# TRIBUNAL CONSTITUCIONAL

## Acórdão do Tribunal Constitucional n.º 464/2019

*Sumário:* Declara a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 3.º da Lei Orgânica n.º 4/2017, de 25 de agosto, na parte em que admite o acesso dos oficiais de informações do Serviço de Informações de Segurança (SIS) e do Serviço de Informações Estratégicas e de Defesa (SIED), relativamente a dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação, para efeitos de produção de informações necessárias à salvaguarda da defesa nacional e da segurança interna, por violação dos artigos 26.º, n.º 1, e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2, da Constituição da República Portuguesa; não declara a inconstitucionalidade da norma constante do artigo 3.º da Lei Orgânica n.º 4/2017, de 25 de agosto, na parte em que admite o acesso dos oficiais de informações destes serviços no âmbito das respetivas atribuições, relativamente a dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação, para efeitos de produção de informações necessárias à prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada; declara a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4.º da Lei Orgânica n.º 4/2017, de 25 de agosto, por violação do disposto no artigo 34.º, n.º 4, da Constituição, no que diz respeito ao acesso aos dados de tráfego que envolvem comunicação intersubjetiva, e por violação do disposto nos artigos 26.º, n.º 1, e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2, todos da Constituição, no que se refere ao acesso a dados de tráfego que não envolvem comunicação intersubjetiva

**Processo n.º 26 2018**

Acordam no Plenário do Tribunal Constitucional

### I — Relatório

1 — Trinta e cinco Deputados à Assembleia da República, ao abrigo do disposto na alínea *a*) do n.º 1 e na alínea *f*) do n.º 2 do artigo 281.º da Constituição da República Portuguesa, pediram a apreciação e declaração da inconstitucionalidade das normas constantes dos artigos 3.º e 4.º da Lei Orgânica n.º 4/2017, de 25 de agosto, que aprova e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança (SIS) e do Serviço de Informações Estratégicas de Defesa (SIED) e procede à segunda alteração à Lei n.º 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário).

2 — As normas questionadas têm o seguinte teor:

*Artigo 3.º*

***Acesso a dados de base e de localização de equipamento***

*Os oficiais de informações do SIS e do SIED podem ter acesso a dados de base e de localização de equipamento para efeitos de produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada e no seu exclusivo âmbito.*

*Artigo 4.º*

***Acesso a dados de tráfego***

*Os oficiais de informações do SIS e do SIED apenas podem ter acesso a dados de tráfego para efeitos de produção de informações necessárias à prevenção de atos de espionagem e do terrorismo.*

3 — Para impugnar a constitucionalidade das normas acima indicadas, os requerentes invocam a violação do n.º 4 do artigo 34.º da Constituição.

Os fundamentos do pedido são, em síntese, os seguintes:

«A questão relevante a apreciar é a de saber quais os tipos de dados que se encontram sob a proteção estabelecida no n.º 4 do artigo 34.º da Constituição que dispõe expressamente que "é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo criminal."

A resposta dada pelo TC, no Acórdão n.º 403/2015, à questão de saber se os dados de tráfego, incluindo os dados de localização, se encontram no âmbito da proteção do n.º 4 do artigo 34.º da Constituição, não podia ser mais clara.

Aí se afirma (p. 16) que "há um largo consenso na doutrina e na jurisprudência, de resto não se conhece posição contrária, no sentido de se incluir os dados de tráfego no conceito de comunicações constitucionalmente relevante para a proibição de ingerência".

E depois de uma ampla explanação doutrinal e jurisprudencial, o TC conclui que "a área de proteção do sigilo das comunicações consagrada no n.º 4 do artigo 34.º da CRP, compreende tanto o conteúdo da comunicação como os dados de tráfego atinentes ao processo de comunicação".

Assente a questão dos dados protegidos pelo sigilo das comunicações, importa saber se o acesso a dados de tráfego previsto nos artigos 3.º e 4.º da LO por parte de oficiais de informações se conforma com a exceção constante da segunda parte do n.º 4 do artigo 34.º da CRP que permite o acesso a dados dessa natureza nos casos previstos na lei em matéria de processo criminal.

O Acórdão n.º 403/2015 do TC também analisa extensamente esse ponto para concluir que "ao autorizar a ingerência das autoridades públicas nos meios de comunicação apenas em matéria de processo penal, e não para quaisquer outros efeitos, a Constituição quis garantir que o acesso a esses meios, para salvaguarda dos valores da justiça e da segurança, fosse efetuado através de um instrumento processual que também proteja os direitos fundamentais das pessoas". E prossegue: "porque a ingerência nas comunicações põe em conflito um direito fundamental com outros direitos ou valores comunitários, considerou-se que a restrição daquele direito só seria autorizada para a realização dos valores da justiça, da descoberta da verdade material e restabelecimento da paz jurídica comunitária, os valores que ao processo penal incumbe realizar".

Mas o citado Acórdão vai mais longe, ao referir que o n.º 4 do artigo 34.º da CRP tem consequências que se refletem no estatuto constitucional do arguido (artigo 32.º n.º 8 da CRP) e que conduzem à consideração da nulidade de provas obtidas por ingerência abusiva nas comunicações.

Por outro lado, conclui ainda o citado Acórdão, que "no caso da ingerência das autoridades públicas nas comunicações, que o artigo 34.º, n.º 4, primeira parte, consagra como princípio geral, as exceções a que se refere o segmento final desse preceito estão condicionadas à matéria de processo penal, e sendo a restrição constitucionalmente autorizada apenas nesses termos, não tem cabimento efetuar uma qualquer outra interpretação que permita alargar a restrição a outros efeitos, como se a restrição não estivesse especificada no próprio texto constitucional ou se tratasse aí de uma restrição meramente implícita que permitisse atender a outros valores ou bens constitucionalmente reconhecidos".

Existe aliás, como é referido, uma abundante jurisprudência constitucional nesse sentido (Acórdãos n.ºs 241/02, 195/85, 407/97, 70/2008, 486/2009 e 699/2013).

O TC considera, pois, que, fora do processo penal, vigora uma proibição absoluta de ingerência das autoridades públicas nos meios de comunicação, incluindo em matéria de dados de tráfego.

Assim sendo, importa então saber se o acesso de oficiais de informações a dados de tráfego, incluindo os dados de localização, se pode considerar como uma atividade "em matéria de processo criminal".

A resposta do TC é "seguramente" negativa, porquanto "os fins e interesses que a lei incumbe ao SIRP de prosseguir, os poderes funcionais que confere ao seu pessoal e os procedimentos de atuação e de controlo que estabelece, colocam o acesso aos dados de tráfego fora do âmbito da investigação criminal".

O que dispõe o artigo 3.º da LO é que os oficiais de informações do SIS e do SIED podem ter acesso a dados de base e de localização de equipamento para efeitos de produção de informações

necessárias à salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada e no seu exclusivo âmbito.

E o artigo 4.º dispõe que os oficiais de informações do SIS e do SIED podem ter acesso a dados de tráfego para efeitos de produção de informações necessárias à prevenção de atos de espionagem e do terrorismo.

Estamos assim no domínio da recolha de informações para efeitos de prevenção, o que no entendimento do TC "se dissocia, de forma clara e precisa, da atividade própria da investigação criminal" (Acórdão cit., p. 23).

Nos termos da Lei n.º 49/2008, de 27 de agosto, a investigação criminal "compreende o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito de processo".

Na verdade, os serviços de informações não possuem quaisquer atribuições policiais ou de investigação criminal, estando-lhes legalmente vedadas tais atividades.

Há, pois, (é o entendimento do TC) "uma distinção radical entre informações e investigação criminal, o que impede os oficiais de informações de intervirem no processo penal".

Ainda que a recolha de informações possa ser utilizada no processo penal, a recolha para esse fim tem que se dirigir a um crime já praticado. Ora, a recolha de informações pela SIRP, porque preventiva, não se orienta para uma atividade investigatória de crimes já praticados ou em execução.

A conclusão perentória do TC é que a atividade de informações produzida pelo SIRP, porque não se dirige à descoberta da autoria de um crime, não reveste a natureza de investigação criminal. (...) São, pois, procedimentos administrativos que, devendo respeitar os direitos, liberdades e garantias, não obedecem aos princípios jurídico-constitucionais conformadores do processo penal (Acórdão cito P. 24).

*Da relevância da natureza da entidade de controlo*

Diferentemente do que acontecia com o Decreto da AR sob o qual incidiu o processo de fiscalização preventiva da constitucionalidade que culminou no Acórdão n.º 403/2015, não se prevê na LO em apreço que o controlo do acesso aos dados de tráfego seja feito por via de uma "comissão de controlo prévio" de natureza administrativa, e como tal qualificada no referido acórdão, apesar de integrada por magistrados judiciais.

No caso presente, nos termos do artigo 8.º da LO, o controlo judicial e a autorização prévia do acesso dos oficiais de informações do SIS e do SIED a dados de telecomunicações e Internet são efetuados por uma formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções.

A intensidade do controlo do acesso aos dados de tráfego por parte dos oficiais de informações é também consideravelmente superior à que se previa no decreto julgado inconstitucional em 2015, de modo a conferir garantias de necessidade, adequação e proporcionalidade ao pedido efetuado.

Todavia, entendem os requerentes que as alterações assim efetuadas não afastam as decisivas razões que levaram à declaração de inconstitucionalidade do Decreto n.º 426/XII.

Se é certo que as secções criminais do Supremo Tribunal de Justiça não podem ser qualificadas como órgãos administrativos, sendo este Tribunal inequivocamente um órgão de natureza jurisdicional, não é menos certo que as funções que a LO lhes atribui — em tudo estranhas às funções que até agora este Tribunal foi chamado legalmente a desempenhar — não constituem matéria de processo criminal.

Assim como no Acórdão n.º 241/02 o TC julgou inconstitucional que, em processo laboral, pudesse ser pedido por despacho judicial aos operadores de telecomunicações informações relativas aos dados de tráfego e à faturação detalhada de linha telefónica, por "não constituir matéria de processo criminal", sendo tal entendimento confirmado em acórdãos posteriores (citados no Acórdão n.º 403/2015, p. 22) designadamente no âmbito do processo civil, também agora é forçoso concluir pela inconstitucionalidade do disposto na LO.

É que o que está em causa não é tanto a natureza administrativa ou judicial da entidade de controlo (embora tal natureza não seja irrelevante) mas a questão de saber se o controlo judicial efetuado se insere, ou não, no âmbito do processo penal.

E pelas razões acima expendidas à luz da jurisprudência constitucional, sobre a distinção radical entre informações e investigação criminal, que impede os oficiais de informações de intervirem no processo penal, parece aos proponentes que a resposta só pode ser negativa».

4 — Notificado para responder, o Presidente da Assembleia da República veio oferecer o merecimento dos autos, aproveitando, no entanto, para explicar, em síntese, o seguinte:

«1 — Breve enquadramento legal

A Lei Orgânica n.º 4/2017, de 25 de agosto, veio aprovar e regular o procedimento especial de acesso a dados de telecomunicações e Internet, previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, por parte dos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa.

A Lei sujeita a controlo judicial a possibilidade de acesso aos dados que se mostrem necessários para a prossecução da atividade de produção de informações pelo Sistema de Informações da República Portuguesa (SIRP) relacionados com a segurança interna, a defesa, a segurança do Estado e a prevenção da espionagem e do terrorismo.

A matéria do acesso pelos Serviços de Informações da República Portuguesa aos dados de telecomunicações e Internet já fora objeto de aprovação parlamentar, tendo o decreto então aprovado — Decreto n.º 426/XII da Assembleia da República (com origem na Proposta de Lei n.º 345/XIV4.ª — Aprova o regime do Sistema de Informações da República Portuguesa) — sido objeto de fiscalização preventiva da constitucionalidade, que culminou na pronúncia do Tribunal Constitucional pela inconstitucionalidade da norma do n.º 2 do seu artigo 78.º, por violação do disposto no n.º 4 do artigo 34.º da CRP, através do Acórdão n.º 403/2015, de 27 de agosto. Este decreto foi objeto de veto no seguimento da referida pronúncia do Tribunal Constitucional.

2 — Trabalhos preparatórios da Lei Orgânica n.º 4/2017

A Lei Orgânica n.º 4/2017, de 25 de agosto, que Aprova e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa e procede à segunda alteração à Lei n.º 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário) teve origem na Proposta de Lei n.º 79/XIII/2.ª, da iniciativa do Governo — "Aprova o regime especial de acesso a dados de base e a dados de tráfego de comunicações eletrónicas pelo SIRP" e no Projeto de Lei n.º 480/XIII/2.ª, da iniciativa dos dezoito Deputados do Grupo Parlamentar do CDS/PP — "Acesso a dados de tráfego, de localização ou outros dados conexos das comunicações por funcionários e agentes dos serviços de informações da República Portuguesa".

As normas objeto do pedido de declaração de inconstitucionalidade com força obrigatória geral — os artigos 3.º (Acesso a dados de base e de localização de equipamento) e 4.º (Acesso a dados de tráfego) da referida Lei Orgânica — correspondem, na sua redação, respetivamente aos artigos 2.º e 3.º da Proposta de Lei n.º 79/XIII. Estas normas não foram objeto de quaisquer propostas de alteração no decurso do processo legislativo que deu origem à Lei, salvo no que respeita à sua numeração (em resultado do aperfeiçoamento operado em redação final, aprovada pela I.ª Comissão em 27 de julho de 2017, que consistiu no desdobramento do artigo 1.º em dois artigos — 1.º e 2.º — com consequente remuneração dos seguintes).

Dos trabalhos preparatórios da Lei Orgânica, — todos os elementos de tramitação da Proposta de Lei n.º 79/XIII e do Projeto de Lei n.º 480/XIII disponíveis na base de dados "Atividade parlamentar" constante do site do Parlamento na Internet, na hiperligação http://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID= 41364) — é possível retirar, com relevância para a questão objeto do presente pedido de fiscalização, que:

1 — Na exposição de motivos da Proposta de Lei n.º 79/XIII, o proponente explicitava que o regime especial de acesso a dados preconizado se revelava adequado e proporcional «aos desafios colocados à segurança nacional e internacional do Estado, considerando os procedimentos e metodologias previstos em regimes jurídicos congéneres, particularmente no espaço europeu (...)»,

e atendendo, ainda, ao regime estabelecido na Estratégia Nacional de Combate ao terrorismo, aprovada pela Resolução do Conselho de Ministros n.º 7-A/2015, de 20 de fevereiro».

A iniciativa previa que a atividade de recolha de informação pelos funcionários do SIRP para efeitos de prevenção fosse precedida de um procedimento de autorização obrigatória da responsabilidade de uma formação das secções criminais do Supremo Tribunal de Justiça, comunicado ao Procurador-Geral da República, estando os dados de telecomunicações e Internet obtidos — dados de base, de localização e de tráfego — sujeitos à fiscalização da Comissão de Fiscalização de Dados do SIRP e do Conselho de Fiscalização do SIRP, «ficando assim...» — nas palavras do proponente — «... acautelados os limites e os níveis cumulativos de fiscalização interna e externa do sistema, bem como as restrições constitucionais em matéria de privacidade e garantias fundamentais».

2 — Uma vez que o proponente Governo solicitou o agendamento da discussão na generalidade da iniciativa — que dera entrada na Mesa da Assembleia da República em 11 de maio de 2017 e fora admitida no subsequente dia 16 de maio — para a sessão Plenária de 17 de maio, por arrastamento com um conjunto de iniciativas sobre matéria idêntica (designadamente o Projeto de Lei n.º 480/XIII), a Proposta de Lei não baixou, na fase de generalidade, à comissão competente, pelo que a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias sobre ela não emitiu parecer, muito embora tenha subsequentemente sido objeto de nota técnica.

Não existe assim, para além deste documento técnico (com pertinência possível na parte relativa ao enquadramento legal internacional e ao tratamento da matéria no plano do Direito da União Europeia), nenhum outro elemento de apreciação — parecer ou ata de reunião em que tivesse sido discutido — suscetível de relevar para a análise do pedido.

3 — Objeto de parecer da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, fora, na reunião de 10 de maio de 2017, o Projeto de Lei n.º 480/XIII, que visava alterar a Lei n.º 30/84, de 5 de setembro (Lei Quadro do Sistema de Informações da República Portuguesa) e a Lei n.º 62/2013, de 26 de agosto (Lei de Organização do Sistema Judiciário), estabelecendo a competência e o procedimento de acesso por parte dos funcionários e agentes dos serviços de informações da República Portuguesa, mediante autorização judicial prévia a cargo de uma secção especial para autorização de acesso a informação e a dados (de tráfego, de localização ou outros dados conexos das comunicações), que propunha criar no Supremo Tribunal de Justiça.

Na exposição de motivos, os proponentes consideravam «essencial dotar o país de todos os mecanismos ao seu alcance para» evitar o terrorismo, devendo ser trabalhada a sua «prevenção e repressão».

Propunha esta iniciativa a sujeição do acesso aos dados a autorização judicial «com audição prévia da Comissão Nacional de Proteção de Dados, no quadro das suas competências próprias» (cf. n.º 1 do artigo 5.º). Previa a mesma iniciativa a criação de uma «secção especial para autorização de acesso a informações e a dados», «constituída por três juízes da secção penal do Supremo Tribunal de Justiça, anual e sucessivamente designados, cabendo a um juiz as funções de relator e aos outros juízes as funções de adjuntos», tal como a atribuição ao Procurador-Geral da República da incumbência de designação anual de «um procurador-geral-adjunto junto da secção especial para autorização de acesso a informação e a dados».

O parecer (e a nota técnica que o acompanha) dão conta de que a iniciativa preconizava a adoção de «regras sobre a forma de transmissão dos dados, estabelecendo a transferência eletrónica encriptada ou codificada como regra, à semelhança do que sucede na Lei n.º 32/2008, de 17 de julho, para a transmissão de dados de tráfego e dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador». Recorde-se que a Lei n.º 32/2008 transpusera para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

A justificação do impulso legislativo residia ainda, segundo o proponente, na Estratégia Nacional de Combate ao Terrorismo, aprovada pela Resolução do Conselho de Ministros n.º 7-A/2015, de 20 de fevereiro, bem como na «prevenção de ameaças à segurança nacional e europeia em matéria de terrorismo», necessidade sublinhada, segundo os autores da iniciativa, pelo Conselho

de Fiscalização do Sistema de Informações da República Portuguesa, tanto no parecer relativo ao ano de 2015, como no respeitante ao primeiro semestre de 2016.

A nota técnica assinalava que com a Lei n.º 30/84, de 5 de setembro (Lei Quadro do Sistema de Informações da República Portuguesa), alterada pelas Leis n.º 4/95, de 21 de fevereiro, n.º 15/96, de 30 de abril, n.º 75-A/97, de 22 de julho, e pela Lei Orgânica n.º 4/2004, de 6 de novembro, que a republicou (incluindo a Declaração de Retificação n.º 44-A/20 14, de 10 de outubro), se haviam estabelecido as bases gerais das informações em Portugal e a definição das regras de funcionamento, direção e controlo dos respetivos órgãos, definindo-se estruturas de fiscalização. A Lei precisava também as missões, deveres e responsabilidades dos serviços e das entidades fiscalizadoras. O SIRP tinha como missão fundamental «a produção de informações necessárias à salvaguarda da independência nacional e à garantia da segurança interna» (artigo 2.º, n.º 2), para o que dispunha de três serviços de informações: o Serviço de Informações Estratégicas de Defesa (SIED), o Serviço de Informações Militares (SIM) e o Serviço de Informações e Segurança (SIS).

A Lei Orgânica n.º 4/2004, de 6 de novembro, introduziu relevantes alterações ao regime do Sistema de Informações, colocando os dois serviços de informações na dependência direta do Primeiro-Ministro e criando o cargo de Secretário-Geral do SIRP, que ficou incumbido de coordenar e conduzir superiormente a atividade dos serviços de informações. O SIEDM perdeu a componente militar e voltou a designar-se SIED (Serviço de Informações Estratégicas de Defesa).

Recorda o mesmo documento que a atividade do SIRP está "especificamente limitada por alguns princípios inscritos nos n.os 1 e 3 do artigo 3.º e n.º 1 do artigo 4.º da Lei Quadro do SIRP: (i) o princípio da constitucionalidade e da legalidade: a atividade dos serviços de informações está sujeita ao escrupuloso respeito pela Constituição e pela lei, designadamente em matéria de proteção dos direitos fundamentais das pessoas, especialmente frente à utilização de dados informatizados; (ii) o princípio da exclusividade: a atividade dos serviços está rigorosamente limitada às suas atribuições, não podendo desenvolver uma atividade de produção de informações em domínio que não lhe tenha sido concedido; (iii) o princípio da especialidade: a atividade dos serviços de informações reduz-se ao seu estrito âmbito, não podendo a sua atividade confundir-se com a atividade própria de outros organismos, como no domínio da atividade dos tribunais ou da atividade policial."

A nota técnica evocava também o que ficara consignado na nota da referida Proposta de Lei n.º 345/XII/4, no sentido de que "os dados (cujo acesso pelo SIRP se estabelece) podem, eventualmente, ser considerados 'dados pessoais' para os efeitos do disposto no artigo 35.º da CRP, artigo que estabelece, no n.º 4, uma proibição genérica do acesso a dados pessoais de terceiros, salvo casos excecionalmente previstos na lei. A estes casos excecionais deve ser aplicado o regime das restrições aos direitos, liberdades e garantias do art. 18.º da CRP, pelo que, de acordo com Gomes Canotilho e Vital Moreira, «só podem ter lugar quando exigidas pela necessidade de defesa de direitos ou bens constitucionalmente protegidos (defesa da existência do Estado, combate à criminalidade, proteção dos direitos fundamentais de outrem, etc.)» (in *Constituição da República Portuguesa Anotada,* Volume I 4.ª Edição revista, pág. 555)». A este propósito, poderá ainda referir-se o n.º 4 do artigo 34.º da CRP, que proíbe toda a «ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo criminal».

