser, sendo assim, rejeitada."

Como se vê, o TJUE reconheceu à Comissão, ao abrigo do Regulamento n.º 1/2003, o mesmo catálogo de poderes conferido à AdC pelo artigo 18.º, n.º 1, alínea c), do RJdC, sem que se observe qualquer censura ou sequer controvérsia sobre a sua compatibilidade com direitos garantidos pela CDFUE ou por outros atos normativos de Direito europeu.

Em *Delta Pekární v. República Checa*, deparando-se perante o TEDH uma ação de busca e apreensão de correio eletrónico no âmbito de um processo por infração à concorrência, o Tribunal abordou os poderes conferidos pelo artigo 20.º, n.º 4, do Reg. (CE) n.º 1/2003, da seguinte forma:



TRIBUNAL CONSTITUCIONAL

“a deteção de infrações às regras da concorrência vem-se tornando cada vez mais difícil e é necessário, para proteger de forma eficaz a concorrência, atribuir à Comissão poderes completos de investigação. Esta deve poder exigir todas as informações, interrogar as pessoas e proceder às inspeções necessárias para detectar as práticas proibidas pelos artigos 81 e 82 do Tratado que institui a Comunidade europeia (transposto para os artigos 101 e 102 do Tratado sobre o Funcionamento da União Europeia), tudo em benefício de uma colaboração ativa das autoridades da concorrência dos Estados membros. A fim de preservar a eficácia das inspeções, os agentes e outras pessoas agenciadas pela Comissão devem poder aceder a todos os locais suscetíveis de resguardar documentos profissionais”

Nunca inspirou preocupações à jurisprudência europeia (TEDH ou TJUE) esta amplitude dos poderes de indagação probatória conferidos à Comissão ou às ANC's em execução do Regulamento n.º 1/2003, tanto menos o formato das mensagens apreendidas ou o aparato tecnológico de armazenamento ou de consulta buscado; os Tribunais ocuparam-se apenas em avaliar a implementação de quadros processuais que garantissem controlo da legalidade e a justificabilidade do exercício desses poderes no plano dos direitos de defesa (v., para além do já citado supra, Acórdãos do TJUE de 18 de junho de 2015, *Deutsche Bahn AG e outros v. Comissão Europeia*, e de 6 de setembro de 2013 *Deutsche Bahn AG v. Comissão Europeia*).

Em suma: a distensão da tutela das comunicações dos *processos comunicativos* para cobrir também *ficheiros eletrónicos armazenados resultantes de transferência prévia de dados* resultará na impossibilidade de conciliar o artigo 34.º, n.º 4, da CRP, com o Regulamento (CE) n.º 1/2003 e com a Diretiva ECN+; ou, quando se aceda à doutrina do Acórdão n.º 91/2023, conduzirá à degradação do estatuto constitucional da defesa da autodeterminação comunicativa pela abertura da reserva de processo penal a procedimentos por contraordenação.

Serve por dizer, o entendimento exposto não se nos afigura apenas a melhor abordagem à questão colocada, constitui também condição da harmonia e continuidade entre o (e do) Direito europeu e a norma do n.º 4, do artigo 34.º, da CRP, ao mesmo tempo que restitui à reserva de processo penal a adequada eficácia na proibição contra ingerências em telecomunicações, ao serviço da defesa da privacidade e da autodeterminação comunicativa.

3. Sobre a necessidade de autorização judicial prévia para a realização de buscas e apreensões de documentos eletrónicos de empresas contendo mensagens fixados em dispositivos de armazenamento, o acórdão faz ver que essa exigência não consta da Lei Fundamental, nem se pode entender implícita a qualquer norma ou princípio constitucionais.

Também aqui, importa relembrar que as operações não importam a invasão em processos de comunicação intersubjetiva realizados através de sistemas de comunicação, seja o webmail, seja qualquer outro sistema de *messaging* (que, sem nenhuma dúvida, beneficiam da tutela do artigo 34.º,



249

TRIBUNAL CONSTITUCIONAL

n.º 4, da CRP, quando realizam trocas de informação através de fluxos de dados entre dispositivos). Importa também ver que as ações estão cingidas ao ambiente empresarial, não representando ingerência na esfera particular e íntima, espaço em que a defesa da privacidade é muito mais intenso (artigo 26.º, n.º 2 e 32.º, n.º 8, da CRP).