A nota faz, por fim, apelo ao acórdão do Tribunal Constitucional n.º 403/2015, de 27 de agosto, que "sublinha a necessidade de «caracterizar o tipo de dados em causa e saber se o acesso aos mesmos é merecedor de proteção constitucional». Recorda que o ordenamento jurídico providencia uma definição legal de «dados de tráfego» (designação utilizada no projeto de lei) — contida na alínea *d*) do n.º 1 do artigo 2.º da Lei n.º 41/2004, de 18 de agosto, sobre Segurança nas Telecomunicações —, que faz corresponder a «quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma». A este propósito, o acórdão em causa convoca a jurisprudência do mesmo Tribunal Constitucional, que acolheu uma classificação tripartida dos dados resultantes do serviço de telecomunicações: «(...) os dados relativos à conexão à rede, ditos dados de base; os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação; e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência), dados de tráfego; dados relativos ao conteúdo da comunicação

ou da mensagem, dados de conteúdo». Atenta esta distinção, o mesmo acórdão considera que os «dados de tráfego», «dados de localização» ou outros «dados conexos» das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, data, hora, duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização, devem ser considerados como dados de tráfego, «por respeitarem aos próprios elementos funcionais da comunicação, reportando-se à direção, destino, via e trajeto de uma determinada mensagem. São dados, pois, que identificam ou permitem identificar a comunicação e, uma vez conservados, possibilitam a identificação das comunicações entre emitente e destinatário, a data, o tempo e a frequência das ligações efetuadas Aludindo à regulamentação legal existente sobre acesso a dados relativos a comunicações, a mesma nota lembra que o tratamento de dados pessoais obedece às condições estabelecidas na Lei n.º 67/98, de 26 de outubro, que, transpondo para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados, aprovou a Lei de Proteção de Dados Pessoais.

Do enquadramento da matéria no plano do Direito da União Europeia, destaca-se a menção, feita na referida nota, à Decisão-Quadro 2008/977/JAI do Conselho, de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação judicial e da justiça penal, que abrange apenas os dados policiais e judiciários trocados entre os Estados-Membros, as autoridades e os sistemas associados da União Europeia e não abrange os dados nacionais, e que será revogada (em maio de 2018) pela Diretiva (UE) 2016/680, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. A diretiva visa proteger os dados pessoais das pessoas singulares tratados pelas autoridades policiais e judiciárias, do mesmo passo que visa melhorar a cooperação no combate ao terrorismo e à criminalidade transfronteiras na UE permitindo às autoridades policiais e judiciárias dos países da UE trocarem informações necessárias para que as investigações sejam mais eficazes e mais eficientes.

O enquadramento internacional do tema apresenta elementos de análise relativos à Alemanha, Espanha, França e Reino Unido, dando nota da possibilidade e condições de interceção de comunicações por partes dos Serviços de Informações de alguns daqueles Estados — aludindo, na Alemanha, à Comissão G-I O, composta por quatro membros (não necessariamente membros do Bundestag), presidida por um juiz e que tem como missão "implementar medidas de fiscalização restritivas no campo da correspondência, mensagens e sigilo de telecomunicações (GG artigo 10), sendo responsável pela autorização de pedidos de interceção de comunicações. O seu poder de controlo também se estende a todo o processo de recolha, processamento e utilização de informações pessoais obtido a partir dessa ação"; em Espanha, "ao acesso a informação pelos serviços de informações (..) o artigo 15 da Ley 5/2014, de 4 de abril, de Seguridad Privada, que admite esta possibilidade, nomeadamente quanto àqueles serviços poderem solicitar às empresas privadas de segurança que lhes concedam acesso aos sistemas de vigilância eletrónica de sinais quando necessário. Tal deve ser feito para evitar um perigo real para a segurança pública ou para efeitos de investigação criminal, devendo sempre respeitar as disposições da lei relativa à proteção de dados"; referindo-se, relativamente a França, "às técnicas de interceção de informação em matéria de segurança", relativamente a cuja regulamentação elenca "a Loi récente n.º 2015-912 du 24 juillet 2015 (..) aprovada com o propósito de aumentar as taxas de detenção no âmbito da ameaça terrorista, pretendeu atualizar o regime do segredo da correspondência transmitida por via das telecomunicações, regulada pela Loi n.º 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications. Aquela lei repesca as disposições existentes sobre interceções de segurança e acesso aos dados de conexão, e transpõe para o campo da prevenção técnicas de recolha de informação já permitidas num contexto judicial (como a captação de imagens em locais privados e a recolha de dados informáticos).

De acordo com a Lei n.º 91-646, são autorizadas as interceções de comunicações emitidas por via eletrónica (v.g. escutas telefónicas) que tenham por fim procurar informações relacionadas com

a segurança nacional, a salvaguarda dos elementos essenciais do potencial científico e económico da França, ou a prevenção do terrorismo, criminalidade e delinquência organizada.

Em termos de procedimento, cabe ao primeiro-ministro, com base num pedido escrito e fundamentado de um dos ministérios responsáveis pelos seis serviços de informações, conceder a autorização para executar, por exemplo, uma escuta telefónica, depois de consultada a Commission nationale de contrôle des interceptions de sécurité (CNCIS).

A Lei n.º 2015-912 de 24 de julho de 2015 altera este regime, prevendo que a autorização seja estendida às pessoas da entourage da pessoa visada (artigo 852-1 código de segurança interna), substituindo-se o CNCIS pela Commission nationale de contrôle des techniques de renseignement (CNCTR).

Importa referir também a Loi n.º 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrâles frontaliers, que instituiu um regime de requisição administrativa dos dados de conexão. Este diploma foi reformulado pela lei de programação militar de 2013. Contudo, a vigência de várias das suas disposições foi sendo sucessivamente prolongada no âmbito da política de luta contra o terrorismo, estando ainda em vigor em finais de 2015. As disposições em causa dizem respeito ao controlo de identidade a bordo de comboios transfronteiriços, dispositivo de requisição administrativa de dados relativos às comunicações eletrónicas e acesso dos serviços luta contra o terrorismo a certos arquivos administrativos. A já mencionada lei de programação militar de 2013 estendeu ainda a capacidade de acesso aos dados de conexão ao conjunto dos serviços de informação — e não apenas serviços relevantes do Ministério do Interior — por qualquer motivo ligado à defesa dos interesses fundamentais da nação. Na realidade, mais do que uma inovação, tratou-se de uma simplificação legal, atendendo a que isto já era possível, No Código de segurança interior precisam-se as técnicas especiais de recolha de informações sujeitas a uma autorização, abrangendo as seguintes matérias: Acesso administrativo aos dados de conexão (artigos L851-1 à L851-7); Interceções de segurança {artigo L852-1); Sonorização de certas instalações e veículos e captação de imagens e dados informáticos (articles L853-1 à L853-3); Medidas de vigilância das comunicações eletrónicas internacionais (articles L854-1 à L854-9). "E, quanto ao Reino Unido, apontando para que a Regulation of Investigatory Powers 2000 (RIPA) é a lei que regula os poderes de entidades públicas no âmbito da vigilância e investigação, assim como da interceção de comunicações. Foi introduzida com o propósito de acomodar mudanças tecnológicas no domínio da comunicação, como a Internet e a encriptação. Mais recentemente, a UK Investigatory Powers Act 2016 veio introduzir alterações no âmbito da interceção de comunicações, interferência de equipamentos (hacking para obter informações) e aquisição de dados de comunicação em massa. Esta lei entrou em vigor no final de 2016.

O sistema de informações do Reino Unido é composto, ao nível de direção estratégica, pela Joint Intelligence Committee (JIC) (Lordes e Comuns), instituída pelo Intelligence Services Act 1994.

O Reino Unido possui ainda a Intelligence and Security Committee, criada por iniciativa governamental, através do qual os membros são nomeados pelo Primeiro-ministro, sob nomeação do Parlamento e consulta do líder da oposição, respondendo a Comissão diretamente ao Primeiro-ministro. A UK Investigatory Powers Act 2016 criou também a Investigatory Powers Commission (IPC), com o fim de supervisionar, conjuntamente com a Intelligence and Security Committee, o uso de todos os poderes investigatórios.

Outra das medidas constantes da nova lei de 2016 prende-se com a exigência de confirmação por um juiz (ao serviço da IPC) da autorização para aceder ao conteúdo de comunicações (ou interferência de equipamento) autorizadas por um secretary of state (equivalente a ministro no sistema português).

Uma descrição detalhada da nova regulamentação da UK Investigatory Powers Act 2016 pode ser consultada nos vários documentos informativos da proposta que lhe deu origem, destacando-se o referente Information Data, Interferência de Equipamento e Interceção de comunicações — e fazendo apelo aos instrumentos de direito internacional e jurisprudência supranacional aplicáveis — o artigo 12.º da Declaração Universal dos Direitos Humanos, em redação retomada pelo artigo 17.º do Pacto Internacional relativo aos Direitos Civis e Políticos; o artigo 8.º da Convenção Europeia dos Direitos Humanos (CEDH), de acordo com cujo n.º 2, «não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir

uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros» e a jurisprudência do Tribunal Europeu dos Direitos do Humanos (TEDH) sobre a proteção do acesso a dados de comunicações, que afirma expressamente que os mesmos se encontram abrangidos pela proteção de «vida privada e familiar» ínsita no n.º 1 do artigo 8.º da CEDH».

O Presidente da Assembleia da República chama ainda a atenção para as pronúncias escritas sobre as iniciativas legislativas da Comissão Nacional de Proteção de Dados, da Comissão de Fiscalização de Dados dos Serviços de Informações da República Portuguesa, do Secretário-Geral do Sistema de Informações da República Portuguesa, do Conselho de Fiscalização do Sistema de Informações da República Portuguesa e da Procuradoria-Geral da República.

Por último, transcreve-se na resposta do órgão autor da norma uma parte do debate parlamentar que precedeu a aprovação da Lei Orgânica n.º 4/2017.

**5** — Discutido em Plenário o memorando elaborado pelo Presidente do Tribunal Constitucional, nos termos do artigo 63.º, n.º 1, da LTC, foi fixada a orientação do Tribunal; distribuído o processo à relatora designada por sorteio, foi apresentado e discutido o projeto de acórdão; perante a posição da Relatora, o Presidente do Tribunal, ouvido o mesmo, designou novo relator para elaborar o acórdão em conformidade com o projeto discutido.

Cumpre agora decidir em harmonia com o que então se estabeleceu.

## II — Fundamentos

6 — Enquadramento

### *a*) As normas questionadas no quadro do novo sistema de acesso aos metadados

As normas questionadas constam, como já se afirmou, da Lei Orgânica n.º 4/2017, que veio instituir um procedimento especial de acesso a dados de telecomunicações e Internet, previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, por parte dos oficiais de informações do SIS e do SIED. O diploma foi regulamentado pela Portaria n.º 237-A/2018, de 28 de agosto, que define as condições técnicas e de segurança da comunicação eletrónica, para efeito de transmissão diferida dos dados de telecomunicações e Internet obtidos de acordo com o regime consagrado na dita Lei Orgânica.

Na exposição de motivos da Proposta de Lei n.º 79/XIII, uma das iniciativas legislativas que conduziram à aprovação da Lei Orgânica ora em questão, o Governo explica o seguinte:

"O Sistema de Informações da República Portuguesa (SIRP), através do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS), no estrito cumprimento da Constituição e da Lei e em regime de exclusividade, assegura a produção de informações necessárias à salvaguarda dos interesses nacionais, da independência nacional e da segurança interna.

Os Serviços de Informações, SIED e SIS, no exercício das suas missões e competências, prosseguem as atividades de produção de informações atinentes à manutenção das condições de segurança dos cidadãos, bem como ao pleno funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de direito democrático.

Nesse âmbito, os resultados da atividade dos Serviços de Informações, SIS e SIED, consubstanciam uma exclusiva e permanente avaliação das principais ameaças ao Estado de direito democrático, algumas especialmente corrosivas dos pilares do Estado de direito democrático tais como o fenómeno terrorista, pela sua abrangência e impacto.

Procurando corresponder os procedimentos e metodologias da atividade dos Serviços de Informações da República Portuguesa aos desafios colocados à segurança nacional e internacional do Estado, considerando os procedimentos e metodologias previstas em regimes jurídicos aplicáveis a serviços congéneres, particularmente no espaço europeu, espaço esse onde naturalmente estes serviços se inscrevem e, atendendo, ainda, ao regime estabelecido na Estratégia Nacional de Combate ao Terrorismo, aprovado pela Resolução do Conselho de Ministros n.º 7-A/2015, de

20 de fevereiro, configura-se adequado e proporcional a consagração de um regime especial de acesso a dados de base e a dados de tráfego de comunicações eletrónicas ao abrigo da Constituição e da lei por parte do SIRP".

A intenção do legislador foi, assim, a de consagrar na legislação ordinária a possibilidade de acesso a um amplo conjunto de dados sobre dados, ou metadados, relativos a comunicações, por parte dos oficiais de informação do SIRP, expurgando o regime jurídico das inconstitucionalidades apontadas pelo Tribunal Constitucional, no seu Acórdão n.º 403/2015, relativo à apreciação preventiva da constitucionalidade do artigo 78.º do Decreto n.º 426/XII da Assembleia da República.

Para bem se compreender o sentido e alcance das normas em análise e poder levar a cabo a ponderação que deverá presidir ao juízo sobre a sua validade constitucional, há que ter presente o sentido prescritivo dos preceitos normativos que lhe são acessórios, quer os consagrados na própria Lei Orgânica n.º 4/2017, quer os que constam da Portaria n.º 237-A/2018.

Deste modo, e salientando apenas as mais relevantes, há que destacar as normas da Lei Orgânica n.º 4/2017, que estatuem o seguinte:

*Artigo 5.º*

***Comunicação ao Ministério Público e autorização judicial***

*1 — O acesso dos oficiais de informações do SIS e do SIED a dados de telecomunicações e Internet no âmbito da atividade de pesquisa depende de autorização judicial prévia e obrigatória, por uma formação das secções criminais do Supremo Tribunal de Justiça, constituída nos termos do artigo 8.º, que garanta a ponderação da relevância dos fundamentos do pedido e a salvaguarda dos direitos, liberdades e garantias constitucionalmente previstos.*

*2 — O processo de autorização de acesso aos dados é sempre comunicado ao Procurador-Geral da República.*

*Artigo 6.º*

***Admissibilidade do pedido***

*1 — O pedido só pode ser autorizado quando houver razões para crer que a diligência é necessária, adequada e proporcional, nos termos seguintes:*

*a*) *Para a obtenção de informação sobre um alvo ou um intermediário determinado; ou*

*b*) *Para a obtenção de informação que seria muito difícil ou impossível de obter de outra forma ou em tempo útil para responder a situação de urgência.*

*2 — É proibida a interconexão em tempo real com as bases de dados dos operadores de telecomunicações e Internet para o acesso direto em linha aos dados requeridos.*

*Artigo 8.º*

***Controlo judicial e autorização prévia***

*O controlo judicial e a autorização prévia do acesso dos oficiais de informações do SIS e do SIED a dados de telecomunicações e Internet são efetuados por uma formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções.*

Quanto à Portaria n.º 237-A/2018, da sua leitura resulta uma perceção mais clara da efetiva forma de funcionamento do sistema de acesso às informações por parte dos oficiais do SIS e do

SIED, sendo de destacar as normas que seguidamente se transcrevem, porque permitem compreender o conjunto de trâmites processuais a realizar:

*Artigo 1.º*

1 — Os trâmites processuais relacionados com a comunicação eletrónica de dados de telecomunicações e Internet aos serviços de informações pelos prestadores de serviços de comunicações eletrónicas, nos termos previstos na Lei Orgânica n.º 4/2017, de 25 de agosto, são praticados por via de um serviço informático, baseado na Internet, especificamente disponibilizado para o efeito no denominado «Sistema de Acesso ou Pedido de Dados aos Prestadores de Serviços de Comunicações Eletrónicas», abreviadamente designado por SAPDOC.

*2 — O SAPDOC é desenvolvido e gerido pelo Instituto de Gestão Financeira e Equipamentos da Justiça, I. P. (IGFEJ, I. P.), a quem caberá também a função de gestão do sistema e da respetiva credenciação de acesso.*

*3 — O SAPDOC é dotado de funcionalidades técnicas que permitam praticar, pelo menos, os seguintes atos procedimentais, em execução dos procedimentos previstos na Lei Orgânica n.º 4/2017, de 25 de agosto:*

*a*) *Apresentação do pedido, elaborado pelos diretores do Serviço de Informações de Segurança (SIS) ou do Serviço de Informações Estratégicas de Defesa (SIED)* e *remetido pelo/a Secretário/a-Geral do Sistema de Informações da República Portuguesa (SIRP)* ao *Presidente do Supremo Tribunal de Justiça (n.º 1 do artigo 9.º da Lei Orgânica n.º 4/2017);*

*b*) *Comunicação do pedido ao/à Procurador/a-Geral da República (n.º 1 do artigo 9.º da Lei Orgânica n.º 4/2017);*

*c*) *Eventual pronúncia do/a Procurador/a-Geral da República ao pedido elaborado pelos diretores do SIS ou do SIED;*

*d*) *Envio do pedido, pelo Presidente do Supremo Tribunal de Justiça, à formação especial de juízes (n.º 1 do artigo 5.º e artigo 8.º da Lei Orgânica n.º 4/2017);*

*e*) *Elaboração ou anexação da deliberação da formação especial de juízes (n.º 3 do artigo 10.º e n.º 1 do artigo 12.º da Lei Orgânica n.º 4/2017);*

*f*) *Comunicação da deliberação ao serviço de informações, ao prestador de serviços de comunicações eletrónicas depositário dos dados e ao/à Procurador/a-Geral da República (n.º 2 do artigo 5.º da Lei Orgânica n.º 4/2017);*

*g*) *Comunicação da deliberação à Comissão de Fiscalização de Dados do SIRP, com referência nominativa;*

*h*) *Eventual reação do SIS ou do SIED, do prestador de serviços de comunicações eletrónicas depositário dos dados ou do/a Procurador/a-Geral da República à deliberação da formação especial de juízes;*

*i*) *Remessa do ficheiro de resposta com os dados, pelo prestador de serviços de comunicações eletrónicas, com conhecimento da formação especial de juízes do Supremo Tribunal de Justiça que deliberou e do/a Procurador/a-Geral da República (n.º 1 do artigo 11.º da Lei Orgânica n.º 4/2017*);

*j*) *Eventual pronúncia do/a Procurador/a-Geral da República;*

*k*) *Validação do tratamento dos dados (n.º 2 do artigo 12.º da Lei Orgânica n.º 4/2017) e respetivo envio, pela formação especial de juízes do Supremo Tribunal de Justiça que deliberou, ao Diretor do Centro de Dados do SIS ou ao Diretor do Centro de Dados do SIED, com conhecimento do/a Procurador/a-Geral da República;*

*l*) *Comunicação, pelo Diretor do Centro de Dados do SIS ou pelo Diretor do Centro de Dados do SIED, da receção e armazenamento com sucesso do ficheiro de resposta;*

*m*) *Cancelamento dos procedimentos em curso de acesso a dados, pela formação especial de juízes do Supremo Tribunal de Justiça (n.º 3 do artigo 12.º da Lei Orgânica n.º 4/2017);*

*n*) *Comunicação da decisão de cancelamento de acesso e de destruição imediata dos dados ao Diretor do Centro de Dados do SIS ou ao Diretor do Centro de Dados do SIED, ao prestador de serviços de comunicações eletrónicas depositário dos dados, ao/à Procurador/a-Geral da República*

*e à Comissão de Fiscalização de Dados do SIRP, para efeitos do exercício das suas competências legais (n.os 3, 4 e 5 do artigo 12.º da Lei Orgânica n.º 4/2017);*

*o*) *Comunicação, pelo Diretor do Centro de Dados do SIS ou pelo Diretor do Centro de Dados do SIED, ao/à Procurador-Geral da República, dos dados obtidos que indiciem a prática de crimes de espionagem e terrorismo (artigo 13.º da Lei Orgânica n.º 4/2017), sempre que tal seja possível e nos termos da legislação aplicável.*

***b*) O quadro europeu**

Decorre dos preceitos acima transcritos que o acesso do SIS e do SIED aos dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas implica que estes últimos procedam ao registo e à organização de dados pessoais para efeitos de armazenamento e à sua transmissão não autorizada a terceiros. Trata-se, pois, de *tratamento* de dados de comunicações sem o prévio consentimento dos seus titulares que interfere naturalmente com a *proteção da privacidade* no setor das comunicações eletrónicas.

Tal matéria é objeto da disciplina constante da Lei n.º 41/2004, de 18 de agosto ("Lei da Privacidade nas Comunicações Eletrónicas"), que transpôs para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (na versão decorrente da Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009) — adiante referida apenas como "*Diretiva n.º 2002/58*".

As disposições da Diretiva n.º 2002/58 visavam especificar e complementar a Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 — transposta para a ordem jurídica portuguesa pela "Lei de Proteção de Dados Pessoais" (Lei n.º 67/98, de 26 de outubro) — a qual foi revogada pelo Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, cuja execução foi assegurada, na ordem jurídica interna, pela Lei n.º 58/2019, de 8 de agosto, que revogou a referida Lei n.º 67/98, de 26 de outubro. No seu artigo 1.º, n.º 1, estabelece-se que o objetivo da Diretiva é prever «a harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações eletrónicas na Comunidade».

A Lei n.º 41/2004, no n.º 4 do artigo 1.º, remete para *legislação especial* a definição das exceções e do respetivo regime jurídico que se mostrem estritamente necessárias para a proteção de atividades relacionadas com a segurança pública, a defesa, a segurança do Estado e a prevenção, investigação e repressão de infrações penais. Tal disposição justifica-se e compreende-se à luz do previsto nos artigos 1.º, n.º 3, e 15.º, n.º 1, da referida Diretiva n.º 2002/58, que preveem o seguinte:

Artigo 1.º

*3 — A presente diretiva não é aplicável a atividades fora do âmbito do Tratado que institui a Comunidade Europeia, tais como as abrangidas pelos títulos V e VI do Tratado da União Europeia, e em caso algum é aplicável às atividades relacionadas com a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando as atividades se relacionem com matérias de segurança do Estado) e as atividades do Estado em matéria de direito penal.*

Artigo 15.º

*1 — Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.os 1 a 4 do artigo 8.º e no artigo 9.º da presente diretivas sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública e a prevenção, a investigação, a deteção e a*

*repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.º 1 do artigo 13.º da Diretiva 95/46/CE. Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.os 1 e 2 do artigo 6.º do Tratado da União Europeia.*

Através de tais disposições, a Diretiva 2002/58 pretende realizar um esforço de compatibilização entre as exigências comunitárias da prevenção da criminalidade grave e os princípios da confidencialidade, do anonimato e da não conservação de dados. Para concretização desse objetivo, a Diretiva prevê a possibilidade de os Estados-Membros adotarem medidas legislativas restritivas do âmbito dos direitos e obrigações previstos nos seguintes preceitos: (i): no artigo 5.º, que estabelece o princípio da confidencialidade das comunicações e respetivos dados de tráfego, incluindo a proibição de armazenamento de dados de tráfego sem o consentimento dos utilizadores, sem prejuízo das exceções legalmente previstas nos termos do artigo 15.º, n.º 1; (ii) no artigo 6.º, que estatui a obrigação de os dados de tráfego relativos a assinantes e utilizadores tratados e armazenados pelo fornecedor de uma rede pública de comunicações ou de um serviço de comunicações eletrónicas publicamente disponíveis serem eliminados ou tornados anónimos «quando deixem de ser necessários para efeitos da transmissão da comunicação», mas sem prejuízo do disposto no citado artigo 15.º, n.º 1; (iii) nos n.os 1 a 4 do artigo 8.º, que respeitam à apresentação e restrição da identificação da linha chamadora e da linha conectada; (iv) e, finalmente, no artigo 9.º, que tem por objeto o tratamento dos dados de localização para além dos dados de tráfego, nomeadamente nos casos da prestação de um serviço de valor acrescentado.

Ora, a Lei Orgânica n.º 4/2017, ao regular o procedimento especial de acesso a dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas necessários para a prossecução da atividade de produção de informações pelo SIRP relacionadas com a segurança nacional, a defesa, a segurança do Estado e a prevenção de espionagem e do terrorismo, traduz justamente uma concretização da *exceção facultativa* ao regime-regra da privacidade em matéria de comunicações eletrónicas admitida no artigo 15.º, n.º 1, da Diretiva n.º 2002/58, com referência a atividades dos Estados-Membros, em princípio excluídas do âmbito de aplicação da mesma Diretiva, segundo o respetivo artigo 1.º, n.º 3. Ou seja, uma medida legislativa adotada por um Estado-Membro para restringir o âmbito dos direitos e obrigações previstos em certas disposições daquela Diretiva destinada a salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública e a prevenção de infrações penais.

Tal medida, enquanto resultado do exercício do poder legislativo de um Estado-Membro, está naturalmente sujeita à respetiva Constituição e, devido à matéria em causa, tem de respeitar igualmente os limites estatuídos no artigo 15.º, n.º 1, da Diretiva n.º 2002/58. O direito da União Europeia não impõe, antes permite a adoção daquele tipo de medidas derrogatórias, em circunstâncias bem identificadas e definidas em leis claras e precisas, em ordem a proteger os direitos fundamentais dos cidadãos afetados.

Nestes exatos termos, e apesar de se tratar de uma iniciativa exclusiva do Estado-Membro — que pode decidir, ou não, fazer uso da faculdade de derrogar certos direitos e obrigações consagrados na Diretiva n.º 2002/58 —, a aprovação de medidas derrogatórias ao abrigo do citado artigo 15.º, n.º 1, também representa uma *aplicação de «direito da União»* para efeitos do disposto no artigo 51.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia ("CDFUE"), com a consequência de vincular imediatamente a República Portuguesa, de acordo com as respetivas competências, ao respeito dos direitos e à observância dos princípios nela previstos.

A tal propósito, pode ler-se no Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson, C-203/15 e C-698/15, EU:C:2016:970 (a seguir "Acórdão *Tele2*"), n.os 73 e 74:

*«73. [O artigo 15.º, n.º 1, da Diretiva 2002/58] pressupõe necessariamente que as medidas nacionais aí mencionadas, como as relativas à conservação de dados para efeitos de luta contra criminalidade, se enquadram no âmbito de aplicação desta mesma diretiva, uma vez que esta*

*última só autoriza expressamente que os Estados-Membros as adotem desde que respeitadas as condições que prevê.*

*74 — Além disso, as medidas legislativas referidas no artigo 15.º, n.º 1, da Diretiva 2002/58 regulam, para os efeitos mencionados nesta disposição, a atividade dos prestadores de serviços de comunicações eletrónicas. Por conseguinte, este artigo 15.º, n.º 1, lido em conjugação com o artigo 3.º da referida diretiva, deve ser interpretado no sentido de que tais medidas legislativas estão abrangidas pelo âmbito de aplicação desta mesma diretiva.»*

Por outro lado, apesar de o artigo 15.º, n.º 1, da Diretiva n.º 52/2008 se referir apenas — mas a título meramente exemplificativo — a medidas legislativas que imponham a conservação dos dados durante um período limitado, nenhuma dúvida existe de que também as medidas nacionais que concedam o acesso aos dados previamente conservados se enquadram no âmbito de aplicação daquele preceito, conforme foi entendido pelo Tribunal de Justiça no já citado Acórdão *Tele2*:

*«76 — Também se enquadra no referido âmbito de aplicação uma medida legislativa que tem por objeto* [...] *o acesso das autoridades nacionais aos dados conservados pelos prestadores de serviços de comunicações eletrónicas.*

*77 — Com efeito, a proteção da confidencialidade das comunicações eletrónicas e dos dados de tráfego com elas relacionados, garantida no artigo 5.º, n.º 1, da Diretiva 2002/58, aplica-se às medidas tomadas por todas as pessoas que não sejam os utilizadores, independentemente de se tratar de pessoas singulares ou de entidades privadas ou públicas. Como confirma o considerando 21 desta diretiva, esta tem como objetivo impedir «o acesso» não autorizado às comunicações, incluindo a «quaisquer dados com elas relacionados», para proteger a confidencialidade das comunicações eletrónicas.*

*78 — Nestas condições, uma medida legislativa através da qual um Estado-Membro impõe, com fundamento no artigo 15.º, n.º 1, da Diretiva 2002/58, aos prestadores de serviços de comunicações eletrónicas, para os efeitos mencionados nesta disposição, a obrigação de conceder às autoridades nacionais, nas condições previstas nessa medida, o acesso aos dados conservados pelos referidos prestadores tem por objeto o tratamento de dados pessoais por parte destes últimos, tratamento que se enquadra no âmbito de aplicação desta diretiva.»*

Ainda a este respeito, importa indicar o pronunciamento decisório formulado pelo TJUE nessa ocasião em resposta às questões concretas objeto do reenvio em que aquele Acórdão foi proferido:

*«1) O artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica.*

*2) O artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União.»*

Este enquadramento à luz do direito da União Europeia é relevante direta e indiretamente: por um lado, determina, por força do princípio do primado daquele ordenamento (relativamente às matérias que relevam das atribuições e competências da União Europeia) e, bem assim, do estatuído no artigo 8.º, n.º 4, da Constituição, que as medidas legislativas nacionais adotadas com base na faculdade consagrada no artigo 15.º, n.º 1, da Diretiva 2002/58 respeitem tal disposição, assim como as demais regras e princípios do direito da União, incluindo os direitos e princípios consagrados na Carta (cf. o respetivo artigo 51.º, n.º 1); por outro, justifica a interpretação e aplicação de tais medidas em conformidade com o mesmo direito.

Sem prejuízo da competência do legislador nacional para adotar as medidas de acesso previstas na Lei Orgânica n.º 4/2017 se fundar no artigo 15.º, n.º 1, da Diretiva 2002/58, reitere-se que se trata de uma faculdade concedida e não de uma obrigação imposta pelo direito da União Europeia. Por outras palavras, os Estados-membros são autorizados, dentro de certos limites, a atuar neste domínio, segundo as formas e com as restrições que as suas ordens jurídicas determinam. Ora, encontrando-se os atos dos poderes públicos na ordem jurídica interna subordinados ao princípio da constitucionalidade (artigo 3.º, n.º 3, da Constituição), coloca-se a questão de saber se a legislação nacional respeita a Constituição. Na exata medida em que tal não seja o caso, compete ao Tribunal Constitucional eliminar as correspondentes normas da ordem jurídica interna, através de declaração de inconstitucionalidade com força obrigatória geral (artigo 282.º, n.º 1, da Constituição). Essa a questão que consubstancia o objeto do presente processo.

Daqui não se segue, todavia, que o Direito da União Europeia, assim como a Convenção Europeia dos Direitos Humanos (para o qual, de resto, o artigo 15.º, n.º 1, da Diretiva n.º 2002/58 também remete — cf. a referência ao n.º 2 do artigo 6.º do Tratado da União Europeia constante da última frase de tal preceito), devam aqui ser objeto de desconsideração, na apreciação da constitucionalidade dos artigos 3.º e 4.º da Lei Orgânica n.º 4/2017. Com efeito, por força das normas do artigo 8.º da Constituição que estabelecem a relevância do Direito Internacional e do Direito da União na ordem jurídica interna e, também, da cláusula aberta no domínio dos direitos fundamentais consagrada no artigo 16.º da Constituição, este Tribunal não pode deixar de considerar os direitos fundamentais consagrados na CDFUE e na referida Convenção, devendo igualmente ter em conta, numa perspetiva de diálogo interjurisdicional, a interpretação que dos mesmos tem vindo a ser feita pelas instâncias competentes para a sua aplicação, nomeadamente o Tribunal de Justiça da União Europeia ("TJUE") e o Tribunal Europeu dos Direitos Humanos ("TEDH").

***c*) A jurisprudência europeia em matéria de proteção da privacidade das comunicações eletrónicas**

Como referido, a problemática do tratamento de dados relativos às comunicações é matéria objeto de regulação por parte do direito da União Europeia e da CEDH, pelo que se justifica tomar em consideração a proteção que o direito à privacidade e à tutela dos dados pessoais tem conhecido na jurisprudência do TJUE e na jurisprudência do TEDH.

***i. A Carta dos Direitos Fundamentais da UE***

Respeitando as tradições constitucionais dos Estados membros da UE, a CDFUE reafirma no seu preâmbulo *«os direitos que decorrem, nomeadamente, das tradições constitucionais e das obrigações internacionais comuns aos Estados-Membros, do Tratado da União Europeia e dos Tratados comunitários, da Convenção europeia para a proteção dos direitos humanos e das liberdades fundamentais, das Cartas Sociais aprovadas pela Comunidade e pelo Conselho da Europa, bem como da jurisprudência do Tribunal de Justiça das Comunidades Europeias e do Tribunal Europeu dos Direitos Humanos»*.

Neste documento proclamatório de direitos fundamentais, de caráter vinculativo para os Estados Membros (artigo 6.º, n.º 1, do TUE), destacam-se duas normas de fundamental relevância nesta matéria, a saber, as normas constantes dos artigos 7.º e 8.º

A norma do artigo 7.º consagra o direito ao respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, sendo a norma tributária de todo o percurso de densificação destes direitos percorrido no plano europeu até à sua aprovação. Aliás, nos termos do n.º 3 do artigo 52.º, este

direito tem um sentido e um âmbito iguais aos do artigo correspondente da CEDH. Por conseguinte, as restrições suscetíveis de lhe serem legitimamente impostas são idênticas às toleradas no quadro do artigo 8.º da Convenção.

Por seu turno, a norma do artigo 8.º consagra o direito à proteção dos dados de caráter pessoal, ao acesso a esses dados e ao seu tratamento leal e com um fundamento legítimo. O conceito de dados, com interesse no presente processo, inclui "*qualquer informação relativa a uma pessoa singular identificada ou identificável, considerando-se identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social*" (cf. Catarina Sarmento e Castro, "Comentário ao art. 8.º", in *Carta dos Direitos Fundamentais da União Europeia Comentada,* Alessandra Silveira e Mariana Canotilho (ed.), Almedina, Coimbra, 2013; v. também a noção legal de "dados pessoais" do artigo 4.º, 1), do Regulamento Geral sobre a Proteção de Dados, relevante nos termos do corpo do artigo 2.º da Diretiva n.º 2002/58). Quanto à densificação do conceito de *tratamento de dados*, que também se reveste de relevância para a presente análise, "*os dados pessoais são objeto de proteção quando sujeitos a qualquer operação ou conjunto de operações (ou seja, a um «tratamento»), efetuadas com ou sem meios automatizados. São exemplos destes tratamentos de dados pessoais, a recolha de dados, o seu registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição de dados)"* (cf. igualmente a definição legal de "tratamento" prevista no artigo 4.º, 2), do citado Regulamento).

O Tribunal de Justiça tem densificado o significado das normas constantes dos artigos 7.º e 8.º da CDFUE em linha com a jurisprudência do TEDH, sustentando que "*no que respeita ao nível de proteção das liberdades e direitos fundamentais garantido dentro da União, uma regulamentação dessa proteção que implique uma ingerência nos direitos fundamentais garantidos pelos artigos 7.º e 8.º da Carta deve, segundo a jurisprudência constante do Tribunal de Justiça, estabelecer regras claras e precisas que regulem o âmbito e a aplicação de uma medida e imponham exigências mínimas, de modo a que as pessoas cujos dados pessoais estejam em causa disponham de garantias suficientes que permitam proteger eficazmente os seus dados contra os riscos de abuso e contra qualquer acesso e qualquer utilização ilícita desses dados"* (Acórdão de 6 de outubro de 2015, *Schrems*, C-362/14, EU:C:2015:650, n.º 91).

Como referido, a Diretiva n.º 2002/58/CE, relativa à privacidade e às comunicações eletrónicas, segundo o seu artigo 1.º, n.º 1, visa harmonizar as disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade, no que respeita ao tratamento de dados pessoais no sector das comunicações eletrónicas. Nesta Diretiva visa realizar-se um esforço de compatibilização entre as exigências comunitárias da prevenção da criminalidade grave e os princípios da confidencialidade, do anonimato e da não conservação de dados (cf. artigos 1.º, 5.º, 6.º, n.º 1, 8.º e 9.º).

A Diretiva admitiu a possibilidade de *derrogação* daqueles princípios, em circunstâncias bem identificadas e definidas em leis claras e precisas. O seu artigo 15.º, n.º 1, perspetiva a abordagem do Direito da União a esta problemática como um conflito entre o interesse público na investigação e prevenção da criminalidade grave e os direitos fundamentais dos cidadãos à liberdade e à privacidade, remetendo a regulação do conflito, através de medidas restritivas, para a margem de determinação dos Estados-membros, mas sem baixar o patamar de proteção dos direitos tal como garantidos na jurisprudência do TJUE e do TEDH.

No considerando n.º 11 da referida Diretiva, afirmou-se, também, que *«Assim sendo, a presente diretiva não afeta a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou tomarem outras medidas, se necessário, para quaisquer desses objetivos e em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, segundo a interpretação da mesma na jurisprudência do Tribunal Europeu dos Direitos do Homem. Essas medidas devem ser adequadas, rigorosamente proporcionais ao objetivo a alcançar e necessárias numa sociedade democrática e devem estar sujeitas, além disso, a salvaguardas adequadas, em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais*».

O TJUE, na sua jurisprudência sobre a matéria do acesso a dados pessoais, decidiu no Acórdão *Tele2*, entre outras questões, que o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da CDFUE, deve ser interpretado no sentido de que uma regulamentação nacional que incida sobre o acesso das autoridades nacionais competentes aos dados conservados, deve obedecer aos seguintes requisitos: 1) o acesso, pelas autoridades nacionais competentes, a dados pessoais deve estar limitado aos casos de criminalidade grave; 2) o referido acesso deve estar submetido a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente; 3) os dados em causa devem ser conservados em território da União.

O TJUE, nesta decisão *Tele2*, apesar de no seu dispositivo referir apenas os três citados requisitos, na fundamentação, exige ainda que os cidadãos sejam informados, *a posteriori*, desse acesso, e tenham ao seu dispor meios de reação ou remédios que lhes permitam controlar e impugnar o acesso aos seus dados, quando ilícito (n.º 121).

Por último, uma palavra para a Diretiva n.º 2006/24/CE do Parlamento Europeu e do Conselho, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações com vista a garantir a disponibilidade desses dados para efeitos de investigação, deteção e de repressão de crimes graves, assim subtraindo tais dados ao âmbito de aplicação do artigo 15.º da Diretiva n.º 2002/58. Tal Diretiva foi declarada inválida, pelo TJUE, no Acórdão de 8 de abril de 2014, *Digital Rights Ireland* e o., C-293/12 e C-594/12, EU:C:2014:238 (a seguir, "Acórdão *Digital Rights*). Considerou o TJUE, no mencionado processo, que "*a Diretiva 2006/24 não estabelece regras claras e precisas que regulem o alcance da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta*" (n.º 65). Consequentemente, entendeu que era inevitável "*concluir que esta diretiva comporta uma ingerência nestes direitos fundamentais, de grande amplitude e particular gravidade na ordem jurídica da União, sem que essa ingerência seja enquadrada com precisão por disposições que permitam garantir que se limita efetivamente ao estritamente necessário*" (*ibidem*).

A diretiva invalidada pelo TJUE foi transposta para a ordem jurídica interna pela Lei n.º 32/2008, de 17 de julho, a qual, todavia, não foi imediatamente afetada pela declaração de invalidade da Diretiva n.º 2006/24/CE (isto sem prejuízo de se considerar "*imperativo avaliar a conformidade desta com o direito da União Europeia, em especial com a Carta dos Direitos Fundamentais da UE*"; nesse sentido, v. C. Guerra e F. Calvão, "Anotação ao Acórdão do Tribunal de Justiça da União Europeia (Grande Secção)", in *Fórum da Proteção de Dados*, n.º 1, julho 2015 e, ainda a Recomendação n.º 1/B/2019 da Provedora de Justiça sobre a Lei n.º 32/2008, de 17 de julho).

Apesar de a Lei n.º 32/2008 se reportar ao tratamento de dados (recolha, registo ou conservação), que serão, num momento posterior, *transmitidos* aos serviços de informação e segurança, encontrando-se, portanto, as suas disposições numa relação de complementaridade com as normas agora em apreciação, relativas ao acesso a dados previamente conservados — embora, como resulta das disposições da Diretiva n.º 2002/58 anteriormente referidas, os prestadores de serviços de comunicações eletrónicas possam ou devam proceder ao armazenamento de dados também por razões técnicas ou ligadas à faturação de serviços —, o problema da sua validade, à luz da Constituição, não foi, contudo, colocado ao Tribunal Constitucional no presente processo, pelo que não será proferida qualquer pronúncia a este respeito.

Com efeito, tal questão não foi integrada no objeto do processo, tal como delimitado pelo princípio do pedido, nem pode afirmar-se existir uma relação de dependência funcional ou de incindibilidade entre normas, suscetível de justificar um alargamento do pedido. Eventuais problemas de constitucionalidade, por violação de normas e princípios constitucionais, terão que ser colocados em processo de fiscalização abstrata sucessiva pelas entidades legitimadas para o efeito, ou em processos de fiscalização concreta, verificados os seus pressupostos específicos de admissibilidade.

***ii. A Convenção Europeia dos Direitos Humanos***

O *standard* mínimo de proteção dos direitos fundamentais é o consagrado nas normas da Convenção Europeia dos Direitos Humanos, interpretadas de acordo com a jurisprudência do TEDH. A

jurisprudência do TEDH deve ser considerada pelo Tribunal Constitucional nas suas decisões como critério coadjuvante na interpretação das normas constitucionais, atendendo, nomeadamente, aos juízos de ponderação no contexto da aplicação do princípio da proporcionalidade e à densificação do conteúdo dos direitos fundamentais, sobretudo quando estão em causa novos direitos ou novas dimensões de direitos preexistentes. Por força da cláusula aberta no domínio dos direitos fundamentais consagrada no artigo 16.º da Constituição, este Tribunal não pode, na verdade, deixar de considerar os direitos fundamentais consagrados na referida Convenção, devendo igualmente ter em conta a interpretação que dos mesmos tem vindo a ser feita pelo Tribunal Europeu dos Direitos Humanos (TEDH).

A pedra de toque deste *standard* europeu de proteção e garantia dos direitos fundamentais à reserva da intimidade da vida privada, ao sigilo das comunicações e à proteção de dados, aqui em causa é, naturalmente, o artigo 8.º da CEDH. Dispõem as normas deste artigo que: 1) q*ualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência* e 2) *não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros*.

O TEDH tem conhecida jurisprudência sobre a matéria, sendo habitual submeter os regimes jurídicos nacionais que possibilitam intervenções estaduais neste campo a um teste de proporcionalidade bastante estrito. Assim, pese embora o facto de o TEDH reconhecer a importância do dever estadual de proteção da sociedade contra todas as formas de terrorismo e de ameaça aos valores democráticos, e de admitir restrições aos direitos consagrados no artigo 8.º da CEDH por esse motivo, exige, contudo, um escrutínio intenso e atento às circunstâncias de cada caso concreto. Em várias decisões, já citadas no Acórdão n.º 403/2015, deste Tribunal, esclareceram-se uma série de pressupostos de validade das intervenções restritivas no âmbito das comunicações e da recolha de dados pessoais.

Como o Tribunal Constitucional já deu nota nesse Acórdão, o TEDH afirmou:

«[...] que um processo de acesso a dados, porque não sujeito ao escrutínio dos indivíduos visados, tem de ser compensado por uma lei suficientemente tuteladora dos direitos fundamentais (Acórdão de 06/06/2006, Segerstedt-Wiberg e outros c. Suécia, queixa n.º 62332/2000); que essa lei deve empregar termos suficientemente claros para possibilitar a todos os cidadãos terem conhecimento das circunstâncias e dos requisitos que permitem ao poder público fazer uso de uma medida secreta que lesa o direito à vida privada pessoal e familiar e à correspondência (Acórdão de 02/08/1984, Malone c. Reino Unido, queixa n.º 8691/79); que seria contrária às exigências do artigo 8.º, n.º 2, da CEDH se a ingerência nas telecomunicações fosse conferida aos poderes públicos através de um poder amplo e discricionário, e que são necessárias regras claras e detalhadas, especialmente devido ao facto de a tecnologia disponível se tornar cada vez mais sofisticada, a fim de garantir uma proteção adequada contra ingerências arbitrárias (Acórdão de 16/02/2000, Amann c. Suíça, queixa n.º 27798/95); e nos casos Valenzuela c. Espanha (Acórdão de 30/07/1998, queixa n.º 27671/95) e Prado Bugallo c. Espanha (Acórdão de 18/02/2003, queixa n.º 58496/00), chegou à mesma conclusão, afirmando que a lei que permitia a ingerência nas comunicações não era suficientemente clara e precisa, não mencionando a natureza das infrações que podem dar lugar às mesmas, a fixação de um limite de duração da medida, as condições de acesso aos dados e a eliminação dos mesmos».