Nenhuma busca em instalações de empresa por autoridades públicas está subordinada a autorização judicial prévia no ordenamento português – sem que se conheça controvérsia a esse respeito ou sequer crítica fundada – e não existe qualquer fundamento válido que imponha outra solução no caso de processos por infrações à concorrência.

Por outro lado, o Regulamento (CE) n.º 1/2003 que, como se disse, conferiu à Comissão poderes para realizar buscas e apreensões de ficheiros informáticos contendo mensagens eletrónicas no âmbito de processos por infrações *antitrust* no espaço europeu, não estabelece a obrigatoriedade de autorização judicial prévia para a realização destas operações, bastando-se com o controlo ulterior pelo Tribunal de Justiça (cfr. artigos 20.º e 31.º). A interpretação da Lei Fundamental em conformidade com o Direito europeu e a eficácia direta do Regulamento na nossa ordem jurídica, pois, permitirá concluir que idêntica solução não está vedada ao Legislador português quanto aos meios de obtenção de prova da AdC.

De resto, o presente acórdão faz ver que o sistema português consagrado na norma sob fiscalização a este respeito *excede o standard* de garantias sobre esta matéria imposto pelo Direito europeu (CEDH e CDFUE): este reside na exigência de controlo jurisdicional *ex post facto*, ao passo que a Lei portuguesa estabelece um quadro de *duplo controlo judiciário* (Ministério Público, prévio à operação e controlo por Juiz, subsequente).

Em *IMI – Imagens Médicas Integradas, SA et al.* (reenvio prejudicial solicitado pelo Tribunal português) a Advogada-Geral junto do TJUE assinalou a consistência da jurisprudência europeia sobre esta matéria, suportando esta mesma conclusão:

"resulta da jurisprudência do TEDH que o direito fundamental à inviolabilidade do domicílio, como protegido pelo artigo 8.º da CEDH, não é violado, tratando-se das inspeções em instalações das sociedades, pela mera inexistência da autorização judicial prévia, um vez que são implementadas garantias adequadas e suficientes contra os abusos, nomeadamente uma fiscalização jurisdicional ex post completadas medidas em causa. O mesmo se aplica ao direito ao respeito pela correspondência, garantido por esse mesmo artigo, estando a questão da apreensão das comunicações das sociedades, na jurisprudência do TBJDH, estreitamente relacionada com as buscas efetuadas nas suas instalações. Encontram-se os mesmos princípios na jurisprudência do Tribunal de Justiça no que respeita ao artigo 7.º da Carta. Assim, no Acórdão WebMindLicenses, quanto à apreensão de mensagens de correio eletrónico no quadro de um processo penal, o Tribunal de Justiça afirmou que, não havendo autorização judicial prévia, a proteção dos indivíduos contra as infrações arbitrárias do poder público aos direitos garantidos por esse artigo exige um enquadramento legal e limites estritos dessa apreensão. Esclareceu, por um lado, que esta apreensão só é compatível com o referido artigo 7.º se a legislação e a prática internas oferecerem garantias adequadas e suficientes contra os abusos e a arbitrariedade"



TRIBUNAL CONSTITUCIONAL

e, por outro, que a não existência de um mandado judicial prévio pode, em certa medida, ser contrabalançada pela possibilidade de a pessoa visada na apreensão solicitar a posterior fiscalização jurisdicional quer da legalidade quer da necessidade desta, devendo essa fiscalização ser eficaz nas circunstâncias particulares do processo em causa.

Quanto, mais precisamente, aos poderes de verificação da Comissão, o Tribunal de Justiça já teve ocasião de esclarecer que o sistema implementado na União Europeia cumpre as exigências do artigo 8.º CEDH, como interpretado pelo TEDH, e do artigo 7.º da Carta, e que a inexistência de autorização judicial prévia não podia acarretar, enquanto tal, a ilegalidade de uma medida de inspeção decidida pela Comissão. O Tribunal de Justiça salientou, nomeadamente, que o artigo 20.º do Regulamento n.º 1/2003 prevê quer um enquadramento legal desses poderes quer limites estritos ao seu exercício e indica expressamente, no seu n.º 8, que o Tribunal de Justiça é competente para exercer uma fiscalização da legalidade da decisão de inspeção adotada pela Comissão, fiscalização que incide tanto sobre as questões de direito como sobre as questões de facto e que é, pois, completa.

Ora, o nível de proteção assegurado pelo artigo 7.º da Carta, como interpretado pelo Tribunal de Justiça, impõe-se claramente ao exercício dos poderes de busca e apreensão das autoridades nacionais da concorrência quando aplicam os artigos 101.º e 102.º TFUE.