Tem entendido o TEDH, a este propósito, que a interferência nestes direitos tem de estar de acordo com a lei, e que, por razões de segurança jurídica, a lei deve ser suficientemente clara nos seus termos para fornecer aos indivíduos uma indicação adequada sobre quais são as circunstâncias e as condições que permitem às autoridades recorrer a essas medidas.

A decisão mais recente do TEDH, de 13 de setembro de 2018 (*Big Brother Watch and Others v. the United Kingdom*, queixas n.os 58170/13, 62322/14 e 24960/15), sobre a proteção do direito à privacidade em face de ingerências nas comunicações e dados de tráfego, incidiu sobre queixas

de jornalistas e organizações de direitos humanos em relação a três distintos regimes de vigilância: (1) a interceção em massa de comunicações; (2) a partilha de informações com governos estrangeiros; e (3) a aquisição de dados de comunicação previamente armazenados pelas empresas fornecedoras de serviços de comunicações.

Embora o TEDH já se tenha pronunciado noutros processos (p. ex. *Centrum För Rättvisa c. Sweden*, *Weber and Saravia c. Germany; Liberty c. the United Kingdom*), o caso *Big Brother Watch* é o primeiro em que o TEDH especificamente considera a interceção e o acesso a dados de tráfego (distintos dos dados de conteúdo) como uma interferência na vida privada das pessoas.

Relativamente à aquisição de dados previamente armazenados, o TEDH, no caso *Big Brother Watch,* estabelece os seguintes critérios de conformidade destas medidas ao artigo 8.º da CEDH (§§464 a 467): (1) o regime deve estar de acordo com a lei, no sentido de esta ser clara, acessível e de efeitos previsíveis para os cidadãos; (2) deve prosseguir um objetivo legítimo, (3) e ser necessário numa sociedade democrática, restringindo-se ao combate à criminalidade grave; (4) o acesso deve estar sujeito a uma autorização prévia decidida por um tribunal ou por uma entidade administrativa independente; (5) a lei deve providenciar garantias adequadas contra a arbitrariedade.

Embora referindo-se à recolha em massa de dados e à interceção das comunicações, questões não em causa no presente processo, afirma o TEDH que a lei tem de prever meios de notificação das medidas de vigilância aos visados, que possibilitem que estes possam usar os recursos previstos para questionar a legalidade das medidas retrospetivamente, ou, em alternativa, que qualquer pessoa que suspeite ter sido monitorizada possa questionar os serviços de informação e recorrer aos tribunais em caso de ilicitude na recolha dos seus dados pessoais (*Big Brother Watch*, § 310, seguindo orientação do Acórdão *Roman Zakharov v. Russia,* decisão de 4, de dezembro de 2015, queixa n.º 47143/06), o que exigiu ao Reino Unido previsão, pela legislação nacional, de providências para *a supervisão das medidas secretas de vigilância, mecanismos de notificação das pessoas visadas e vias de recurso.*

7 — Os dados pessoais a transmitir ao SIRP nos termos dos artigos 3.º e 4.º da Lei Orgânica n.º 4/2017

A Lei Orgânica n.º 4/2017 atribui aos oficiais de informação do SIRP o poder funcional de aceder a dados de comunicação que permitam identificar, entre outros dados, o assinante ou utilizador do meio de comunicação, a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como identificar o equipamento de telecomunicações utilizado ou a sua localização.

Ora, a atividade destes oficiais de informações já foi amplamente caraterizada por este Tribunal, no mencionado Acórdão n.º 403/2015, onde se entendeu que a recolha de "informações" para efeitos de "prevenção" — que é a definição legal do âmbito da atividade dos serviços de informação — a dissocia, naturalmente, da atividade de investigação criminal. De facto, nos termos da Lei n.º 30/84 (Lei Quadro do Sistema de Informações da República Portuguesa), "*aos serviços de informações incumbe assegurar, no respeito da Constituição e da lei, a produção de informações necessárias à preservação da segurança interna e externa, bem como à independência e interesses nacionais e à unidade e integridade do Estado*" (n.º 2 do artigo 2.º).

Também nos termos do n.º 2 do artigo 3.º da Lei n.º 9/2007 (que estabelece a orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa e do Serviço de Informações de Segurança), "*o SIED é o único organismo incumbido da produção de informações que contribuam para a salvaguarda da independência nacional, dos interesses nacionais e da segurança externa do Estado Português*"; e nos termos do n.º 3 do mesmo artigo "*o SIS é o único organismo incumbido da produção de informações destinadas a garantir a segurança interna e necessárias a prevenir a sabotagem, o terrorismo, a espionagem e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido*".

É certo que a existência de serviços de informações se afigura como um dos instrumentos ao dispor do Estado para garantir a segurança nacional, objetivo plasmado em diversos preceitos constitucionais, demonstrativos tanto da sua importância, quanto do seu lugar no quadro da Constituição. A garantia da segurança enquanto tarefa fundamental do Estado estabelece-se, desde logo, nas alíneas *a*) e *b*) do artigo 9.º, nos termos das quais lhe cabe: *a*) *Garantir a independência nacional e criar as condições políticas, económicas, sociais e culturais que a promovam;* e *b*) *Garantir os*

*direitos e liberdades fundamentais e o respeito pelos princípios do Estado de direito democrático*; tem ainda eco, na forma de direito fundamental, no n.º 1 do artigo 27.º, e no plano organizacional, nos artigos 272.º e 273.º do texto constitucional.

O enunciado do artigo 9.º da Constituição investe, assim, o Estado de um conjunto de obrigações no domínio da segurança e tem implícito o dever de empreender os esforços necessários à sua prossecução. Tal dever resulta, ao longo da Constituição, da definição dos atributos para as distintas instituições para tal criadas, e constitucionalmente consagradas, como a polícia, as forças armadas ou o sistema de informações da República (previsto na alínea *q*) do artigo 164.º da Constituição, que integra nas matérias de reserva absoluta de competência parlamentar a aprovação do seu regime jurídico).

Todavia, o próprio enquadramento legal da atividade do SIRP impõe limites claros à sua atuação, consagrando, designadamente, (i) o *princípio da constitucionalidade e da legalidade*, nos termos do qual a atividade dos serviços de informações está sujeita ao escrupuloso respeito pela Constituição e pela lei, designadamente em matéria de proteção dos direitos fundamentais das pessoas, especialmente frente à utilização de dados informatizados; (ii) o *princípio da exclusividade*, nos termos do qual a atividade dos serviços está rigorosamente limitada às suas atribuições, estando-lhes vedada a produção de informações em domínio que lhe não tenha sido concedido; (iii) e o *princípio da especialidade*, segundo o qual atividade dos serviços de informações se reduz ao seu estrito âmbito, não podendo confundir-se com a atividade própria de outros organismos, entre os quais os tribunais e as forças policiais (Acórdão n.º 403/2015 — ponto 7).

A questão de constitucionalidade ora em análise reduz-se, verdadeiramente, à averiguação da conformidade constitucional da possibilidade de acesso, pelos oficiais de informações do SIS e do SIED, a dados de base e de localização de equipamento (artigo 3.º) e a dados de tráfego (artigo 4.º). No primeiro caso, o legislador restringe esse acesso aos casos em que seja indispensável a *produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada e no seu exclusivo âmbito*; no segundo, e de forma ainda mais restritiva, prevê-se que o acesso a dados de tráfego deve limitar-se à produção de *informações necessárias à prevenção de atos de espionagem e do terrorismo*.

A Lei Orgânica n.º 4/2017 adota, no artigo 2.º, n.º 1, uma distinção entre dois grupos de dados — os «dados de telecomunicações» e os «dados de Internet» — definidos, respetivamente, nas alíneas *a*) e *b*) do n.º 1:

*"a*) «*Dados de telecomunicações», os registos ou informação constantes de bancos de dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas relativos à prestação de serviços telefónicos acessíveis ao público e à rede de suporte à transferência, entre pontos terminais da rede, de comunicações vocais, serviços de mensagens e multimédia e de outras formas de comunicação;*

*b*) «*Dados de Internet», os registos ou informação constantes de bancos de dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, relativos a sistemas de transmissão e a equipamentos de comutação ou encaminhamento que permitem o envio de sinais ou dados, quando não deem suporte a uma concreta comunicação".*

Dentro desta designação genérica de «Dados de telecomunicações e Internet», o n.º 2 do mesmo artigo 2.º adere a uma classificação tripartida — dados de base, dados de localização de equipamento e dados de tráfego — que define nas suas alíneas *a*), *b*) e *c*), nos seguintes termos:

*"a*) «*Dados de base», os dados para acesso à rede pelos utilizadores, compreendendo a identificação e morada destes, e o contrato de ligação à rede;*

*b*) «*Dados de localização de equipamento», os dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de telecomunicações que indiquem a posição geográfica do equipamento terminal de um serviço de telecomunicações acessível ao público, quando não deem suporte a uma concreta comunicação;*

*c*) «*Dados de tráfego», os dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou no âmbito de um serviço de telecomunicações, ou para efeitos da faturação da mesma".*

Estes conceitos são distintos dos utilizados habitualmente pela jurisprudência constitucional. Com efeito, é isso que resulta do Acórdão n.º 241/2002, em que o Tribunal acolheu a classificação tripartida que distingue dados de base, dados de tráfego e dados de conteúdo, classificação que foi reiterada pelos Acórdãos n.º 486/2009 e n.º 420/2017 (este, seguindo a jurisprudência do já mencionado Acórdão n.º 403/2015).

Reconhece-se, contudo, que as categorias de dados e a sua designação mudam consoante a evolução tecnológica e consoante a fonte normativa utilizada: por exemplo, enquanto a Lei n.º 32/2008, no artigo 2.º, n.º 1, al *a*), usa um conceito amplo de «dados», que inclui os dados de tráfego, os dados de localização e os dados conexos para identificar o assinante ou o utilizador, a Lei n.º 41/2004, de 18 de agosto, usa uma categoria bipartida de dados de localização e dados de tráfego, definindo-os, respetivamente, nas alíneas *e*) e *d*) do artigo 2.º

Por outro lado, alguns dos dados de localização podem ser reconduzidos a um conceito mais amplo de dados de tráfego, tal como é expressamente assumido no Acórdão n.º 403/15 e sustentado pela doutrina (cf. Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, Almedina, 2005, p. 181), enquanto outros dados de localização surgem dissociados de qualquer ato de comunicação. Esta última categoria é, porém, meramente residual, pois, segundo o parecer da CNPD n.º 38/2017, nos dias de hoje ocorrem comunicações mesmo quando o utilizador do equipamento de comunicação não o aciona direta e intencionalmente. É, por exemplo, o caso das atualizações efetuadas pelas aplicações de correio eletrónico ou outro tipo de mensagens, o que significa que a geração e troca de dados são praticamente constantes, mesmo quando os cidadãos utilizadores dos equipamentos nada fazem.

Por último, os meros dados de identificação do utilizador (designados por dados de base), isoladamente considerados, segundo a jurisprudência do Tribunal Constitucional (Acórdãos n.º 241/02, 486/2009, 403/2015 e 421/2017), não estão cobertos pelo segredo das comunicações, mas pelo direito à vida privada (artigo 26.º, n.º 1, da CRP) e à autodeterminação informativa (artigo 35.º, n.º 1, da CRP).

Seja como for, o aspeto relevante para apreciar a questão da constitucionalidade agora colocada não é o plano categorial ou conceitual, mas sim o plano material e teleológico, e por isso normativo, para efeitos de determinação do parâmetro que pode servir de referência à apreciação da constitucionalidade.

Por isso, apesar de a letra da lei estabelecer uma distinção entre *dados de base, dados de localização de equipamento* (artigo 3.º da Lei Orgânica n.º 4/2017) e *dados de tráfego* (artigo 4.º da Lei Orgânica n.º 4/2017), na apreciação da constitucionalidade das normas questionadas ter-se-á sobretudo em conta a subdivisão entre duas grandes categorias com as quais se cruza esta classificação legal tripartida: (i) os dados associados a um *ato de comunicação* (consumado ou tentado) entre duas pessoas e que são os dados de telecomunicações e os dados de tráfego de internet ligados às circunstâncias da comunicação interpessoal; (ii) e os dados que *não estão associados a uma comunicação* efetiva ou tentada entre dois sujeitos, mas que se traduzem nos dados de identificação do sujeito (nome, morada, número de telemóvel), nos dados de localização do equipamento, quando não deem suporte a uma concreta comunicação, e nos dados de tráfego que apenas envolvem comunicação entre um sujeito e uma máquina, como por exemplo, a consulta de sítios na internet.

Assim, quer os *dados de base*, quer os *dados de localização de equipamento*, a que se refere o artigo 3.º da Lei Orgânica, n.º 4/2017, não devem ser considerados como dados atinentes a uma *comunicação*, já que tanto nuns quanto noutros inexiste qualquer dimensão *subjetiva* inerente à comunicação. Os primeiros são, nos termos da alínea *a*) do n.º 2 do artigo 2.º da mesma Lei, 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; os segundos abrangem a deteção de dados de localização a partir de um telefone ligado, mas em *stand by*, e/ou através do sistema de satélite GPS ou outro (ver, neste sentido, Manuel da Costa

Andrade, "Comentário ao artigo 194.º do Código Penal", in J. Figueiredo Dias (direção), *Comentário Conimbricense do Código Penal — Tomo I,* 2.ª Edição, Coimbra Editora, 2012, pág. 1104). Contudo, ainda que incluam, como dispõe a alínea *b*) do n.º 2 do artigo 2.º da mesma Lei, "os dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de telecomunicações que indiquem a posição geográfica do equipamento terminal de um serviço de telecomunicações acessível ao público", não podem incluir dados que "*deem suporte a uma concreta comunicação*".

Já no que se refere aos *dados de internet*, a ressalva que é feita no último segmento da alínea *b*) do n.º 1 do artigo 2.º da Lei Orgânica n.º 4/2017 — «*quando não deem suporte a uma concreta comunicação*» — impõe que se distinga dados de internet que traduzem *comunicações intersubjetivas*, envolvendo um número finito de interlocutores, por regra determinado pelo emissor da comunicação, por via de *email* ou outro tipo de mensagem (v.g. *whatsapp*, *skype*, etc), e dados de internet que exprimem *comunicações de massa*, dirigidas a um número potencialmente infinito de utilizadores, como a simples "navegação" em rede, saltando *"link to link"*, visitando e lendo informação em *websites*. Qualquer um destes tipos de interatividade — interpessoal e bidirecional ou massiva e unidirecional — gera dados que permitem a identificação da comunicação, como a fonte, direção, percurso, destinatário, hora, duração, intensidade/frequência e equipamento utilizado. Correspondem a elementos funcionais da comunicação, na medida em que constituem elementos necessários ao estabelecimento da comunicação e, quando conservados e tratados, permitem identificar os utilizadores da rede.

Estes dados pessoais são de vários tipos: códigos de identificação atribuídos ao utilizador e ao destinatário, número de telefone da comunicação telefónica através da internet, nome e endereço do assinante e utilizador registado, endereço IP — *Internet Protocol* —, data e hora do início (*log in*) e do fim (*log off*) da ligação ao serviço de acesso à internet ou ao serviço de correio eletrónico, serviço de internet utilizado, número que solicita o acesso por linha telefónica, linha do assinante digital ou qualquer outro identificador terminal do autor da comunicação.

Qualquer um destes dados integra o conceito de *dados de tráfego* constante da alínea *c*) do n.º 2 do referido artigo 2.º: dados que permitem a ligação à rede e que são gerados automaticamente pela própria utilização ou transmissão em rede, sendo facultados para identificar ou permitir identificar o acesso à internet, o correio eletrónico ou outra troca de mensagens através da internet e as comunicações telefónicas sobre IP. De modo que os dados de internet compreendem dados de tráfego que servem de suporte a comunicações intersubjetivas e dados de tráfego que suportam e produzem comunicações eletrónicas de massa.

E por isso, o conteúdo da previsão normativa do artigo 4.º da mesma Lei Orgânica n.º 4/2017 — uma das normas questionadas no presente processo — integra todas as categorias de dados de tráfego: as que respeitam a comunicações telefónicas através de rede fixa, móvel ou internet, e as relativas ao próprio acesso à rede assim como ao correio eletrónico e outras formas de comunicação *on line*.

8 — Os parâmetros do controlo de constitucionalidade

O parâmetro constitucional invocado pelos requerentes, que corresponde, como veremos, ao mobilizado pelo Tribunal Constitucional em casos análogos, é o do direito fundamental à inviolabilidade do domicílio e da correspondência, concretizado, nos termos do n.º 4 do artigo 34.º da CRP, numa proibição de "*ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal*".

Contudo, a alegação dos requerentes não obsta a que, nos termos do artigo 51.º, n.º 5 da LTC, o Tribunal Constitucional possa e deva conhecer a questão de constitucionalidade com fundamento «na violação de normas ou princípios constitucionais diversos daqueles cuja violação foi invocada».

É o que se passa com a norma do artigo 3.º da Lei Orgânica n.º 4/2017, que está fora do perímetro do n.º 4 do artigo 34.º da Constituição, na medida em que os «dados de base e de localização de equipamento» não respeitam, segundo as definições desses conceitos dadas no n.º 2 do artigo 2.º da Lei n.º 4/2017, a uma «*concreta comunicação*». Foi o que se entendeu no Acórdão n.º 403/2015: a proibição de ingerência das autoridades públicas nas telecomunicações, constante do artigo 34.º da CRP, abrange os chamados «metadados», mas pressupõe uma «concreta co-

municação» entre pessoas (ponto 15). Sendo assim, os *dados de base* (v.g. número de telefone, endereço eletrónico, contrato de ligação à rede) e os *dados de localização* de equipamento, quando não dão suporte a uma concreta comunicação, ainda que protegidos pela reserva da vida privada, não estão abrangidos pela tutela do sigilo das comunicações.

E é também o que acontece com o segmento ideal do artigo 4.º da Lei Orgânica n.º 4/2017 que tem por objeto dados de tráfego que não envolvem comunicações intersubjetivas. De facto, a distinção que se faz no artigo 2.º dessa Lei, tendo por referência o conjunto de "dados previamente armazenados" pelos prestadores de serviços de comunicações eletrónicas, entre «*dados de telecomunicações*» e «*dados de Internet*», e dentro desta categoria, entre *dados que dão suporte a uma comunicação* e dados que *não dão suporte a uma comunicação*, acaba por refletir-se na determinação do parâmetro constitucional que protege o acesso a tais dados. Ainda que efetuada exclusivamente para efeitos dessa Lei, cujos preceitos não preveem um regime jurídico diferenciado para cada uma das referidas categorias, a distinção pode implicar que a legitimidade constitucional das normas de acesso seja aferida por diferentes parâmetros constitucionais, tendo por referência o âmbito de proteção definido para o artigo 34.º da Constituição, restringido à comunicação intersubjetiva e às suas circunstâncias ou elementos funcionais (por meio de telecomunicações ou internet). A inclusão dos dados de internet, *que não deem suporte a uma concreta comunicação intersubjetiva,* no conceito de dados de tráfego pode convocar parâmetro constitucional distinto daquele com o qual se procede ao controlo da conformidade constitucional do acesso aos dados de tráfego das comunicações interpessoais efetuadas através de telecomunicações ou por outros meios de comunicação, se se considerar a jurisprudência do Acórdão n.º 403/2015 quanto ao sentido e alcance do citado preceito constitucional.

Como se referiu, o objeto de proteção do sigilo de comunicações, consagrado no n.º 4 do artigo 34.º da Constituição, reporta-se exclusivamente à interatividade entre utilizadores, possibilitada por meios como o correio eletrónico, o *chat* ou a videoconferência (utilizador-utilizador). Já os dados de internet tratados para outro tipo de interatividade, nomeadamente a do utilizador com o computador e os respetivos programas (de organização, pesquisa e seleção de informação) e a navegação *intra* e *inter* documentos publicados nas páginas *web*, estão fora do âmbito de proteção daquele preceito constitucional.

Todavia, como o tratamento informático dessa categoria de dados permite identificar o nome, morada e outros dados de identificação do utilizador, os mesmos são considerados "*dados pessoais*" protegidos pelo artigo 35.º da Constituição. O n.º 2 deste artigo atribui à lei a definição do conceito de dados pessoais, o que foi feito na alínea *a*) do artigo 3.º da Lei n.º 67/98, de 26 de outubro: «*qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social*». Portanto, a informação constante dos dados de tráfego, mesmo que separada de um processo de comunicação intersubjetiva, é considerada de caráter pessoal, pois permite identificar o respetivo titular.

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

Em consequência do exposto, a constitucionalidade das normas do artigo 3.º e de um segmento ideal do artigo 4.º — que regulam o acesso a dados pessoais que *não envolvem comunicação intersubjetiva* (dados de base, dados de localização e dados de tráfego, dissociados de um ato de comunicação, consumado ou tentado, entre duas pessoas) — terá de ser aferida à luz dos direitos fundamentais consagrados nos artigos 26.º, n.º 1, e 35.º, n.os 1, 3 e 4, da Constituição; enquanto o acesso àqueles dados de tráfego que *envolvem comunicação entre pessoas* (mensagens de correio eletrónico, chamadas de telemóvel, conversas por *Voip,* designadamente, *Skype* ou *Whatsapp*) estará, na referida perspetiva, abrangido, desde logo (e sem prejuízo de também se tratar de dados pessoais tutelados nos termos dos citados artigos 26.º, n.º 1, e 35.º, n.os 1, 3 e 4), pelo âmbito de proteção do artigo 34.º, n.º 4, da Constituição.