Assim, (...) bá que concluir que o artigo 7.º da Carta não se opõe à legislação de um Estado-Membro ao abrigo da qual, no quadro de uma investigação sobre uma alegada violação do artigo 101.º TFUE ou do artigo 102.º TFUE, a autoridade nacional da concorrência pode proceder à busca e à apreensão de mensagens de correio eletrónico cujo conteúdo está relacionado com o objeto da inspeção sem dispor de uma autorização judicial prévia, desde que estejam previstos um enquadramento legal estrito dos poderes dessa autoridade e garantias adequadas e suficientes contra os abusos e a arbitrariedade, nomeadamente uma fiscalização judicial ex post completa das medidas em causa.”

Para além de todo o exposto, a Advogada-Geral neste mesmo processo assinala uma outra questão de grande importância a propósito da recente jurisprudência do TC (Acórdão do TC n.º 91/2023 e, mais recentemente, 314/2023, que remete para o primeiro).

A distensão do âmbito de tutela da autodeterminação comunicativa a ficheiros informáticos armazenados em dispositivos importou, para o Acórdão do TC n.º 91/2023, a obrigatoriedade de autorização judicial prévia a operações de busca e apreensão de ficheiros armazenados em dispositivos eletrónicos em empresas em processos por infrações à concorrência, excedendo as garantias conferidas a particulares pela CEDH e pela Carta.

A aplicabilidade desse nível reforçado de garantias em Direito interno não é, em princípio, incompatível com o Direito europeu, que reconhece a prevalência de estatutos mais garantísticos que aquele que resulta das suas fontes (cfr. artigo 53.º, *in fine*, da CDFUE). No entanto, se é lícito aos Estados reconhecerem maior estatuto defensivo, não lhes é permitido, por essa via, atingirem a eficácia do Direito europeu na jurisdição interna ou obstruírem a sua aplicabilidade, designadamente os princípios e normas de proteção da concorrência e de regulação do mercado europeu contidos nos artigos 101.º e 102.º do TFUE.

É neste plano que a jurisprudência introduzida pelo Acórdão do TC n.º 91/2023 gera uma segunda entorse na compatibilidade entre a CRP e o Direito europeu, já que significa a invalidação de uma peça central do quadro processual português de efetivação do Direito *antitrust* da União



TRIBUNAL CONSTITUCIONAL

Europeia, remontando de 2003 até à data presente, impedindo o enforcement do disposto nos artigos 101.º e 102.º do TFUE no território nacional e, por necessária deriva, ofendendo o princípio da efetividade do Direito da União na jurisdição portuguesa.

No sobreido processo, a Advogada-Geral junto do TJUE fez ver o seguinte:

"aplicação de padrões nacionais de proteção dos direitos fundamentais não deve comprometer o primado, a unidade e a efetividade do direito da União. A este respeito, o Tribunal de Justiça rejeitou qualquer interpretação do artigo 53.º da Carta segundo a qual este autoriza, em geral, um Estado-Membro a aplicar o nível mais elevado de proteção desses direitos garantido pela sua Constituição, e a opô-lo, se for caso disso, à aplicação de disposições do direito da União. A possibilidade de um Estado-Membro aplicar as suas próprias garantias constitucionais em matéria de buscas e apreensões no quadro das investigações por infrações aos artigos 101.º e 102.º TFUE, que asseguram um nível de proteção do direito fundamental ao respeito pela correspondência mais elevado do que o garantido pela Carta depende, portanto, nomeadamente, da questão de saber se essa aplicação pode prejudicar a eficácia da repressão das práticas anticoncorrenciais na União. A este propósito, recordo que o Tribunal de Justiça afirmou repetidamente que incumbe às autoridades de concorrência dos Estados-Membros e aos seus órgãos jurisdicionais aplicar os artigos 101.º e 102.º TFUE, quando os factos sejam abrangidos pelo âmbito de aplicação do direito da União, e garantir a sua aplicação efetiva no interesse geral.

(...) A AdC alega que a interpretação do Tribunal Constitucional não só põe em causa a possibilidade de utilizar enquanto meios de prova as mensagens de correio eletrónico apreendidas durante as buscas que são objeto dos processos principais, como arrisca também levar à invalidação das decisões definitivas de constatação da infração aos artigos 101.º e 102.º TFUE, devido à obtenção ilegal dos elementos probatórios em que esta autoridade se baseou, num período que cobre os últimos dez anos. Esta interpretação obsta, portanto, a uma aplicação efetivadas regras de concorrência da União.

(...) embora o estabelecimento e a aplicação destas regras [relativas às condições de obtenção das provas e à sua utilização nos processos administrativos nacionais de aplicação dos artigos 101.º e 102.º TFUE] sejam da competência dos Estados-Membros, estes devem exercer essa competência no respeito pelo direito da União e, em especial, pelo princípio da efetividade. Assim, não podem tornar impossível, na prática, ou excessivamente difícil a aplicação do direito da União e, especificamente, no domínio da concorrência, devem providenciar no sentido de que as regras que estabelecem ou aplicam não prejudiquem a aplicação efetiva dos artigos 101.º e 102.º TFUE, que as autoridades nacionais de concorrência são chamadas a assegurar no interesse geral.

Ora, no caso em apreço, por um lado, considero que incumbe ao órgão jurisdicional de reenvio, quando da apreciação das consequências a retirar dos Acórdãos de 2023, ter em conta a necessidade de assegurar uma aplicação efetiva das regras de concorrência da União, recorrendo a todas as possibilidades oferecidas pelo direito nacional — incluindo, sendo caso disso, a de sanar, em circunstâncias como as dos litígios nos processos principais, a inexistência de autorização judicial prévia através de uma fiscalização judicial a posteriori — para assegurar que o desrespeito dessas regras seja punido.

Por outro lado, a fim de dar plena execução aos artigos 101.º e 102.º TFUE, os tribunais portugueses podem ser levados a não aplicar uma regra nacional que reconhece à interpretação adotada nos Acórdãos de 2023 um efeito retroativo que tem como consequência pôr em causa a responsabilidade das empresas em questão em situações em que uma infração ao direito da concorrência da União foi definitivamente constatada pela AdC, gerando um risco sistémico de impunidade para tais infrações."

Impõe-se, portanto, convocar o referido princípio e observar o problema por esta perspetiva: o Direito interno não pode constituir um obstáculo à efetividade do Direito europeu na jurisdição nacional e a CRP não pode ser interpretada em sentido que represente a obstrução da vigência e efetividade prática do Direito da Concorrência em Portugal.

452
8

TRIBUNAL CONSTITUCIONAL

Pois bem, o presente Acórdão, à semelhança do Acórdão do TC n.º 91/2023 e da jurisprudência do TEDH e do TJUE citadas, sublinham o caráter crucial das medidas de busca e apreensão de documentos eletrónicos contendo mensagens no âmbito de infrações contra a concorrência, bem como a sua centralidade para a punição deste tipo de infrações. Será desnecessário, aqui, repisar essa evidência flagrante e coeva à natureza das coisas.

Porque alinhou a solução positivada com a doutrina e jurisprudência (Acórdãos do TC n.ºs 7/1987, 452/89, 67/97, 593/2008 e 596/2008), desde a introdução da Lei da Concorrência em 2003 e até à data presente, *unico* o Legislador nacional fez depender de prévia autorização judicial as operações de busca e apreensão de documentos informáticos armazenados em dispositivos eletrónicos em investigações em empresas por infrações aos artigos 101.º e 102.º do TFUE (e, antes, aos artigos 81.º e 82.º do TCE) (cfr. artigo 17.º, n.º 1, alínea c) e 2, da Lei n.º 18/2003, de 11 de junho; artigo 18.º, n.º 1, alínea c), do RJdC, nas redações conferidas pela Lei n.º 19/2012, de 8 de maio e da Lei n.º 17/2022, de 17 de agosto).

Por outro lado, nunca este Tribunal Constitucional sinalizou fricções desta solução com a Lei Fundamental, nem sequer quando foi chamado a pronunciar-se especificamente sobre esta matéria, muito pelo contrário (v. Acórdãos do TC n.ºs 593/2008 e 596/2008).

Pois bem, a pretensa inconstitucionalidade deste quadro legal de meios de obtenção de prova (por preterição de autorização judicial prévia em intrusão em telecomunicações) significará a impossibilidade de *enforcement* do disposto nos artigos 101.º e 102.º do TFUE na jurisdição portuguesa em todos os processos por infrações à concorrência pendentes, bem como, mais grave, suscita a *revisibilidade* das decisões transitadas em julgado há menos de cinco anos que hajam feito uso deste tipo de meios de prova (cfr. artigos 80.º e 81.º, n.º 1, alínea b), do RGCO e artigos 449.º, n.º 1, alínea e), e 126.º, n.º 3, ambos do CPP).