Dada a especialidade da tutela dispensada por este último preceito, cumpre começar por fixar o respetivo sentido e alcance, tendo presente o decidido no Acórdão n.º 403/2015.

9 — A tutela constitucional das comunicações intersubjetivas

No seu pedido de fiscalização abstrata sucessiva das normas dos artigos 3.º e 4.º da Lei Orgânica n.º 4/2017, os requerentes invocam a violação do artigo 34.º, n.º 4, da Constituição:

*«É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo criminal».*

Recorde-se que foi com base em tal parâmetro que este Tribunal, no Acórdão n.º 403/2015, se pronunciou pela inconstitucionalidade do n.º 2 do artigo 78.º do Decreto n.º 426/XII da Assembleia da República, que versava justamente sobre o acesso a dados e informações por parte de oficiais do SIS e do SIED, designadamente a «*dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização*».

Na ocasião, o Tribunal, atentos os termos do pedido, limitou a sua apreciação aos dados de tráfego, tal como definidos na Diretiva n.º 2002/58 e na Lei n.º 41/2004 (cf. os respetivos pontos 6 e 9 e *supra* o ponto 7): dados «que identificam ou permitem identificar a comunicação e, uma vez conservados, possibilitam a identificação das comunicações entre emitente e destinatário, a data, o tempo e a frequência das ligações efetuadas». E foi justamente o acesso *não consentido* a estes dados — dados das comunicações efetivamente realizadas ou tentadas — *fora do âmbito do processo penal* que o Tribunal considerou lesivo de direitos fundamentais das pessoas envolvidas no ato comunicacional.

Com efeito, reconheceu o Tribunal, «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.», já 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*" (cf. "Bruscamente no verão passado — A Reforma do Código de Processo Penal"*, Revista de Legislação e Jurisprudência,* Ano 137.º, julho-agosto 2008, pág. 338)» e o ponto 12 do Acórdão n.º 403/2015). É, por conseguinte, claro «que a manipulação ilegal ou ilegítima do conteúdo e das circunstâncias da comunicação pode violar a *privacidade* dos interlocutores intervenientes, atentando ou pondo em risco esferas nucleares das pessoas, das suas vidas, ou dimensões do seu modo de ser e estar. De sorte que a possibilidade de se aceder aos dados das comunicações colide com um conjunto de valores associados à *vida privada* que fundamentam e legitimam a proteção jurídico-constitucional» (v. *ibidem*).

9.1 — É nesse contexto que o Tribunal analisa a liberdade de ação e uma série de direitos relacionados com a esfera íntima e a esfera privada (direito à solidão, direito ao anonimato e direito à autodeterminação informacional) como reserva da intimidade da esfera privada e, mais amplamente, do direito ao desenvolvimento da personalidade consagrados no artigo 26.º da Constituição.

Ora, uma das dimensões da liberdade de ação inerente ao desenvolvimento da personalidade consiste na liberdade de comunicar, tuteladora da comunicação interpessoal: «a comunicação que se destina a um recetor individual ou a um círculo de destinatários previamente determinado» (Acórdão n.º 403/2015, ponto 13). Tal liberdade abrange, deste modo, «a faculdade de comunicar com segurança e confiança e o domínio e autocontrole sobre a comunicação, enquanto expressão e exteriorização da própria pessoa» (v. ibidem). E é essa mesma liberdade, enquanto refração do direito ao desenvolvimento da personalidade e da tutela da privacidade, que mereceu no texto constitucional um recorte material específico, através da autonomização, no artigo 34.º, do sigilo dos meios de comunicação privada (v. ibidem).

É com referência a este último que se pode autonomizar o direito à autodeterminação comunicativa, que é simultaneamente um direito negativo (ou de defesa, nomeadamente da reserva da intimidade da vida privada) e um direito a ações positivas (v. ibidem, pontos 13 e 14):

«Na vertente de defesa da reserva da intimidade da vida privada, o direito à autodeterminação comunicativa protege a esfera pessoal perante as ingerências públicas ou privadas, ou seja, o interesse das pessoas que comunicam em impedir ou em controlar a tomada de conhecimento, a divulgação e circulação do conteúdo e circunstâncias da comunicação. Neste sentido, os interlocutores intervenientes têm *direito a um ato negativo*: à não intervenção de terceiros na comunicação e nas circunstâncias que a acompanham. Trata-se de uma garantia de que devem beneficiar, *prima facie*, todas as comunicações privadas, independentemente de as mesmas dizerem ou não respeito à intimidade dos intervenientes [...].

No entanto, o direito à autodeterminação comunicativa abrange ainda esferas de proteção mais amplas que a da simples reserva da vida privada. É que o progresso tecnológico, ao facilitar a acumulação, conservação, circulação e interconexão de dados referentes às comunicações, aumentou as possibilidades de devassa. Agora é o próprio domínio de atuação do indivíduo que é posto em causa, pois já não tem meios para assegurar a confidencialidade da comunicação. A liberdade de, à distância, trocar com os destinatários livremente escolhidos por cada um, informações, notícias, pensamentos e opiniões está comprometida com as inimagináveis possibilidades da sua afronta pelos avanços tecnológicos. Por isso, é necessário assegurar que a comunicação à distância entre privados se processe como se os mesmos se encontrassem presentes, *i.e.,* que as comunicações entre emissor e recetor, bem como o seu circunstancialismo, se tenham como uma *comunicação fechada*, em que os sujeitos se *autodeterminam* quanto à realização da mesma e esperam, legitimamente, que a comunidade proteja o circunstancialismo daquela pretendida comunicação. Ora, como a interação entre pessoas que se encontram à distância tem de ser feita através da mediação necessária de um terceiro, de um fornecedor de serviços de comunicação, exige-se que esse operador e o Estado regulador também garantam a *integridade* e *confidencialidade* dos sistemas de comunicação.

Neste contexto, o direito à autodeterminação comunicativa assume-se como um direito de liberdade, de liberdade para comunicar, sem receio ou constrangimentos de que a comunicação ou as circunstâncias em que a mesma é realizada possam ser investigadas ou divulgadas. Sem essa confiança, o indivíduo sentir-se-á coartado na liberdade de poder comunicar com quem quiser, quando quiser, pelo tempo que quiser e quantas vezes quiser. Trata-se, pois, de permitir um livre desenvolvimento das relações interpessoais e, ao mesmo tempo, de proteger a confiança que os indivíduos depositam nas suas comunicações privadas e no prestador de serviços das mesmas. Como refere Costa Andrade, «a tutela da inviolabilidade das telecomunicações radica assim na "*específica situação de perigo*" decorrente do domínio que o terceiro detém — e enquanto detém — sobre a comunicação (conteúdo e dados). Domínio que lhe assegura a possibilidade fáctica de intromissão arbitrária subtraída ao controlo do(s) comunicador(es). Por ser assim, o regime jurídico do sigilo na segurança e reserva dos sistemas apenas visa proteger a confiança na segurança e reserva dos sistemas (empresas) de telecomunicações» (*cf. Costa Andrade, ob. cit.*, pág. 339). Neste sentido, os comunicadores têm *direito a ações positivas* dos operadores e do Estado que não só assegurem a confidencialidade das comunicações e das circunstâncias em que elas se realizam como também lhes permitam controlar os dados produzidos, guardados e transmitidos que respeitem a comunicações já efetuadas.

[...]

14 — A autodeterminação comunicativa é protegida no artigo 34.º da CRP através da inviolabilidade das comunicações. A "*inviolabilidade de princípio*" justifica-se, como referem Gomes Canotilho e Vital Moreira, para «limitar na maior medida possível a possibilidade de restrições, sujeitando-se estas a pressupostos bastante vinculados» (cf. *ob. cit,* Vol. I, pág. 540). Nessa inviolabilidade inclui-se, no n.º 4 daquele preceito constitucional, a *proibição de ingerência* das autoridades públicas nos meios de comunicação, não só as que estão investidas de *poderes públicos de autoridade* como, mas por maioria de razão, as demais entidades públicas e entidades privadas (n.º 1 do artigo 18.º da CRP).

A garantia de não ingerência tem, porém, um sentido mais vasto que o sigilo de comunicações, podendo assumir um duplo relevo.

Desde logo, ela configura-se como uma garantia de *sentido negativo,* de inviolabilidade, que protege o indivíduo de ingerências do Estado ou de terceiros. Neste contexto assume-se como um direito que garante ao respetivo titular posições jurídicas perante o Estado para defesa de abusos relativos à utilização dos dados em causa. Como correspondência desta garantia, cabe ao Estado um dever de não ingerência*, de não agressão*. Deste direito deriva, como já se referiu, não só a obrigação de princípio de não divulgar o conteúdo das comunicações privadas, mas também não aceder às circunstâncias em que as mesmas foram efetuadas.

Por outro lado, a garantia de não ingerência pode, ainda, reclamar um correspondente dever a *ações positivas* por parte do Estado. Desde logo, a obrigação de o Estado adotar os instrumentos jurídicos necessários para manter a comunicação e seu circunstancialismo como "fechados" (nomeadamente, através da aprovação de leis destinadas à proteção dos dados de comunicação). Nesse sentido, o n.º 2 do artigo 26.º da CRP estabelece, precisamente, uma obrigação legiferante, obrigando o legislador a estabelecer garantias contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações. Depois, através da efetivação do referido "direito ao apagamento" ou ao "bloqueio" dos dados de tráfego, que vai ínsito no direito à autodeterminação comunicativa, e no correspondente "direito ao esquecimento". De facto, o direito à autodeterminação comunicativa tem, nos dias de hoje, e face à tendencial perenidade dos registos de dados, de passar pela imposição de limites temporais à conservação dos dados.»

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

Partindo deste entendimento, cumpre delimitar negativamente o âmbito da regra consagrada no n.º 4 do artigo 34.º da Constituição, no sentido de excluir da proteção conferida pela norma todos os dados e todas as ações que não possam, verdadeiramente, qualificar-se como *telecomunicação* ou *meio de comunicação pessoal*. Por isso, o sigilo das telecomunicações «só vale para os autênticos dados de comunicação, isto é, aqueles que se reportam a ações de telecomunicação e são, como tais, protegidos contra a intromissão arbitrária» (Manuel da Costa Andrade, "Comentário ao artigo 194.º do Código Penal", *ob. cit.* 2012, pág. 1103). Nestes termos, a área de tutela constitucional das telecomunicações comporta, ao lado de uma dimensão *objetiva*, uma indispensável dimensão *subjetiva*, na medida em que o ato comunicativo pressupõe sempre a existência de uma relação intersubjetiva, um contacto ou, pelo menos, uma tentativa de contacto entre *pessoas*.

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

Posição semelhante encontra-se na doutrina e jurisprudência alemãs, a propósito do âmbito de proteção do artigo 10.º da Lei Fundamental: *«Desenha-se aqui, no âmbito do Artigo 10.º, um nível diferenciado de proteção. O círculo mais estreito é constituído pelo núcleo essencial da privacidade, que é garantida não apenas dentro da habitação, mas também na comunicação à distância. De forma menos intensiva, mas também com um nível elevado de proteção, é protegido o conteúdo da comunicação, contra escutas, leituras ou outras formas de intromissão. No que respeita aos dados sobre as circunstâncias do processo comunicativo, designadamente, os dados de*

*conexão, o Tribunal Constitucional federal enfatiza a importância da proteção efetiva dos direitos fundamentais»* (Mangoldt/Klein/Starck, *GG — Grundgesetz Kommentar, Band 1,* 7. Auflage, C. H. Beck, 2018, art. 10, Abs. 2, 75, p. 1084).

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

9.2 — O n.º 4 do artigo 34.º, embora proíba as ingerências na correspondência, nas telecomunicações e nos demais meios de comunicação, admite-as nos «casos previstos na lei em matéria de processo penal», ou seja, «a autorização constitucional expressa para a restrição do direito à inviolabilidade das comunicações é completada com a discriminação dos *fins e interesses* a prosseguir com a lei restritiva ou com o *critério* que deve balizar a intervenção do legislador ordinário» (v. Acórdão n.º 403/2015, ponto 16). Tal constitui, ao mesmo tempo, a «garantia de que tais restrições não estão autorizadas noutras matérias e para outras finalidades» (v. *ibidem*).

Deste modo, o n.º 4 do artigo 34.º da CRP conduz à inevitável conclusão de que o legislador constitucional resolveu explicitamente, no texto da Constituição, o sentido no qual devem ser resolvidas as eventuais colisões entre os valores constitucionalmente protegidos, e os correspetivos direitos fundamentais, à liberdade individual, e à sua específica dimensão de direito à inviolabilidade das telecomunicações, por um lado, e, por outro, à segurança e preservação da ordem constitucional, que se traduz na necessidade de prevenir a ocorrência de atos passíveis de a colocar em perigo. Ao resolver de forma expressa tal tensão axiológica e jusfundamental, o legislador constituinte retirou ao intérprete constitucional o espaço para encontrar, por via interpretativa, solução distinta para a operação de concordância prática em questão.

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

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

Que não estamos perante uma "incompletude contrária ao plano normativo" da Constituição é confirmado, de forma implícita, mas clara, pelas opções valorativas tomadas aquando da 4.ª e da 5.ª revisões constitucionais. Nessas revisões foram abertamente tidos em conta imperativos acrescidos de segurança e a necessidade de incrementar medidas contra a criminalidade referida na alínea *c*) do n.º 2 do artigo 4.º do Decreto n.º 426/XII. Esse objetivo levou a alterações que se traduziram em restrições a direitos fundamentais, nesta área, com a consagração de novos equilíbrios normativos entre os valores aqui em confronto.

Assim, pela 4.ª revisão, o artigo 33.º, n.º 3, passou a prever a extradição de cidadãos portugueses, em condições de reciprocidade estabelecidas em convenção internacional, nos casos de terrorismo e de criminalidade internacional organizada, e desde que a ordem jurídica do Estado requisitante consagre garantias de um processo justo e equitativo. Também o n.º 4 do mesmo artigo passou a admitir a extradição por crimes puníveis com a prisão perpétua (ainda que só mediante a garantia de não aplicação ao caso).

O próprio artigo 34.º foi objeto de reponderação, na 5.ª revisão constitucional, passando a admitir-se, no n.º 3, a entrada durante a noite no domicílio das pessoas, com autorização judicial, "em casos de criminalidade especialmente violenta ou altamente organizada, incluindo o terrorismo e o tráfico de pessoas".

O repensamento desta matéria, nas referidas revisões constitucionais, deixou inalterados os termos da norma permissiva de ingerência nas telecomunicações, estabelecida na 2.ª parte do n.º 4 do artigo 34.º, e o seu alcance restrito a "matéria de processo criminal". Apenas se alargou o âmbito da proibição aos "demais meios de comunicação", na revisão de 1997.

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.»

Pode falar-se, por isso, de uma *reserva absoluta de processo criminal*:

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

Esta reserva de processo criminal constitucionalmente estabelecida tem, além do mais, relevantíssimas consequências na esfera jurídica da pessoa, em particular quando constituída arguida, como a determinação do regime de nulidade de provas obtidas através de métodos inadmissíveis e a obrigatoriedade de intervenção de um juiz quando esteja em causa a prática de atos potencialmente lesivos de direitos fundamentais:

«[O] artigo 34.º, n.º 4, ao delimitar a restrição à matéria de processo penal tem também outras consequências com reflexo no estatuto constitucional do arguido.

Desde logo, a realização da justiça, não sendo um fim único do processo criminal, apenas pode ser conseguida de modo processualmente válido e admissível e, portanto, com o respeito pelos direitos fundamentais das pessoas que no processo se veem envolvidas. O respeito desses direitos conduz, por exemplo, a considerar inadmissíveis certos métodos de provas e a cominar a nulidade de «todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações» (cf. artigo 32.º, n.º 8, da CRP). A nulidade das provas, com a consequente impossibilidade da sua valoração no processo, quando sejam obtidas por ingerência abusiva nas comunicações, corresponde assim a uma *garantia do processo criminal* e resulta de ter havido

acesso à informação fora dos casos em que a própria Constituição consente a restrição ao princípio da inviolabilidade dos meios de comunicação privada.

Por outro lado, a referência ao processo criminal implica que a intervenção restritiva careça de prévia autorização judicial. Sendo o processo criminal uma forma heterocompositiva através da qual se realizam as funções de *jurisdictio* referidas à atuação de pretensões baseadas em normas públicas de direito criminal, exige-se a intervenção de um órgão qualificado para essas funções (cf. artigo 202.º da CRP). Embora se não trate de um caso em que a reserva do juiz ou a reserva de primeira decisão se encontre especialmente individualizada na Constituição [...], não pode deixar de reconhecer-se que a reserva absoluta do juiz tende a afirmar-se quando não existe qualquer razão ou fundamento material para a opção por um procedimento não judicial de resolução de litígio (Gomes Canotilho, *ob. cit.,* pág. 663). O que é particularmente evidente quando se trate de questões que se reportam ao *núcleo duro da função jurisdicional*, como é o caso das competências exclusivas do juiz de instrução (artigos 268.º e 269.º do Código de Processo Penal), em que releva a prática de atos que afetam direitos, liberdades e garantias das pessoas (cf. Vieira de Andrade, "Reserva do juiz e intervenção ministerial em matéria de fixação da indemnizações por nacionalizações", *Scientia ivridica,* Tomo XLVII, n.os 274-276, julho/dezembro, 1998, pág. 225). Esse é seguramente o caso quando está em causa a interceção, gravação ou registo de comunicações (artigo 269.º, n.º 1, alínea *c*), do CPP).»

Daí a conclusão, que agora se reitera:

«Estando excluída a possibilidade, em todo este contexto, de efetuar uma interpretação da norma constitucional que consinta o acesso a dados de tráfego, de localização ou outros dados conexos das comunicações no âmbito das atribuições dos serviços de informações, à revelia de qualquer processo penal ou autorização judicial, ainda que tenha em vista a prevenção penal de bens jurídicos muito relevantes (artigos 4.º, n.º 1, alínea *c*), e 78.º, n.º 2, do Decreto), dificilmente se poderá encarar a ideia de uma ampliação do âmbito da restrição contida no artigo 34.º, n.º 4, 2.ª parte, a partir do fim da regulação ou da conexão de sentido da norma. Desde logo, porque a finalidade do preceito, como assinalou o Acórdão do Tribunal Constitucional n.º 241/2002, é a de *delimitar* o âmbito das restrições à garantia da inviolabilidade das comunicações. E, como se deixou exposto, essa delimitação é expressamente assumida pela Constituição como sendo apenas reconduzível às situações enquadradas pelo processo penal. Não há aqui, por isso, uma qualquer lacuna oculta que justifique, contra o seu sentido literal, uma interpretação conforme com a teleologia imanente da norma, já que ela própria tem por objetivo definir o âmbito preciso da restrição, sem que se torne possível estabelecer uma identidade valorativa entre o processo penal e a investigação levada a efeito pelos serviços de informações. Além de que o alargamento do âmbito da norma constitucional, a ser admitida, teria um duplo sentido, implicando não apenas uma ampliação do âmbito aplicativo da restrição ao princípio da não ingerência nas comunicações, mas também uma redução da garantia de reserva de juiz, através da remissão do controlo de atos que afetam direitos fundamentais para uma entidade meramente administrativa.

Pode, então, concluir-se que, no caso da proibição de ingerência das autoridades públicas nas comunicações, que o artigo 34.º, n.º 4, primeira parte, consagra como princípio geral, as *exceções* a que se refere o segmento final desse preceito estão condicionadas à *matéria de processo penal*, e sendo a restrição constitucionalmente autorizada apenas nesses termos, não tem cabimento efetuar uma qualquer outra interpretação que permita alargar a restrição a *outros efeitos*, como se a restrição não estivesse especificada no próprio texto constitucional ou se tratasse aí de uma restrição meramente implícita que permitisse atender a outros valores ou bens constitucionalmente reconhecidos.»

Resulta deste modo, claramente, que no entendimento firmado no Acórdão 403/2015, a limitação da restrição do direito de sigilo das comunicações a matéria de processo penal não se baseia exclusivamente no elemento literal ou gramatical de interpretação (a letra da lei), mas numa combinação de vários elementos — o sistemático, o histórico e o teleológico — que atribuem um especial significado à exigência constitucional de reserva absoluta de processo criminal, de acordo

com a nossa tradição sociopolítica baseada na importância do processo penal para a defesa dos direitos, liberdades e garantias dos cidadãos suspeitos de prática de um crime. Mesmo considerando a hermenêutica jurídica particular da interpretação constitucional, que confere ao intérprete uma maior liberdade, em face do argumento literal, do que a normalmente atribuída ao intérprete do direito ordinário, o conceito jurídico-constitucional de processo penal reveste-se de um significado unívoco e determinado, que não consente o grau de flexibilização ou de evolução, por via interpretativa, típico dos conceitos constitucionais abertos e plurissignificativos.

10 — A tutela constitucional da autodeterminação informativa

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

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

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

10.1 — Com efeito, o artigo 35.º da Constituição institui "*um direito fundamental à autodeterminação informativa, traduzido num conjunto de direitos relacionados com o tratamento automático das informações pessoais dos cidadãos, que visam, simultaneamente, protegê-las perante ameaças de recolha e de divulgação, assim como de outras utilizações possibilitadas pelas novas tecnologias, e, também, assegurar aos respetivos titulares um conjunto de poderes de escolha nesse âmbito*" (Catarina Sarmento e Castro, "40 Anos de "Utilização da Informática" — O artigo 35.º da Constituição da República Portuguesa", in *e-Pública* vol. 3, n.º 3, dezembro 2016, págs. 42-66).

Segundo Gomes Canotilho e Vital Moreira, «A fórmula *tratamento* abrange não apenas a individualização, fixação e recolha de dados, mas também a sua conexão, transmissão, utilização e publicação. O enunciado linguístico *dados* é o plural da expressão latina *datum* e está utilizado na Constituição no sentido que hoje lhe empresta a ciência informática: representação convencional de informação, sob a forma analógica ou digital, possibilitadora do seu tratamento automático (introdução, organização, gestão e processamento de dados)» (*Constituição da República Portuguesa Anotada,* Volume I, *ob. cit.,* pág. 550).