Considerando que estas decisões poderão remontar a infrações praticadas mais de cinco anos antes do respetivo trânsito em julgado (cfr. artigo 74.º, n.º 1, alínea b), do RJdC, contabilizando suspensões e interrupções do prazo prescricional), isto significa que existirá um arco temporal superior a *10 anos* (!) em que a violação da Lei *antitrust* europeia constante dos Tratados se considerará impassível de ações públicas punitivas em território nacional.

Por outras palavras, a jurisprudência do Acórdão do TC n.º 91/2023 é caracterizável como um processo hermenêutico que representa a *suspensão* da efetividade do Direito da concorrência europeu em território português por um período não inferior a dez anos.

Em face do exposto, também o princípio da efetividade do Direito da União Europeia na jurisdição nacional proíbe a aplicação do proposto *standard* de Direito interno (em excesso do

453
L



TRIBUNAL CONSTITUCIONAL

parâmetro da CDFUE), o que, associado aos princípios de primado e de unidade, conduz a que uma interpretação das normas constitucionais conforme com o Direito europeu em causa não conduza a exigir autorização judicial prévia para a realização de operações em empresas de busca e apreensão de ficheiros informáticos contendo mensagens em dispositivos eletrónicos no âmbito de processos por infrações à concorrência.

É precisamente esta a solução que se defende no presente acórdão, sem sacrifício ou compressão da defesa das telecomunicações, incluindo quanto a reserva de processo penal.

Assinado por: ANTÓNIO JOSÉ DA ASCENSÃO
RAMOS
Num. de Identificação: 04386182
Data: 2024.07.04 14:32:03+01'00'
Certificado por: Diário da República
Atributos certificados: Juiz Conselheiro - Tribunal
Constitucional
 CARTÃO DE CIDADÃO



454
a

TRIBUNAL CONSTITUCIONAL

Processo n.º 1104/2022

Pleno

DECLARAÇÃO DE VOTO *

30.07.2024
(Signature)

Vencido, por entender que a norma do artigo 18.º, n.º 1, alínea c), da Lei n.º 19/2012, de 8 de maio, que aprovou o Regime Jurídico da Concorrência (na redação original, anterior à conferida pela Lei n.º 17/2022, de 17 de agosto), no sentido indicado nos autos, é inconstitucional, por violação do artigo 34.º, n.º 4, da Constituição, pelas razões expressas pelo Conselheiro Afonso Patrão, em declaração de voto apostada ao mesmo Acórdão n.º 91/2023.

Assinado por: JOSÉ EDUARDO DE OLIVEIRA
FIGUEIREDO DIAS
Nº de identificação: 07762361
Data: 2024.07.04 16:12:18+01'00'



(Signature)

452
d.

TRIBUNAL CONSTITUCIONAL

Processo n.º 1104/22
2.ª secção

Declaração de voto

Vencida quanto à subalínea iii) da alínea a) e quanto à alínea b) do dispositivo do acórdão que fez vencimento, por considerar que a norma extraída da alínea c) do n.º 1 do artigo 18.º do Regime Jurídico da Concorrência (RJdC), na redação original, anterior à conferida pela Lei n.º 17/2022, de 17 de agosto, interpretada no sentido de “admitir o exame, recolha e apreensão de correio eletrónico em processo de contraordenação da concorrência sem despacho judicial prévio”, é inconstitucional, por violação do disposto nos artigos 32.º, n.º 4, e 34.º, n.ºs 1 e 4, este conjugado com o artigo 18.º, n.º 2, todos da Constituição da República Portuguesa (CRP).

Na sua essência, e em apertada síntese, o nosso dissenso reside em duas ordens de razões que temos, uma, como certa e, outra, como segura.

A primeira, que temos como certa, reside na consideração de que a Constituição, no artigo 34.º, n.º 4, ao limitar os possíveis casos de ingerência nas comunicações «à matéria de processo penabili», consagra uma reserva qualificada em matéria de restrição de direitos, liberdade e garantias, que pretende assegurar que o acesso a dados de comunicação apenas possa ser autorizado pelo legislador ordinário quando a medida que o concretiza participar da finalidade de defesa dos bens fundamentais da comunidade, e se mantiver, por via disso, dentro do critério de valor que caracteriza e singulariza o domínio da vida que justifica tal restrição. Por esse motivo, a conformidade constitucional de qualquer ingerência deste tipo, a ser levada a cabo em processos contraordenacionais, exigirá sempre um enquadramento legal específico e uma justificação robusta, não podendo deixar de se assegurar o respeito, no caso concreto, pela adequação, necessidade e proporcionalidade stricto sensu daquele meio de obtenção de prova, sob um juízo de ponderação de um juiz, como garantia da proteção dos direitos convocados, e que deverá ter em conta a gravidade das práticas anticoncorrenciais indiciadas, o peso das razões invocadas para justificar a ingerência nas mensagens de correio eletrónico e a indispensabilidade da diligência para a realização das finalidades que com ela se pretendem prosseguir.



TRIBUNAL CONSTITUCIONAL

456
g

A segunda, que temos como segura, reside no convencimento adquirido acerca da primeira, por via da inteira adesão à jurisprudência decorrente do Acórdão n.º 91/2023, muito em particular os fundamentos constantes dos parágrafos 17 e 18 (natureza das mensagens de correio eletrónico); 18.1 a 18.3 (irrelevância da distinção entre correio eletrónico lido e não lido para o âmbito de proteção contido do n.º 4 do artigo 34.º da CRP); 19 a 19.2 e 20 a 24 (âmbito material da exceção prevista no segmento final do n.º 4 do artigo 34.º da CRP); 25 e 26 (necessidade de intervenção prévia de um juiz; aqui se reafirmando, também, a jurisprudência que decorre do Acórdão n.º 687/2021, cujo sentido remonta, aliás, à Comissão Constitucional, designadamente, do Acórdão n.º 7/1987).

Sem prejuízo, enfatiza-se o seguinte: a compreensão do âmbito de incidência da exceção contida no segmento final do n.º 4 do artigo 34.º da Constituição, a que aqui aderimos, elimina o risco de que a opção pela criminalização de determinado comportamento — no caso, as práticas restritivas da concorrência — se fique verdadeiramente a dever, não à necessidade de pena, mas à essencialidade de assegurar o acesso a determinados meios de obtenção de prova, não disponíveis de outro modo e — o que é mais relevante ainda —, permite que a ordem jurídico-constitucional se realize por inteiro, enquanto sistema axiológico coerente e unitário, livre de aporias e de insanáveis contradições.

Por outro lado, as garantias asseguradas pela existência de um *processo penal ex ante* — e, mais do que isso, aquelas que são suscetíveis de o ser — resultam da verificação dos pressupostos legais que condicionam a admissibilidade do acesso aos meios probatórios em causa, ou seja, tipo de crime, moldura da pena aplicável e relevância ou indispensabilidade da ingerência do ponto de vista das finalidades que com ela se prosseguem, o que demanda a intervenção judicial e o juízo de ponderação que por via desta se convoca. Ora, entendemos nós que estas garantias são inteiramente transponíveis para o âmbito de aplicação da norma extraída da alínea c) do n.º 1 do artigo 18.º do RjdC, na redação original, anterior à conferida pela Lei n.º 17/2022, de 17 de agosto, no sentido de apenas admitir o exame, recolha e apreensão de correio eletrónico em processo de contraordenação da concorrência mediante despacho judicial prévio.

Assinado por: Dora Sofia Lucas Neto Gomes
Nº de identificação: 10153047
Data: 2024/07/11 12:38:33+01'00'
Certificado por: Diário da República
Atributos certificados: Juíza Conselheira - Tribunal Constitucional



TRIBUNAL CONSTITUCIONAL

Processo n.º 1104/2022

2.ª Secção

Relator: Conselheiro António José da Ascensão Ramos

DECLARAÇÃO DE VOTO

Vencida.

I. Subscrevo, convictamente, a rejeição que no presente Acórdão se faz da solução consagrada no Acórdão n.º 91/2023, nos termos da qual a CRP admitiria intromissões nas comunicações *em processos contraordenacionais*. Não é verdade que o faça, e o n.º 4 do artigo 34.º da Lei Fundamental estatui, aliás, uma *regra constitucional* bem explícita: “é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, *salvos os casos previstos na lei em matéria de processo criminal*.” Processo criminal e processo contraordenacional são, apesar dos elementos em comum, realidades substancialmente distintas, quer no plano do ordenamento constitucional, quer no plano da lei ordinária, e não é tarefa do juiz constitucional proceder a uma espécie de “interpretação corretiva”, em sentido inverso. Nestes termos, partilho, no essencial, da fundamentação do Acórdão até ao final do ponto 9., e é meu entender que o caminho interpretativo contrário tem consequências muitíssimo nefastas no que respeita à garantia da *força normativa da Constituição*.