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

O direito à autodeterminação informativa confere assim a cada pessoa o direito de controlar a informação disponível a seu respeito, desdobrando-se em vários direitos: «*a*) o *direito de acesso*, ou seja o direito de conhecer os dados constantes de registos informáticos, quaisquer que eles sejam (públicos ou privados); *b*) o *direito ao conhecimento da identidade dos responsáveis, bem como o direito ao esclarecimento* sobre a finalidade dos dados; *c*) o direito de contestação, ou seja o direito à retificação dos dados e sobre identidade e endereço do responsável; *d*) o *direito de atualização* (cujo escopo fundamental é a correção do conteúdo dos dados em caso de desatualização); *e*) finalmente, *o direito à eliminação* dos dados cujo registo é interdito»; e o direito a conhecer a finalidade a que se destinam os dados é «um direito à autodeterminação sobre informações referentes a dados pessoais que exige uma proteção clara quanto ao «desvio dos fins» a que se

destinam essas informações. Daí as exigências jurídico-constitucionais relativas às finalidades das informações: (1) l*egitimidade;* (2) d*eterminabilidade;* (3) e*xplicitação;* (4) a*dequação e proporcionalidade*; (5) e*xatidão e atualidade;* (6) l*imitação temporal* (cf. *ob. cit.* Vol. I*,* págs. 552 e 553).

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

Isto mostra claramente que a consagração constitucional da proteção de dados pessoais constitui um instrumento do livre desenvolvimento da pessoa humana numa sociedade democrática e uma condição para o gozo da liberdade e da afirmação da identidade pessoal. Como referem Gomes Canotilho e Vital Moreira, «o conjunto de direitos fundamentais relacionados com o tratamento informático de dados pessoais arranca de alguns «direitos-mãe» em sede de direitos, liberdades e garantias. É o caso do direito à dignidade da pessoa humana, do desenvolvimento da personalidade, da integridade pessoal e da autodeterminação informativa. O enunciado «dados pessoais» exprime logo a estreita conexão entre estes direitos e o respetivo tratamento informático; podendo afirmar-se que quanto mais os dados relacionam a dignidade, a personalidade e a autodeterminação das pessoas, tanto mais se impõem restrições quanto à sua utilização e recolha (banco de dados). É neste contexto que se situam dois problemas fundamentais relativos ao processamento de dados informáticos: (1) determinação das categorias de dados; (2) graduação das ingerências necessárias à proteção de outros bens constitucionais» (*ob. cit.* Volume I, *ob. cit.,* p. 550).

Pode, na verdade, afirmar-se que o segredo dos dados pessoais e o poder de controlo do sujeito sobre os mesmos constituem uma garantia do direito ao livre desenvolvimento da personalidade enquanto possibilidade de «interiorização autónoma» da pessoa ou o direito a «autoafirmação» em relação a si mesmo, contra quaisquer imposições heterónomas (de terceiros ou dos poderes públicos). Este direito à «autoafirmação» dá guarida a vários «direitos de personalidade inominados», mesmo que não especificamente positivados na Constituição, como por exemplo, o direito aos documentos pessoais e o direito à autodeterminação informativa quanto a dados pessoais constantes de ficheiros manuais ou informáticos, o direito à confidencialidade de dados pessoais constantes de atos ou decisões públicas respeitantes ao estado civil, o direito de não ser espiado no desenvolvimento de atividades lícitas (cf. Gomes Canotilho/Vital Moreira, Vol. I, *ob. cit.,* pp. 464-465).

Por outro lado, como refere Filipa Urbano Calvão: «Enquanto modo de garantir a privacidade, afirma-se ainda como instrumento de garantia da liberdade (liberdade de ação, de expressão, de pensamento) e de desenvolvimento da personalidade de cada um e da livre participação na sociedade. Nessa medida, é ainda imprescindível para assegurar a própria democracia, no sentido de aí ser reconhecido um espaço próprio de pensamento e de escolhas, livre de influências e pressões externas públicas e privadas» (cf. *ob. cit*., pág. 88).

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

Verifica-se, assim, que existe uma forte interação entre as normas constantes do artigo 35.º e os direitos fundamentais consagrados no artigo 26.º da Constituição. As normas do artigo 35.º são enriquecidas no seu conteúdo pelos direitos fundamentais consagrados no artigo 26.º, que se referem ao desenvolvimento da personalidade e à reserva da intimidade e vida privada e familiar dos cidadãos. Por sua vez, o direito à reserva da vida privada é um direito vulnerável aos avanços

tecnológicos, protegido também pelo artigo 35.º da Constituição, que consagra, como vimos, a proteção dos cidadãos perante o tratamento de dados pessoais informatizados.

Pode, por isso, dizer-se que os direitos fundamentais consagrados nos artigos 34.º (inviolabilidade do domicílio e da correspondência) e 35.º, n.º 4 (proibição do acesso a dados pessoais de terceiros) funcionam como garantias do *direito à vida privada*., que se analisa em dois direitos menores: (a) o direito de impedir o acesso de estranhos a informações sobre a vida privada e familiar e (b) o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem. Os direitos de personalidade consagrados no artigo 26.º significam, na expressão de Gomes Canotilho e Vital Moreira (Vol. I, *ob. cit.,* p. 468), um «direito ao segredo do ser» (direito à imagem, direito à voz, direito à intimidade da vida privada, direito a praticar atividades da esfera íntima sem video-vigilância). Por força da dimensão valorativa destes direitos, a Constituição impõe ao legislador a obrigação de lhes garantir efetiva proteção contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias (artigo 26.º, n.º 2, da Constituição), em face dos sofisticados meios técnicos usados para a devassa da vida privada e para a colheita de dados sobre ela (cf. Acórdãos n.os 255/2002 e 207/2003).

Finalmente, importa sublinhar que a tutela da privacidade está ligada, por inerência, à liberdade individual. Ser livre é ter direito de expressão, mas, também, ter direito a reservar a sua vida privada e a construir um espaço existencial livre de terceiros — «o direito a estar só» ou, como afirma Paulo Mota Pinto, «o interesse do indivíduo na sua privacidade, isto é, em subtrair-se à atenção dos outros, em impedir o acesso a si próprio ou em obstar à tomada de conhecimento ou à divulgação de informação pessoal» (cf. «O Direito à Reserva sobre a Intimidade da Vida Privada», *BFD*, Universidade de Coimbra, LXIX (1993), pp. 508-509).

**10.2** — Acontece que, para estes direitos, o legislador constituinte autoriza, de forma explícita, a intervenção do legislador ordinário na esfera dos direitos fundamentais à reserva de intimidade da vida privada e à proteção de dados pessoais. É o que sucede, nomeadamente, nos n.os 1, 3 e 4 do artigo 35.º da Lei Fundamental, onde são admitidas exceções ao direito de proteção de dados pessoais, nas várias dimensões em que ele se exprime, designadamente em relação à proibição absoluta de tratamento de certo tipo de dados respeitantes à «vida privada» e à interdição de acesso de terceiros. Nesses preceitos, a Constituição autoriza a lei ordinária a restringir o conteúdo do direito, atribuindo poderes de regulação que estão sujeitos ao regime de restrição dos direitos, liberdades e garantias consagrado no artigo 18.º

É sabido que o n.º 2 do artigo 18.º impõe a observância do princípio da proporcionalidade em matéria de intervenções restritivas de direitos fundamentais, estabelecendo que a lei deve *limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos.* Por isso, na matéria a que respeita o presente processo, não pode deixar de se ter em conta a necessidade da *concordância prática* entre os direitos fundamentais das pessoas acerca das quais o SIRP pretenda reunir informações e os interesses da segurança pública e do combate à criminalidade organizada, como a espionagem e o terrorismo. É evidente que a intromissão em dados de comunicações põe diretamente em conflito direitos e valores constitucionais: por um lado, atinge um espectro de bens jurídicos ou direitos fundamentais tão eminentes como a dignidade humana, o desenvolvimento da personalidade, a integridade pessoal, a privacidade/intimidade, a autodeterminação informativa e a confidencialidade e integridade dos sistemas técnico-informáticos; e por outro, assegura valores constitucionais da comunidade, como a segurança interna e a defesa nacional.

De onde se segue que, no juízo de ponderação, à luz do princípio da proibição do excesso, tem que ser analisado se a intervenção das entidades públicas na privacidade e na liberdade dos cidadãos constitui ou representa um custo para os direitos dos cidadãos, desrazoável, excessivo ou desproporcionado, em relação aos fins visados pela medida em causa.

Importa, porém, não esquecer que a ponderação, de acordo com o princípio da proporcionalidade, à luz do artigo 18.º, n.º 2, da Constituição, se faz em moldes metodológicos semelhantes aos previstos na jurisprudência do TJUE (artigo 52.º, n.º 1, da CDFUE), e na jurisprudência do TEDH relativa ao artigo 8.º da CEDH. Nestes termos, o artigo 52.º, n.º 1, da CDFUE, à semelhança do artigo 18.º, n.º 2, da Constituição, exige que a limitação de um direito fundamental, nomeadamente, dos direitos à vida privada e à proteção dos dados pessoais, consagrados nos artigos 7.º e 8.º da

Carta, esteja prevista na lei, respeite o conteúdo essencial dos direitos fundamentais e seja justificada e necessária para a concretização dos objetivos de interesse geral reconhecidos pela UE ou para satisfazer uma necessidade de proteção dos direitos e liberdades de outrem.

Uma vez delimitado o âmbito de proteção das normas constitucionais que consagram o direito à autodeterminação informativa, é agora o momento de apreciar a constitucionalidade das normas sindicadas começando pelas questões suscitadas pelos *dados de tráfego*, tendo em conta o maior grau de lesividade da intromissão nesse domínio.

11 — A questão da constitucionalidade do artigo 4.º da Lei Orgânica n.º 4/2017

Os dados de tráfego, cujo acesso está regulado no artigo 4.º, terão, na sequência do anteriormente exposto, de ser subdivididos em duas categorias: (i) os dados de tráfego associados a atos de comunicação intersubjetiva e às suas circunstâncias; (ii) e os dados de tráfego desligados de uma intercomunicação subjetiva, como é o caso da consulta de sítios na internet e dos atos de comunicação entre uma pessoa e uma máquina*,* ou entre máquinas.

Esta segunda categoria de dados de tráfego de internet, embora não envolva comunicação intersubjetiva, exprime vários aspetos da personalidade e do comportamento dos utilizadores, pertencendo a cada pessoa o direito de escolha quanto à partilha, ou não, destas informações com terceiros, bem como o poder de vedar o acesso de terceiros a estes dados e de controlar quem tem acesso a eles e em que momento. Por isso mesmo, estes *dados de tráfego* encontram-se incluídos no âmbito objetivo de proteção das normas constitucionais atinentes à reserva de intimidade da vida privada e à autodeterminação informativa, protegidas pelos artigos 26.º, n.º 1, e 35.º da CRP.

Como se disse atrás, as normas constantes dos n.os 1 e 4 do artigo 35.º da Constituição admitem exceções ao direito à proteção dos dados pessoais, nas várias dimensões em que ele se exprime, atribuindo poderes de regulação que estão sujeitos ao regime de restrição dos direitos, liberdades e garantias (artigo 18.º da CRP).

Porém, diversamente do tipo de restrição admitido pelo n.º 4 do artigo 34.º da Constituição, que apenas autoriza a restrição do direito à inviolabilidade das comunicações em determinado domínio específico — *"em matéria de processo penal"* —, a restrição admitida pelo artigo 35.º ao direito à proteção dos dados pessoais e à autodeterminação informativa — através da expressão "*nos termos da lei*" — assume contornos distintos, menos exigentes, que conferem ao legislador uma maior margem de determinação. Quer dizer: no domínio normativo do artigo 34.º, a autorização constitucional expressa para a restrição é completada com a discriminação dos fins e interesses a prosseguir com a lei restritiva ou com o critério que deve balizar a intervenção do legislador ordinário; já quanto aos direitos fundamentais consagrados no artigo 35.º, a Constituição atribui uma competência genérica de regulação, podendo o legislador criar a restrição, tendo, no entanto, de sujeitar-se aos requisitos de legitimidade impostos pelo princípio da proporcionalidade, tal como decorre do n.º 2 do artigo 18.º da Constituição.

11.1 — O acesso a dados de tráfego que envolvem comunicação intersubjetiva

Quanto aos dados de tráfego abrangidos pelo sigilo das comunicações, como se assinalou, o legislador constituinte levou a cabo a sua própria ponderação, nos termos estabelecidos no n.º 4 do artigo 34.º Essa norma limita, como é sabido, a possibilidade de ingerência estadual nas comunicações ao âmbito do *processo criminal*. Importa, deste modo, indagar se existe alguma diferença relevante atinente ao *sistema de acesso aos dados de tráfego* ora em análise que justifique uma apreciação distinta da realizada pelo Tribunal Constitucional no Acórdão n.º 403/2015.

No fundo, trata-se de questionar se as alterações introduzidas no sistema de acesso pela Lei Orgânica n.º 4/2017 apresentam diferenças de tal forma significativas em relação às normas anteriormente analisadas por este Tribunal, que o aproximem, de forma decisiva, do *processo penal*, fundamentando uma mudança quanto ao juízo de constitucionalidade.

11.1.1 — O acesso dos oficiais de informações do SIS e do SIED aos *metadados*, incluindo os *dados de tráfego*, à luz da Lei Orgânica n.º 4/2017, está sujeito a vários pressupostos de admissibilidade:

*a*) Em primeiro lugar, e desde logo, o respeito pelo *princípio da proporcionalidade*, em sentido lato, incluindo as dimensões de necessidade, adequação e proporcionalidade em sentido estrito.

Esta exigência reflete-se na obrigatoriedade de fundamentação adequada do pedido de acesso aos dados (artigos 5.º e 6.º da Lei Orgânica n.º 4/2017);

*b*) Em segundo lugar, nos termos do n.º 2 do artigo 6.º da Lei Orgânica mencionada, a *proibição de interconexão* de dados em tempo real;

*c*) Em terceiro lugar, a existência de uma *autorização prévia de acesso*, para a qual é competente uma formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções (artigo 8.º). A decisão de concessão ou de denegação da autorização deve ser também fundamentada com base em informações claras e completas, nomeadamente quanto aos objetivos do processamento (n.º 3 do artigo 10.º).

*d*) Por último, a colocação em prática de *um sistema de controlo permanente*, tanto interno como externo, designadamente, para assegurar tanto a atualidade dos dados, quanto o cancelamento dos procedimentos de acesso e a destruição dos dados obtidos de forma ilegal, para além do âmbito da autorização previamente concedida, ou que não importem para o processo. Neste sistema de autorização e controlo intervêm juízes conselheiros do Supremo Tribunal de Justiça, o Procurador-Geral da República, a Comissão de Fiscalização de dados do SIRP e o Conselho de Fiscalização do SIRP, respetivamente, nos termos dos artigos 4.º a 11.º, 14.º e 15.º da Lei Orgânica n.º 4/2017.

Desta forma, no fundo, e como já se tinha explicado, as normas em causa parecem procurar responder às objeções de natureza jurídico-constitucional anteriormente colocadas, promovendo a intervenção obrigatória de uma autoridade composta por magistrados judiciais e um sistema de controlo que permita enquadrar e limitar a atividade dos serviços de informações nesta matéria.

Assim, e tendo em mente tudo o que até agora se afirmou, o que cabe questionar é se, neste caso, pode considerar-se que a intervenção de juízes e a existência de mecanismos de controlo do acesso aos *dados de tráfego* podem ter-se por *materialmente equivalentes* aos que caracterizam uma estrutura processual penal num Estado de Direito democrático, nos termos exigidos inequivocamente pela Constituição.

Ora, pode, desde já, adiantar-se que a resposta a essa pergunta não pode deixar de ser negativa, por distintas razões.

**11.1.2** — Em primeiro lugar, é de recordar, nesta sede, o que este Tribunal afirmou, no Acórdão n.º 403/2015, acerca da caracterização o SIRP: "*os fins e interesses que a lei incumbe ao SIRP de prosseguir, os poderes funcionais que confere ao seu pessoal e os procedimentos de atuação e de controlo que estabelece, colocam o acesso aos dados de tráfego fora do âmbito da investigação criminal*", pelo que "*a caracterização dessa concreta atividade como recolha de "informações" para efeitos de "prevenção" dissocia-a, de forma clara e precisa, da atividade própria de investigação criminal*" (cf. o respetivo ponto 19).

Desta forma, e apesar das mudanças operadas no sistema de acesso aos *dados de tráfego*, em relação ao que se previa nas normas fiscalizadas no Acórdão n.º 403/2015, não pode deixar de se considerar que, também nas normas ora em causa, o acesso aos dados se destina, tão-só, e sem qualquer dúvida, à prossecução das atribuições do SIRP, nos termos legalmente definidos; ou seja, a recolha de *dados de tráfego* não se destina a investigação ou produção de prova no âmbito de um processo penal em curso. Destina-se, sim, como pode ler-se no artigo 1.º da Lei Orgânica n.º 4/2017, a permitir, sempre que necessário "*a prossecução da atividade de produção de informações pelo Sistema de Informações da República Portuguesa (SIRP*) r*elacionadas com a segurança interna, a defesa, a segurança do Estado e a prevenção da espionagem e do terrorismo*".

Ora, os Serviços de Informações desempenham, no quadro do ordenamento jurídico-constitucional, uma função própria, manifestamente distinta da polícia ou do Ministério Público, que atuam no âmbito dos processos criminais. Entre o processo criminal e o serviço de informações medeia uma diferença intransponível. No processo penal, o Estado reage a um facto passado, recondutível a uma lesão ou a um perigo para bens jurídicos. A atividade do Estado parte da suspeita fundada da prática do facto, tratando-se então de confirmar (ou infirmar) a sua ocorrência, identificar e punir os seus agentes. Diferentemente, os serviços de informações movem-se à margem de qualquer indício ou suspeita da prática de um facto ilícito: atuam no "campo avançado" (*Vorfeld*) de

recolha de dados para antecipação de perigos, visando clarificar as áreas ou situações de perigo e eventualmente acompanhar pessoas supostamente perigosas. Não lhes assistindo, para além disso, a prática de quaisquer atos de intromissão ou invasão na esfera de liberdade das pessoas-alvo.

Acresce que as instâncias do processo criminal (Ministério Público e órgãos de polícia criminal) agem, em princípio, de forma pública, obedecendo a um princípio de transparência e a um conjunto de significativas e detalhadas normas legais. Já, diferentemente, aqueles serviços atuam, pela própria natureza da sua missão, em segredo, devendo limitar-se a observar, recolher e processar informações sobre factos que possam implicar risco significativo para os direitos e valores constitucionalmente protegidos. Os serviços de informações operam, assim, apenas em obediência aos princípios fundamentais da ordem jurídica, e não às normas processuais penais (veja-se a distinção traçada, neste mesmo sentido, no Acórdão do Tribunal Constitucional Alemão de 24 de abril de 2013, 1 BvR 1215/07).

Existe, conforme se concluiu no Acórdão n.º 403/2015:

«(...) uma distinção radical entre informações e investigação criminal, o que impede os oficiais de informação de intervirem no processo penal. As informações, no sentido de «elementos de conhecimento sistematizado em quadros interpretativos, através de critérios que sobrepõem a estrutura de sentido à relação causal (...) produzidas através de método próprio e preservadas da atenção e conhecimento de terceiros», nisso se traduzindo os «dois traços distintivos essenciais: — um método próprio; — um regime de segredo» (cf. Arménio Marques Ferreira, "O Sistema de Informações da República Portuguesa", in Estudos de Direito e Segurança, Almedina, 2007, pág. 69), visam a obtenção de um conhecimento específico necessário à tomada de decisões e não a recolha de prova conducente ao exercício da ação penal. Ainda que a recolha e análise de informações possa ser utilizada na investigação criminal e com vista a medidas de prevenção policiais, não deixa de ser uma atividade autónoma e prévia à investigação criminal» (cf. o ponto 19 do aresto citado).

Não pretendendo negar-se as conexões e semelhanças entre a atividade de recolha de informações, a cargo do SIRP, e o exercício da ação penal, no quadro do processo criminal, a verdade é que, inexistindo processo penal, falta um elemento essencial, no quadro constitucional vigente, para o equilíbrio entre, por um lado, a necessidade de acesso do Estado às comunicações privadas, para garantia de direitos e valores constitucionais como a liberdade e a segurança, e por outro, a obrigação de respeito pelos direitos, liberdades e garantias, como é o caso da inviolabilidade do domicílio e da correspondência, plasmadas no artigo 34.º da CRP. Esse elemento consubstancia-se na existência de *garantias constitucionais do arguido*. É certo que é possível que, em fase inicial, inexista arguido mesmo em sede de processo penal. Contudo, a verificar-se a existência de fundadas suspeitas de crime em relação a uma pessoa, a consequência natural do processo penal será a sua constituição como arguida, nos termos dos artigos 57.º e 58.º do Código de Processo Penal. Esta posição processual assegura-lhe, à luz dos artigos 60.º e 61.º do dito Código, um importante leque de direitos e deveres processuais, designadamente, o direito de intervenção no inquérito e na instrução e o direito a recorrer de decisões desfavoráveis.

Ora, *fora do processo penal nunca há arguido*, não estando, assim, assegurado o conjunto de garantias de exercício dos direitos fundamentais associado a esse estatuto.

Por isso, e tendo em mente a intrínseca ligação entre *processo penal* e *garantias constitucionais do arguido*, é fácil compreender que a simples intervenção, ou intermediação, de um grupo de juízes — ainda que tratando-se de magistrados experientes, provindos do Supremo Tribunal de Justiça — no acesso a dados de comunicação e internet por parte dos oficiais de informação do SIRP não é suficiente para conferir a tal processo natureza *criminal*, nem mesmo uma natureza materialmente análoga. De facto, aquela intervenção não assegura a possibilidade de *defesa* dos afetados pela restrição de direitos fundamentais que o acesso aos dados de comunicações necessariamente comporta. Estes afetados desconhecerão, aliás, por completo, na maioria das situações, a existência da intervenção restritiva na sua esfera jurídica individual, uma vez que o poder do executivo é, neste campo, exercido em segredo. Tal circunstância, ainda que possa facilmente justificar-se, aumenta também, de maneira inevitável, o risco de arbitrariedade e de lesão grave daqueles direitos.