II. Por outro lado, porém, afasto-me decisivamente da conclusão subscrita pelo Acórdão, a partir do ponto 10.2, segundo a qual as mensagens de correio eletrónico não configuram *comunicações*, para efeitos do respetivo regime de inviolabilidade. O arresto recorre a justificações técnicas, robustas, mas não convincentes, para retirar os e-mails do âmbito do conceito, entendido como *processo de transmissão de informação de uma pessoa para outra*. No que a este ponto diz respeito, atenho-me a toda a jurisprudência constitucional até ao momento, que sempre incluiu o correio

458
R



TRIBUNAL CONSTITUCIONAL

eletrónico no âmbito das comunicações, entendendo, além do mais, que se impõe, neste campo, uma certa evolução interpretativa, fruto da impossibilidade de distinção fiável entre mensagens abertas e fechadas, quando armazenadas em plataformas de arquivo remoto, e não no dispositivo físico usado pelos arguidos (vejam-se, em particular, os Acórdãos n.º 687/2021 e 91/2023). Mas, sobretudo, afasto-me da conclusão do Acórdão porque me parece impossível convencer, no tempo presente, uma sociedade aberta de intérpretes constitucionais, que inclui todos os cidadãos destinatários das normas em questão, que não constituem *comunicação* as mensagens de correio eletrónico acerca das quais não pode determinar-se que tenham chegado *definitivamente ao destinatário*.

III. Da conjunção das duas premissas anteriormente descritas resulta, pois, o meu claro e convicto juízo de inconstitucionalidade, no que respeita às normas questionadas. No atual quadro constitucional, e em situação de normalidade, não pode haver, *em caso algum*, ingerências por parte do Estado nas comunicações, no âmbito de um processo contraordenacional, com ou sem intervenção de um juiz. Como bem ensina REIS NOVAIS “*bá algumas garantias a que a própria Constituição atribui uma força normativa de natureza absoluta, definitiva, irrestringível; há direitos que o legislador constituinte retirou, desde logo, da possibilidade de posterior ponderação e eventual cedência*” (J. REIS NOVAIS, “Direitos Fundamentais e inconstitucionalidade em situação de crise – a propósito da epidemia COVID-19”, in *e-Pública*, Vol. 7, N.º 1, abril 2020, pg. 78-117).

A solução material subjacente a esta conclusão – segundo a qual se torna quase impossível a interceção de mensagens de correio eletrónico, em sede de processo contraordenacional - pode revelar-se desadequada da realidade de 2024. Essa é uma possibilidade, como é também possível que o concreto desenho constitucional da proteção conferida à esfera das comunicações já não corresponda, sequer, ao desejo maioritário dos cidadãos portugueses. Não cabe, porém, aos juízes constitucionais alterar, por via interpretativa, as específicas e expressas soluções de concordância prática entre bens constitucionais em conflito, que o legislador constituinte entendeu plasmar sob a forma de *regra constitucional*. A opção de conferir diferentes níveis de tutela a direitos fundamentais reconduzíveis aos mesmos valores, ou aos mesmos bens jurídico-constitucionais, é uma prerrogativa sua. Tais diferenças garantísticas corresponderão, certamente, ao equilíbrio possível para determinados dissensos, lidos no contexto de cada momento histórico, e devem ser acatadas pelo poder jurisdicional. Cabe, pois, ao órgão legislativo, mediante a assunção de poder

459
ex



TRIBUNAL CONSTITUCIONAL

constituente, evitar um fosso entre as normas da Constituição e a realidade da vida - devido a certas contingências históricas e da normal, e natural, evolução social, tecnológica, política e constitucional - de tal forma profundo que conduza ao desgaste da primeira. Assim, sendo minha convicção firme que a Constituição é um instrumento *vivo*, que evolui e pode ser objeto de diferentes leituras, de acordo com o tempo e o modo em que cada intérprete é chamado a atuar, creio que o juiz constitucional não pode deixar de reconhecer, em regras constitucionais como as que se plasmam nas normas questionadas, o *limite* do exercício da sua função. A resolução das disfunções que daqui possam resultar é, pois, tarefa exclusiva do legislador.