Em segundo lugar, e se não bastassem as considerações acima tecidas, uma análise mais atenta do processo de acesso aos *dados de tráfego* de comunicações pelos serviços de informações permite concluir que, apesar de as novas normas terem, claramente, a pretensão de apertar os mecanismos de controlo em relação ao previsto na legislação anterior, a propalada maior exigência de tais mecanismos parece, afinal, na prática, ainda insuficiente, sobretudo se pretendermos a sua equiparação ao processo criminal.

Efetivamente, parte das objeções materiais levantadas por este Tribunal no Acórdão n.º 403/2015 podem repetir-se a propósito das normas em análise:

*(i) Escassa densificação da moldura legislativa*

Assim, atente-se, desde logo, no n.º 1 do artigo 6.º da Lei Orgânica n.º 4/2017, nos termos do qual só se autorizará aos serviços de informações o acesso aos dados em causa "*quando houver razões para crer que a diligência é necessária, adequada e proporcional, nos termos seguintes: a*) *Para a obtenção de informação sobre um alvo ou um intermediário determinado; ou b*) *Para a obtenção de informação que seria muito difícil ou impossível de obter de outra forma ou em tempo útil para responder a situação de urgência*". Esta formulação, que se pretende *garantista*, repete na verdade um elemento que é, por força da Constituição, inerente a toda a atuação do Estado em matéria de direitos fundamentais — o respeito pelo princípio da proporcionalidade. Ao mesmo tempo, atribui um amplo poder discricionário de apreciação da possibilidade de intervenções estaduais restritivas de tais direitos, sem uma moldura normativa suficientemente densificada, visto que o recurso a conceitos imprecisos e indeterminados ("muito difícil de obter de outra forma", "tempo útil") impossibilita a construção de limites legais prévios e claros à concretização das restrições. Nestes termos, a ponderação quanto à proporcionalidade e legitimidade de uma intervenção restritiva de direitos fundamentais por parte dos oficiais do SIRP não se subordina a qualquer critério minimamente preciso ou determinado de distinção entre intervenções lícitas e ilícitas, de que possam socorrer-se os juízes da formação do STJ para decidir acerca da sua autorização.

*(ii) Natureza administrativa do processo, apesar da intervenção de magistrados*

A "formação das secções criminais do Supremo Tribunal de Justiça", que fiscaliza o processo não tem, de igual modo, uma natureza jurídica bem definida. Ainda que tratando-se de um conjunto de juízes, este tipo de atuação parece situar-se fora do âmbito jurisdicional, pelo que estamos perante uma atuação de natureza administrativa e não judicial. Contudo, a transferência da discricionariedade decisória em matéria de acesso aos dados, de órgãos do SIRP para magistrados, se bem que represente um passo positivo em termos de garantias dos cidadãos, dada a experiência e a formação dos juízes Conselheiros do Supremo Tribunal de Justiça, bem como a sua sensibilidade particular em matéria de direitos fundamentais e de processo penal, não é, contudo, passível de provocar a transmutação de um *processo administrativo* num *processo criminal*, pois continua coartada a possibilidade de defesa dos cidadãos contra a ingerência do Estado na sua esfera privada.

*(iii) Indefinição do sentido e alcance do papel do Procurador-Geral da República*

Mais ainda, note-se, no que respeita à intervenção da Procuradora-Geral da República, prevista no n.º 2 do artigo 5.º da Lei Orgânica n.º 4/2017 ("*o processo de autorização de acesso aos dados é sempre comunicado à Procuradora-Geral da República*"), e apresentada como um dos elementos de garantia de respeito pelos direitos fundamentais dos cidadãos, que esta tem escassa relevância prática. Logo, e em definitivo, porquanto a intervenção do MP neste processo não se ajusta ao papel e à função do MP no processo criminal. Além do mais, o seu papel em todo o processo carece de densificação, mesmo após a entrada em vigor da Portaria n.º 237-A/2018, não se compreendendo cabalmente a natureza da sua intervenção, mais ainda quando esta consistiria num dos elementos de equiparação das garantias do acesso aos *dados de tráfego* às garantias do processo penal.

Assim, a Lei prevê que a Procuradora-Geral da República tenha "conhecimento" do pedido de acesso a dados (artigo 9.º), da transmissão diferida desses mesmos dados (artigo 11.º); que seja notificado das decisões de cancelamento de acesso e de destruição dos dados, para efeitos do exercício das suas competências legais (artigo 12.º); e que lhe sejam imediatamente comunicados os dados obtidos que indiciem a prática de crimes de espionagem e terrorismo (artigo 13.º). Do disposto na Portaria n.º 237-A/2018 conclui-se que a Procuradora-Geral poderá pronunciar-se sobre o pedido de acesso (alínea *c*) do n.º 3 do artigo 1.º) e que é informada da deliberação da formação

de juízes do Supremo Tribunal de Justiça sobre o acesso aos dados, podendo reagir, sem que se saiba em que termos (alíneas *f*) e *h*) do n.º 3 do artigo 1.º); tem ainda conhecimento da remessa do ficheiro de resposta com os dados, pelo prestador de serviços de comunicações eletrónicas, podendo também aqui pronunciar-se (alíneas *i*) e *j*) do n.º 3 do artigo 1.º). Desta forma, fica patente a indefinição do papel do Ministério Público no processo de acesso a *dados de tráfego* por parte dos oficiais de informações do SIRP, não sendo claras as suas competências nesta matéria, nem os efeitos jurídicos de eventuais pronúncias da Procuradora-Geral, quando legalmente admissíveis.

*(iv) Dificuldade de exercício do direito de acesso aos dados conservados*

Por último, note-se que o direito de acesso dos cidadãos aos dados processados ou conservados nos centros de dados do SIS e do SIED, que corresponde ao direito fundamental previsto no n.º 1 do artigo 35.º da Constituição, só pode ser exercido através da Comissão de Fiscalização de Dados do SIRP, à luz do n.º 6 do artigo 15.º da Lei Orgânica n.º 4/2017. Ou seja, é um direito que só pode ser efetivado nos termos do artigo 26.º da Lei n.º 30/84, sendo, nos termos legais, da exclusiva competência da Comissão de Fiscalização de Dados do SIRP. Esta atua, assim, como intermediário entre o cidadão e os serviços de informações, e desempenha as suas funções de fiscalização através de verificações periódicas dos programas, dados e informações por amostragem, fornecidos sem referência nominativa; e, igualmente, pelo acesso a dados e informações com referência nominativa (particularmente quando a Comissão entenda estar perante denúncia ou suspeita fundamentada da sua recolha ilegítima ou infundada). A Comissão de Fiscalização deve ordenar o cancelamento ou retificação de dados recolhidos que envolvam violação dos direitos, liberdades e garantias consignados na Constituição e na lei e, se for caso disso, exercer a correspondente ação penal. Contudo, e como se assinala no Parecer da CNPD acima mencionado, "*não se impõe aos Diretores do SIS e do SIED um dever de colaboração e de prestação de todas as informações que lhes forem solicitadas (como sucede, por exemplo, no artigo 24.º, n.º 1, da LPDP), mas antes a mera prestação de um especial apoio, não estando por isso afastado que a natureza secreta da atividade do SIRP justifique a negação da prestação de qualquer informação*".

11.1.3 — Ante o que fica dito, pode afirmar-se que, além de o procedimento de acesso a dados de comunicações e de internet por parte dos oficiais de informações do SIRP não ser, natural e obviamente, um *processo criminal* do ponto de vista formal, também dele é muito distinto do ponto de vista material e garantístico.

Na verdade, é de afastar uma interpretação jurídico-constitucional segundo a qual pudesse arredar-se o elemento literal do n.º 4 do artigo 34.º da Constituição, e admitir a existência, nesta matéria, de uma restrição a um direito fundamental não expressamente autorizada pela Constituição, cujo escrutínio se centraria, por parte do Tribunal Constitucional, num mero juízo de proporcionalidade, nos termos do artigo 18.º da Constituição, atentos os direitos e valores constitucionais conflituantes cujo equilíbrio se procura. São demasiado patentes as divergências em relação ao processo criminal, tal como é concebido no nosso Estado de direito democrático, para que possa cabalmente sustentar-se essa posição.

Note-se, no entanto, que o Tribunal Constitucional não ignora que esta é uma matéria na qual, tal como na questão mais lata da interferência nas comunicações privadas em sede de processo penal, e por maioria de razão, ecoam "*com particular ressonância, as antinomias político-criminais de fundo, subjacentes a todo o direito das proibições de prova*"; não se olvida, igualmente, que neste campo "*releva sobremaneira daquela 'dramatização da violência e da ameaça' (HASSEMER) induzida nas representações coletivas pela mais recente explosão do crime organizado,* maxime *do terrorismo e do tráfico de estupefacientes*" (Manuel da Costa Andrade, *Sobre as proibições de prova em processo penal*, Coimbra Editora, 1992, p. 281).

E não ignora, igualmente, que neste tipo de matéria se impõe a consideração do dever estadual de garantir a segurança, que decorre do n.º 1 do artigo 27.º da Constituição. Contudo, o Tribunal Constitucional é o garante *de um determinado parâmetro constitucional*, em que muitas das ponderações entre direitos e valores constitucionais potencialmente em conflito foram já levadas a cabo pelo legislador constituinte. Não lhe cabe, pois, no quadro de um Estado de direito democrático, substituir-se-lhe, pelo que deve, na questão ora em análise, respeitar-se a operação de *concordância*

*prática* realizada pelo legislador e consagrada no n.º 4 do artigo 34.º da Constituição, porque foi esta a opção do poder constituinte democraticamente legitimado.

11.2 — *O acesso a dados de tráfego que não envolvem comunicação intersubjetiva*

Importa agora analisar a constitucionalidade, à luz dos artigos 26.º, n.º 1 e 35.º, n.os 1 e 4, ambos da Constituição, do segmento ideal do artigo 4.º que se refere ao acesso aos dados de tráfego, que não envolvem uma comunicação intersubjetiva, pois o conhecimento destes dados pelo SIS e pelo SIED representa, necessariamente, uma mais intensa devassa da vida privada do que o acesso aos dados de base ou a dados de localização, previstos no artigo 3.º

Na avaliação da extensão da ingerência necessária à proteção de outros bens constitucionais deve começar por se analisar se o grau de danosidade causado pelo acesso e tratamento desta específica categoria de dados de tráfego difere substancialmente da intensidade da intromissão e devassa que o acesso aos demais dados de tráfego incluídos na previsão daquele artigo 4.º provoca à privacidade e à autodeterminação informacional do titular dos dados.

Não obstante aqueles dados não se reportarem a concretas e efetivas comunicações realizadas ou tentadas entre pessoas, mas apenas entre pessoas e máquinas ou até mesmo entre máquinas (*machine-to-machine communications*) proporcionadas por "*agentes de software*", a verdade é que podem assentar nos mesmos dados de base dos segundos e, tal como estes, possibilitar a monitorização, vigilância e controlo de movimentos de pessoas, assim como a construção de perfis de utilizadores que comportam riscos evidentes de perda de privacidade. Com efeito, a recolha e tratamento de "dados de navegação" na internet, ainda que não seja em tempo real ou através de acesso à totalidade dos dados armazenados pelos prestadores de serviços de comunicações eletrónicas, possibilita conhecer as escolhas, comportamentos, hábitos, inclinações, gostos, vivências e centros de interesse do titular dos dados, e com base neles, avaliar e tipificar o seu comportamento e as suas particularidades. Por isso, tal como se verifica com a recolha e tratamento dos dados de uma autêntica comunicação interpessoal, em que é evidente e significativa a perda de privacidade dos respetivos interlocutores, o conhecimento e tratamento do rasto das marcas e sinais que a ligação à internet deixa atrás de si pode causar equivalente prejuízo à privacidade da pessoa em causa.

De facto, com exceção dos dados necessários para encontrar e identificar o destinatário do correio eletrónico através da internet ou de uma comunicação telefónica através da internet, o tratamento dos demais dados de tráfego de internet afeta as mesmas dimensões da privacidade e proteção de dados pessoais, qualquer que seja a utilização que se tenha da internet. Em ambos os modos de utilização, comunicações intersubjetivas e comunicações de massa, o tratamento não consentido dos respetivos dados de tráfego põe em causa valores e interesses do utilizador, tais como *(i)* a confiança que tem na segurança e reserva dos sistemas informáticos do fornecedor do serviço de acesso à internet; *(ii)* o interesse em decidir, ele mesmo, acerca da utilização que poderá ser efetuada das suas informações pessoais; *(iii)* o interesse em não ser sujeito a decisões exclusivamente automatizadas dos seus dados; *(iv)* o interesse em conhecer, dispor, controlar, atualizar, corrigir ou apagar os dados pessoais que lhe digam respeito; *(v)* o interesse em conhecer a finalidade do tratamento dos seus dados *(vi)* o interesse na não divulgação de dados objeto de tratamento.

Daí que, face à semelhança dos valores e interesses afetados pelo tratamento não consentido de ambas as categorias de dados de internet e ao equivalente grau de danosidade que ele pode causar ao utilizador, a densidade de escrutínio a aplicar pela jurisdição constitucional à avaliação da escolha legislativa não possa ser menor em alguns deles. Ainda que se admita que nem todos os dados de internet constantes da previsão do artigo 4.º da Lei Orgânica n.º 4/2017, de 25 de agosto, estejam abrangidos pela mesma área de tutela que a Constituição reserva às comunicações eletrónicas, o seu tratamento não autorizado pode contender diretamente com os mesmos bens jurídico-constitucionais. À semelhança do que acontece com o sigilo das telecomunicações assegurado no n.º 4 do artigo 34.º da Constituição, também aqui o que está em causa é assegurar o livre desenvolvimento da personalidade e a privacidade de cada um através da utilização da internet à margem da publicidade. Por causa disso, a densidade de escrutínio terá que ser tanto maior quanto mais evidente, ou manifesta, for a inexistência de fundamento para um regime diferenciado de intromissões com referência aos dados de internet.

11.2.1 — É certo que, como vimos, a Constituição consagra um regime diferenciado de intromissão nos dados de internet: de acordo com a previsão do artigo 34.º, n.º 4, da Constituição, os dados de tráfego relativos a comunicações entre pessoas estão abrangidos pela área de tutela da inviolabilidade das telecomunicações, existindo uma autorização constitucional *especial* para a ingerência das autoridades públicas nesse domínio, circunscrita apenas a matéria de *investigação criminal;* já os dados de tráfego na internet que não envolvam comunicações interpessoais, na medida em que permitem identificar o nome, morada e outros dados de identificação do utilizador, são considerados "*dados pessoais*" protegidos apenas pelas *normas gerais* do artigo 35.º da CRP, que admitem restrições em domínios que podem extravasar o âmbito da investigação criminal.

Não há dúvida de que, no que concerne aos dados de tráfego no âmbito das comunicações intersubjetivas, incluindo os dados de internet, a tutela especial da *autodeterminação comunicativa* afasta ou dispensa a tutela geral da *autodeterminação informativa*; e quanto aos dados de tráfego de internet fora desse âmbito, é convocável apenas esta última tutela geral.

Daqui não decorre, contudo, que as dimensões da privacidade e da proteção de dados pessoais dos utilizadores eventualmente em causa tenham menor merecimento constitucional do que aquelas que também podem ser lesadas no âmbito das comunicações interpessoais. E, por isso, a intensidade de escrutínio exigida, apesar da diferença dos parâmetros constitucionais em causa, não pode deixar de ser similar ou equivalente.

Na verdade, se a Constituição autoriza o tratamento não consentido de dados de tráfego relativos a comunicações entre pessoas, dir-se-á que também não exclui a invasão de dados de tráfego que não dão suporte a autênticas comunicações, uma vez que nesse caso a perda de privacidade não atinge uma das dimensões daquela outra (a privacidade das comunicações). Mais: a razão de ser da legitimidade constitucional da ingerência relativa aos dados de tráfego não estará tanto na diferente categoria de dados — pressuporem ou não um ato de comunicação intersubjetiva —, mas sobretudo nas especificidades em termos de interesse público e de garantias próprias do domínio em que a restrição pode atuar: a *investigação criminal*.

11.2.2 — Sucede que a atividade da entidade pública que pretende o acesso aos dados de tráfego da internet que não respeitam a comunicações intersubjetivas — o SIRP — e a finalidade a que os mesmos se destinam situa-se no domínio da *prevenção*: «*informações necessárias à prevenção de atos de espionagem e do terrorismo*». A produção de informações necessárias à preservação da segurança interna e externa, bem como à independência e interesses nacionais e à unidade e integridade do Estado, em princípio, está dissociada da prevenção e investigação criminais em sentido estrito, não podendo os serviços de informação praticar quaisquer atos da competência dos órgãos de polícia criminal ou das autoridades judiciárias ou lesivos dos direitos, liberdades e garantias dos cidadãos (artigos 3.º e 4.º da Lei n.º 30/84, de 5 de setembro, alterada por último pela Lei n.º 4/2014, de 13 de agosto; v. também *supra* o ponto 11.1.2. e o ponto 19 do Acórdão n.º 403/2015).

No contexto da Lei Orgânica n.º 4/2017, de 25 de agosto, a natureza preventiva da atividade de recolha e tratamento de dados de tráfego surge reforçada, já que, se no âmbito da mesma se indiciar a prática de crimes de espionagem e terrorismo, estes têm que ser *imediatamente* comunicados ao Ministério Público (artigo 13.º). O acesso a essa categoria de dados — que integram o conceito de dados pessoais — também permite prognosticar a ocorrência desse tipo de crimes ou identificar pessoas relativamente às quais existam indícios de que os cometeram ou de que se preparam para os cometer. Trata-se, pois, de uma atividade que possibilita obter "informações" através de atos que contendem com direitos, liberdades e garantias, e que se integra num conceito amplo de prevenção criminal, uma "fase prévia" à própria prevenção criminal a cargo da polícia, e que, por isso mesmo, comporta acrescidos riscos de erro de prognose, dada a incerteza de que se reveste o fenómeno do terrorismo.

11.2.3 — A prevenção de crimes como função da polícia de segurança e da polícia judiciária tem respaldo constitucional no n.º 3 do artigo 272.º da Constituição, com os seguintes limites: «*só pode fazer-se com observância das regras gerais sobre polícia e com respeito pelos direitos, liberdades e garantias dos cidadãos*». Como já foi referido no Acórdão 403/2015, a atividade do SIRP — serviço que faz parte das forças e serviços de segurança (alínea *c*) do n.º 2 do artigo 25.º

da Lei n.º 53/2008, de 29 de agosto — Lei de Segurança Interna — LSI) —, também está abrangida por este preceito constitucional (cf. o respetivo ponto 19).

E dele resulta que «as medidas de prevenção de crimes serão apenas medidas de proteção de pessoas e bens, vigilância de indivíduos e locais suspeitos, mas não podem ser medidas de limitação dos direitos, liberdades e garantias dos cidadãos» (Gomes Canotilho e Vital Moreira, *Constituição da República Portuguesa Anotada,* 4.ª ed. Vol. II, p. 861).

Por regra, as leis infraconstitucionais que definem a atividade material da polícia de segurança pública, da polícia criminal ou dos órgãos de polícia criminal diferenciam as funções de *prevenção* das funções de *investigação criminal* através de um critério temporal: a aquisição da notícia da prática do crime é condição *sine qua non* para o início da investigação criminal. Desde logo, o artigo 1.º da Lei n.º 49/2008, de 27 de agosto — Lei de Organização da Investigação Criminal — começa por definir investigação criminal como «o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a suas responsabilidade e descobrir e recolher provas, no âmbito do processo»; depois, as várias leis orgânicas das polícias, além de atribuírem competência para a prática de atos dentro de um processo penal, enquanto órgãos coadjuvantes das autoridades judiciárias, definem os poderes que lhes cabem no âmbito da prevenção criminal *extradelictum* ou *post-delictum* (artigos 3.º e 4.º da Lei n.º 37/2008, de 6 de agosto — Lei Orgânica da Polícia Judiciária); por fim, tipificam-se as "medidas cautelares ou de polícia", administrativas ou processuais penais, que as polícias podem tomar por *iniciativa própria* (artigos 28.º e 29.º da LSI e artigos 248.º a 253.º do Código de Processo Penal).

Ora, como a generalidade das polícias com funções de investigação criminal, desenvolvida nas fases de inquérito ou de instrução de um processo penal, também detêm funções de prevenção quanto às infrações relativas às suas competências, por vezes, verificam-se dificuldades de caraterização e diferenciação entre estes dois domínios, tanto mais delicadas quanto é certo que as regras a observar consoante se atua no domínio da prevenção ou no da investigação, não são — ou podem não ser — as mesmas. O critério formal e tradicional de distinção entre prevenção e investigação, assente no *tempo* de intervenção das autoridades, perde os seus contornos claros. Os meios ocultos de investigação, mesmo quando partem do processo penal, podem descobrir "crimes" possíveis ou prováveis ou perigos suscetíveis de vir a atualizar-se. Uma prevenção criminal positiva ou pró-ativa, como aquela que o Estado pretende para combater as novas formas de criminalidade organizada, não espera pela prática do crime para começar a investigar e recolher provas. Daí que, em certos casos, a colheita de informação mesmo antes de surgir o *fumus commissi delicti,* para ser valorada num futuro processo penal, possa consubstanciar uma "investigação de campo avançado", ou de um *tertium genus* ou terceira tarefa da polícia, materialmente elevada ao estatuto de investigação própria do processo penal (cf. Costa Andrade, ob. cit., "Bruscamente no verão passado", a reforma do Código de Processo Penal", pág. 324).

Seja como for, a verdade é que o procedimento de recolha de informações através de dados de tráfego, previsto no questionado artigo 4.º da Lei Orgânica n.º 4/2017, não está orientado para uma atividade *investigatória* de crimes praticados, nem visa reunir «*provas*» do planeamento de crimes organizados de terrorismo. Nos termos em que o acesso aos dados de tráfego está regulado no diploma, com os pressupostos previstos no seu artigo 6.º, não se trata de finalidade de investigação criminal, mas apenas de acumulação funcional de informação por razões preventivas, ou seja, uma atividade exclusivamente inserida na função preventiva.