Maria da Cunha
Mariana Rodrigues Canotilho



460
X

TRIBUNAL CONSTITUCIONAL

Processo n.º 1104/2022

2.ª Secção

Declaração de Voto

Vencido quanto ao juízo de não constitucionalidade do disposto no artigo 18.º, n.º 1, alínea q), da Lei n.º 19/2012, de 8 de maio (na redação original, anterior à conferida pela Lei n.º 17/2022, de 17 de agosto), interpretado no sentido de se «admitir o exame, recolha e apreensão de mensagens de correio eletrónico em processo de contraordenação da concorrência sem despacho judicial prévio», remetendo para a fundamentação do Acórdão n.º 91/2023, da 3.ª Secção, que subscrevi sem reservas, e para a do Acórdão n.º 314/2023, da 1.ª Secção, que para aquele remeteu.

Sendo praticamente certa a interposição, pela recorrente, de recurso para o plenário, ao abrigo do n.º 1 do artigo 79.º-D da Lei do Tribunal Constitucional, dispenso-me, nesta ocasião, de ensaiar a refutação dos argumentos que constam do presente aresto, designadamente aqueles através dos quais se procura impugnar a fundamentação do Acórdão n.º 91/2023, evitando, deste modo, acrescentar complexidade a uma decisão já de si muito complexa.

Como presidente da 2.ª Secção não devo, porém, omitir uma palavra de explicação sobre uma circunstância processual que suponho ser incompreensível para quem não se encontre profundamente familiarizado com o nosso sistema de justiça constitucional: a aprovação de um julgamento de não constitucionalidade por um colégio de 5 juízes dos quais 4 estão vencidos por entenderem que alguma das três dimensões normativas sindicadas é constitucional – em suma, o facto de ter sido aprovado um acórdão que exprime a posição de um único juiz, o conselheiro relator.

Pois bem, usando da maior parcimónia de palavras e argumentos, basta dizer que tal se deve ao facto de não haver *uma maioria de juízes* que considere alguma das normas em que se decompõe o objeto do recurso constitucional. Acresce o facto de que, para julgar uma norma constitucional, tem de se verificar uma maioria, quer de votos no sentido da constitucionalidade, quer de *fundamentação* de tal juízo. Assim é porque, no nosso sistema, não há juízos positivos de constitucionalidade – como seria o caso se o Tribunal Constitucional julgassem



461

TRIBUNAL CONSTITUCIONAL

normas «constitucionalmente conformes» –, mas apenas juízos positivos e negativos de *inconstitucionalidade*.

Ora, há uma assimetria entre estes, uma vez que, para se fundamentar o juízo positivo de inconstitucionalidade, indispensável é, em virtude do dever de fundamentação das decisões judiciais, que se invoque uma razão imputável ao colégio, apurada segundo a regra da maioria. Ao passo que para se fundamentar um juízo de não inconstitucionalidade – o juízo, quer isto dizer, de que certa norma *não é inconstitucional* –, basta que o colégio não tenha razão suficiente, apurada segundo a regra da maioria, para a julgar inconstitucional.

Esta assimetria é uma forma de obviar a decisões de *non liquet*, geralmente tomadas como inaceitáveis, prevenindo precisamente aquelas hipóteses em que o colégio não tem razão suficiente, apurada segundo a regra da maioria, para um juízo positivo, ou seja, para julgar a conformidade ou desconformidade constitucional de certa norma. O juízo negativo de inconstitucionalidade – «não julgar inconstitucional...» – opera, pois, como uma decisão por defeito ou omissão, que exclui logicamente o impasse deliberativo.

No presente recurso, se é certo que os quatro votos de vencido convergem no sentido de que alguma das dimensões normativas sindicadas é inconstitucional, todos ademais invocando o n.º 4 do artigo 34.º da Constituição, e ainda que os que entendem que a primeira ou a segunda dimensões são inconstitucionais não estão inibidos, nem desonerados, de se pronunciar sobre a inconstitucionalidade da terceira, a distância de razões é de tal modo expressiva que não é possível convergir numa fundamentação com aquele mínimo de coerência e rigor que o respetivo dever impõe.

O *sentido objetivo* do presente aresto não é, assim, o de que o colégio julgou o objeto do recurso constitucionalmente conforme – esse é o *sentido subjetivo* do mesmo, correspondente ao pensamento do relator expresso na fundamentação –, mas, como é da natureza do nosso sistema e resulta do próprio teor do dispositivo, o de que o colégio não proferiu nenhum juízo de inconstitucionalidade, por não possuir razão própria e suficiente para tanto.

Assinado por: Gonçalo Manoel de Vilhena de
Almeida Ribeiro
Num. de identificação: 8112362262
Data: 2024.07.10 12:48:19+01'00'



CHAVE MÓVEL
• • •