Ora, o *princípio da proporcionalidade* preceitua que este poder do Estado, no acesso a dados pessoais dos cidadãos, além de exigir um fundamento, preciso e determinado, na lei — *princípio da determinabilidade* —, não pode ser utilizado para além do estritamente necessário. Não basta que tenha um conteúdo suficientemente definido na lei, impõe-se ainda que obedeça aos requisitos da necessidade, exigibilidade e proporcionalidade (ou proibição do excesso). Com efeito, decorre do artigo 272.º da Constituição a preocupação de limitar e vincular as medidas policiais restritivas dos direitos fundamentais, as quais «só serão legítimas se *idóneas* (próprias para a eliminação de perigo), *necessárias* (necessidade de eliminar um perigo grave e atual de «desordem»), *proporcionais* (proporção entre o sacrifício dos direitos e o resultado), tempestivas e de duração limitada ao perigo» (cf. Vieira de Andrade, *Direitos Fundamentais, na Constituição Portuguesa de 1976,* 5.ª ed., p. 333).

As ações de prevenção da polícia devem traduzir-se, assim, em medidas de defesa contra perigos concretos. Com efeito, a probabilidade/previsibilidade de ocorrência de situações potencialmente lesivas para bens jurídicos cuja proteção se encontra a cargo do Estado reclama medidas necessárias para as evitar — negar tal afirmação significa exonerar as autoridades estaduais de uma das suas tarefas primordiais: garantir a segurança de pessoas e bens. Por isso, as medidas preventivas pressupõem habilitações legais de ingerência contra situações de perigo, entendido no sentido de «ameaça objetiva de lesão imediata de bens jurídicos por condutas individuais ilegais particularmente suscetíveis de a gerar numa situação concreta» (Sérvulo Correia, *O Direito de Manifestação — Âmbito de Proteção e Restrições, Coimbra*, 2006, p. 98).

Deve notar-se, contudo, que, como os serviços de informação não são órgãos policiais, revestindo-se a sua atividade de uma natureza secreta e não observável pelos cidadãos afetados, a norma constante do artigo 4.º deve estar sujeita a um rigoroso controlo de constitucionalidade.

Assim, o princípio da necessidade, uma das dimensões do princípio da proibição do excesso, impõe que o acesso aos dados de tráfego lesivo da autodeterminação informativa se destine a reagir a situações de *perigo suficientemente indiciadas*, ou seja, a situações em que se nada for feito para o evitar, bens constitucionalmente protegidos — como a vida, a liberdade e a integridade pessoal ou a independência e a integridade nacionais — serão provavelmente lesados.

Ora, no âmbito das ações de prevenção criminal, a lei não tem previsto intromissões nas comunicações eletrónicas: o acesso ao conteúdo das comunicações só pode ser autorizado no "inquérito" ou em qualquer outra fase do processo penal (artigos 187.º e 189.º do CPP e artigo 18.º da Lei n.º 109/2009, de 15 de setembro, relativo ao domínio do cibercrime). Por via disso, o tratamento de dados pessoais para fins de investigação criminal «deve limitar-se ao necessário para prevenção de um *perigo concreto* ou repressão de uma infração determinada» (n.º 3 do artigo 8.º da anterior Lei n.º 67/98, de 26 de outubro — LPDP); e a conservação e transmissão de dados têm por «finalidade exclusiva a *investigação* deteção e repressão de crimes graves» (n.º 1 do artigo 3.º da Lei n.º 32/2008, de 17 de julho).

De um modo geral, pode afirmar-se que a "concordância prática" entre os valores constitucionais de perseguição e punição do crime com os direitos fundamentais deve ser feita em sede de processo penal. Qualquer ação preventiva que interfira, no sentido de os comprimir ou devassar, com direitos, liberdades e garantias, não pode ter lugar fora de um processo criminal devidamente formalizado, porque «é evidente que uma atuação investigatória processualizada e publicizada, na forma de *inquérito preliminar* ou de *instrução*, não só salvaguarda a liberdade e segurança no decurso do processo como dá garantia de que a prova para ele canalizada foi obtida com respeito pelos direitos fundamentais. A mesma conclusão não se pode extrair de uma *ação de prevenção* não processualizada ou mesmo não suficientemente formalizada, coberta pelo segredo de Estado, que decorre na total ausência de instrumentos defensivos que comportem um mínimo de dialética processual*»* (Acórdão n.º 403/2015, ponto 19).

11.2.4 — Simplesmente, a norma do artigo 4.º da Lei Orgânica n.º 4/2017, enquadrada no respetivo regime jurídico, afasta-se claramente deste paradigma.

A necessidade do acesso aos dados de tráfego funda-se em dois pressupostos alternativos, mencionados no artigo 6.º: *(i)* obtenção de informação de um alvo ou um intermediário determinado; *(ii)* impossibilidade ou dificuldade em obter a informação por outra forma ou em tempo útil para responder a uma situação de urgência. A ação preventiva modela-se assim por uma abertura de conceitos (*"alvo determinado",* "*situação de urgência",* "*muito difícil de obter"*, "*tempo útil"*), semanticamente maleáveis e insuficientemente determinados, no âmbito dos quais a incerteza sobre os pressupostos de acesso aos dados de tráfego é bastante grande, atendendo à singularidade de cada caso concreto.

Com efeito, a intromissão nesta categoria de dados depende unicamente da existência de um alvo determinado e da impossibilidade ou dificuldade de em tempo curto obter informações através de meios abertos. O apuramento de um «alvo» ou a avaliação de uma «situação de urgência» depende da existência material de pressupostos de facto totalmente escolhidos pelos serviços de informação e do juízo valorativo que sobre eles faça. O mesmo se passa, aliás, com a própria *conexão* da informação visada pelo pedido de acesso (seja sobre o "alvo" ou outra informação não especificada) e a prevenção de atos de espionagem ou de terrorismo: os factos que suportam

tal pedido, as finalidades que o fundamentam e as razões que aconselham o mesmo acesso são aqueles que os serviços entenderem dever indicar no pedido de autorização [cf. o artigo 9.º, n.º 2, alínea *b*), da Lei Orgânica n.º 4/2017]. Consequentemente, a *relevância dos fundamentos do pedido*, que, enquanto fator de ponderação da decisão dos juízes, limita a salvaguarda dos direitos fundamentais concretamente em causa (cf. o artigo 5.º, n.º 1, do mesmo diploma), também só pode ser apreciada em função do que os próprios serviços enunciarem no pedido que apresentem. Deste modo, qualquer cidadão pode ser potencialmente referenciado como alvo, assim como qualquer situação poderá ser configurada como urgente. Tudo depende do juízo de prognose ou da avaliação que os serviços de informação façam da situação concreta vivida.

Na definição do cidadão alvo da medida, a lei não indica critérios objetivos para a seleção, relacionados com a probabilidade de as pessoas visadas estarem envolvidas direta ou indiretamente na preparação ou execução de ataques terroristas, ou uma relação, pelo menos indireta, com atos de criminalidade grave, nomeadamente a espionagem, não passando a norma, também neste ponto, o teste da proporcionalidade, por falta de densificação do regime jurídico que lhe serve de pressuposto.

Ora, tendo em conta que o fenómeno da prevenção se basta com uma suspeita, que pode ser vaga, em relação ao indivíduo a cujos dados pessoais se pretende obter acesso, podendo ser suficiente, para fundar tal acesso, uma relação meramente aparente, espacial ou circunstancial (critério geográfico), com pessoas suspeitas ou a sua presença em locais ou contextos normalmente associados a atentados terroristas (aeroportos, viagens em determinados países estrangeiros), tem de se reconhecer que os poderes que a lei confere ao Estado no domínio da prevenção de atos de terrorismo ou de espionagem podem atingir, pelo menos potencialmente, qualquer pessoa, sem que esta tenha consciência disso ou tenha qualquer poder de reação *a posteriori* para pedir a destruição dos dados e responsabilizar as entidades que a eles tiveram acesso ou que os forneceram aos serviços de informação, sem qualquer indício ou relação de causalidade com atos correspondentes à prática dos mencionados crimes. Encontramo-nos, pois, perante situações em que o indivíduo perde o controlo sobre a circulação dos seus dados pessoais e em que claramente pode ser violado o seu direito à autodeterminação informativa, sendo transformado em «objeto de informações».

Dada a sensibilidade da questão para os direitos fundamentais, deve entender-se que os pressupostos substanciais da ação de intromissão nos dados de tráfego não se revestem de suficiente densidade na lei, ou seja, não estão preordenados à prevenção de *perigos* cuja ameaça assente em circunstâncias de facto, normativamente descritas, para bens jurídicos de importância transcendente para o indivíduo e para a comunidade organizada em Estado de direito. Nos termos difusos e indeterminados que resultam da articulação do artigo 4.º com o referido artigo 6.º, cabe aos serviços de informações escolher os elementos da situação concreta relevantes para o acesso aos dados de tráfego, não resultando da lei que o acesso apenas deve ocorrer perante a existência, no caso concreto, de uma situação em que, com probabilidade bastante, e num tempo relativamente próximo, ocorrerá um dano para bens jurídicos ou para direitos fundamentais de relevância transcendente para os cidadãos e para toda a comunidade. A autorização legal para a invasão legítima nos dados de tráfego não integra sequer como pressuposto um determinado grau de *suspeita* da prática dos crimes de espionagem e terrorismo, nem o *perigo* ou a *suspeita de perigo concreto* está enunciado na lei como objeto possível da ação preventiva. Com efeito, daquele preceito não resulta expresso que a recolha da informação tenha por objeto *notícias de factos suscetíveis de fundamentar suspeitas de perigo da prática de determinados crimes* contra um número circunscrito de bens jurídicos fundamentais para a comunidade.

A necessidade de intervenção em matéria de direitos, liberdades e garantias tem que figurar formalmente como pressuposto da ação preventiva. A existência de um determinado alvo ou de uma situação de urgência, sem especificação de diretrizes que balizem a escolha dos elementos relevantes à deteção do alvo ou à qualificação da situação como urgente, não permite avaliar, por si só, a necessidade da intromissão e devassa dos dados de tráfego. Sem a fixação legal de tais orientações, o acesso aos dados de tráfego tanto se pode fundar numa defesa contra perigos como numa antecipação de riscos. É evidente que, para justificar uma ação preventiva à luz da proporcionalidade, um perigo pressentido, mas não comprovável, não tem o mesmo peso valorativo

que um perigo concreto e suscetível de demonstração objetiva. Naturalmente que os riscos sem potencial de perigosidade conhecido — as meras suspeitas de perigo — são mais tolerados pela comunidade do que as situações de perigo iminente, não constituindo os primeiros, por isso, um fundamento legítimo para as restrições a direitos fundamentais, dada a necessidade de respeitar um mínimo de liberdade.

Daí que as normas atributivas do poder de defesa contra perigos tenham que estabelecer com precisão e densidade suficiente os *pressupostos* que fundamentam a necessidade de tomar medidas de prevenção ou de ingerência. Acolhendo-nos à fundamentação do Tribunal Constitucional alemão, quando estão em causa intromissões em direitos fundamentais assentes em "juízos de prognose", exige-se que as "*pertinentes autorizações legais contenham elementos tipificadores limitadores da ação".* Isto para que "*a limitação do âmbito da intromissão autorizada* [...] *permita tornar tolerável, em matéria de direitos fundamentais, o risco de uma prognose errada"* (*BVerfGE*, 110, 33, 57 e 60).

No mesmo sentido, a jurisprudência do TJUE exige que a regulamentação nacional contenha normas claras e precisas que indiquem em que circunstâncias e em que condições materiais e processuais os prestadores de serviços de comunicações eletrónicas devem conceder às autoridades nacionais acesso aos dados, não podendo a legislação nacional limitar-se a remeter para os objetivos gerais do artigo 15.º, n.º 1, da Diretiva 2002/58 (cf. TJUE *Acórdão Tele 2,* n.os 117 e 118 e *Digital Rights,* n.º 61). De acordo com a jurisprudência do TEDH e do TJUE, só pode ser concedido o acesso de uma autoridade pública a dados de comunicação ou de tráfego, mediante critérios determinados e objetivos, definidos numa lei clara e detalhada nos seus termos, acessível e de efeitos previsíveis para os cidadãos, e relativa a pessoas suspeitas de estarem a planear ou terem planeado, de estarem a cometer, ou terem cometido um ato terrorista, ou de estarem, de algum modo, envolvidas nessa infração (TJUE *Tele 2* n.º 119, TEDH *Zakharov v. Russia*, §260).

A ausência ou indeterminação normativa desses pressupostos possibilita intervenções restritivas em situações cuja potencialidade lesiva não obriga à adoção de medidas preventivas. A possibilidade de se tomarem medidas preventivas sem especificação das condições substanciais do seu exercício, constituiria um agravo imprevisível para os cidadãos, sem qualquer compensação de certeza e segurança. Como refere Reis Novais, «uma restrição de contornos não antecipadamente bem firmados alarga potencialmente a margem de atuação restritiva dos poderes constituídos a um plano não consentâneo com o princípio de *repartição* de Estado de Direito e de proibição do excesso e gera efeitos inibitórios no *lado* do exercício das liberdades» (*Os Princípios Constitucionais Estruturantes da República Portuguesa*, Coimbra Editora, 2004, p. 192).

A norma do artigo 4.º da Lei Orgânica n.º 4/2017 versa sobre matéria de reserva de lei parlamentar: direitos, liberdades e garantias (artigos 165.º, n.º 1, alínea *b*), e 18.º n.º 2, ambos da Constituição). Nestas matérias, designadamente no domínio utilização da informática relativamente ao tratamento de dados pessoais, a lei deve prever e prescrever de forma clara e precisa o quadro de circunstâncias em que as intervenções restritivas podem ser tomadas, não podendo ser redigida em termos tão latos que possa ser interpretada como incluindo, na sua previsão, a liberdade de escolha dos pressupostos que justificam a necessidade da intervenção. Uma lei vaga, imprecisa e demasiado abrangente converteria as medidas restritivas em arbítrio, por ausência de critérios objetivos quanto à razão de ser da sua utilização.

Tanto mais que, neste caso, o acesso aos dados de tráfego representa uma intromissão sem que os respetivos titulares tenham conhecimento do facto nem dele se apercebam, ou sem que possam reagir durante a sua execução, ou mesmo no seu termo, já que dele não são notificados, nem se prevê quaisquer atos ou procedimentos que permitam o conhecimento ou cognoscibilidade da intromissão pelos interessados, contrariamente ao exigido pelo Tribunal de Justiça: *«importa que as autoridades nacionais competentes às quais foi concedido o acesso aos dados conservados informem desse facto as pessoas em causa, no âmbito dos processos nacionais aplicáveis, a partir do momento em que essa comunicação não seja suscetível de comprometer as investigações levadas a cabo por essas autoridades»*, já que essa informação é indispensável ao acionamento por tais pessoas da proteção jurisdicional efetiva dos seus direitos neste domínio, nomeadamente o direito à retificação ou à eliminação dos dados em causa (cf. o Acórdão *Tele2*, n.º 121, e o Acórdão *Schrems*, C-362/14, EU:C:2015: 650, n.º 95).

Tal como decidiu o TEDH, no seu Acórdão de 6 de junho de 2006 (caso *Segrstedt — Wiberg e outros c. Suécia,* pedido n.º 62332/00), «*nestes casos, o risco de arbitrariedade é, naturalmente maior; porque as medidas de vigilância secreta não são suscetíveis, pela sua natureza, de ser controladas pelo público em geral nem são conhecidas dos indivíduos visados, a lei deve indicar, com precisão e suficiente clareza, o âmbito desse poder discricionário conferido às autoridades nacionais competentes, e o modo como deve ser por elas exercido, concedendo-se, assim, ao particular a defesa contra ingerências arbitrárias nos seus direitos*».

Não é, pois, qualquer alvo ou carência urgente de informação que legitima uma lei restritiva do direito à autodeterminação informativa dos dados de tráfego.

Como se disse, a recolha de informações através de dados de internet só está em conformidade com a autodeterminação informacional quando se verificam situações face às quais seja possível um *juízo materialmente fundado de prognose* de ocorrência do perigo para um número circunscrito de bens jurídicos de importância extrema para a comunidade, como a vida, corpo e a liberdade das pessoas, ou a segurança do Estado de direito. O princípio da proporcionalidade impõe que o Estado invoque uma situação de *perigo previsível, concreta e de verificação altamente provável*, justificando os juízos de prognose através da *identificação normativa da situação fáctica* que está na origem do perigo, a possibilidade de ocorrência de eventos lesivos num prazo próximo e a relação da situação de perigo com pessoas determinadas.

Todavia, os enunciados normativos retirados do artigo 4.º em articulação com o preceituado no artigo 6.º da Lei Orgânica n.º 4/2017 não respondem a estas exigências. Tal como estão formulados os pressupostos da intromissão, existe a possibilidade de acesso a esses dados em situações indefinidas, em eventos de verificação mais ou menos improvável, sem qualquer referência de circunstâncias de facto, caso em que é impossível evitar o arbítrio.

É evidente que o Estado, para salvaguarda de valores sociais inquestionáveis, como a segurança pública ou o perigo público de ações terroristas, pode e deve tomar medidas preventivas.

E foi com esse objetivo que a LSI criou a Unidade de Coordenação Antiterrorismo (UCAT), na dependência do Secretário-Geral de Sistema de Segurança Interna, composto pelos representantes de vários serviços, entre os quais o Secretário-Geral do SIRP e dos diretores do SIED e do SIS, cuja função principal é a «coordenação e partilha de informações, no âmbito do combate ao terrorismo», que foi posta em funcionamento pelo Decreto Regulamentar n.º 2/2016, de 23 de agosto. Porém, a ação deste serviço e das polícias que o integram move-se sobretudo no campo avançado da antecipação, avaliação e gestão de riscos do terrorismo, um domínio em que, devido à incerteza que encerra, é excessivo restringir o direito fundamental à autodeterminação informativa.

No juízo de proporcionalidade sobre as medidas restritivas tem que ser equacionado o risco de, sob a capa da luta contra o terrorismo e a espionagem, os cidadãos serem reduzidos a *identidades digitalmente criadas* e *heteroconstruídas,* baseadas em perfis definidos por terceiros, com a consequente desumanização das pessoas e estandardização dos seus comportamentos, aniquilando-se a privacidade e condicionando-se a liberdade, assim acabando por perverter a democracia. O desvalor do sacrifício imposto à liberdade dos cidadãos assume aqui um especial peso na análise da relação meio-fim inerente ao teste da proporcionalidade

Entende-se, pois, que a ação de prevenção prevista no artigo 4.º da Lei Orgânica n.º 4/2017, de 25 de agosto, tal como articulada com as condições de admissibilidade previstas no artigo 6.º do mesmo diploma e tendo em conta a insuficiência dos meios de reação dos cidadãos contra intervenções ilícitas, desequilibra desrazoavelmente a ponderação de meio-fim ínsita na vertente apontada do princípio da proporcionalidade, violando o direito à autodeterminação informativa, consagrado nos artigos 26.º, n.º 1 e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2, da CRP.

12 — A questão da constitucionalidade do artigo 3.º da Lei Orgânica n.º 4/2017

Como já foi dito e se repete, não se aplicando o artigo 34.º, n.º 4, da Constituição, ao domínio coberto por aquele artigo 3.º, a constitucionalidade desta norma deve ser apreciada com base nos artigos 26.º, n.º 1 (direito ao desenvolvimento da personalidade e à reserva de intimidade da vida privada) e 35.º, n.os 1 e 4 (proibição de acesso a dados pessoais) da Constituição. Os dados a que a norma do artigo 3.º da Lei Orgânica n.º 4/2017 permite acesso são «dados pessoais de terceiros», para efeitos do artigo 35.º, n.º 4, da Constituição, abrangidos, portanto, por um princípio de proibição do acesso, em que sobressai sobretudo a vertente negativa de defesa perante o Estado.

O direito à autodeterminação informativa abrange uma proteção mais ampla do que a simples reserva da vida privada, incluindo os dados pessoais dos indivíduos, ainda que autonomizados de concretos atos de comunicação, cuja possibilidade de devassa aumenta exponencialmente com o progresso tecnológico, e que refletem, por exemplo, os hábitos de vida de um indivíduo, os locais que frequenta, os seus gostos, a sua saúde, a forma como passa os tempos livres, a conduta e as características do utilizador ou até traços fundamentais da sua personalidade. O acesso pelos SIRP a dados dessa natureza condiciona a autodeterminação informativa dos cidadãos a que esses dados digam respeito — uma das refrações da tutela constitucional do livre desenvolvimento da personalidade — e constitui uma ameaça de invasão da privacidade dos visados.

Conforme se afirma no ponto 13 do Acórdão n.º 403/2015, o *direito à autodeterminação informativa* consagrado no artigo 35.º da Constituição, com vista à proteção das pessoas perante o tratamento de dados pessoais informatizados, não se reporta, como o *direito à autodeterminação comunicativa,* a *comunicações individuais* efetivamente realizadas ou tentadas, estas já protegidas pelo sigilo de comunicações. «Naquele outro direito protege-se as *informações pessoais* recolhidas e tratadas por entidades públicas e privadas, cuja forma de tratamento e divulgação pode propiciar ofensas à privacidade das pessoas a que digam respeito. [...] Neste caso, pretende-se impedir que as informações prestadas a um particular ou a uma entidade possam por estes ser divulgadas a outras pessoas ou entidades, ou seja, que a pessoa se torne "simples objeto de informações", face a todos os registos informáticos que vai deixando no seu dia a dia. A proibição de ingerência ou devassa neste domínio implica não apenas a proibição de acesso a terceiros aos dados pessoais, mas ainda a proibição de divulgação ou mesmo de interconexão de ficheiros com dados da mesma natureza».

Contudo, como se referiu, estes direitos podem ser objeto de restrições por via legislativa — as leis restritivas de direitos, liberdades e garantias. Nalgumas normas constitucionais, a Constituição autorizou a lei ordinária a restringir determinados direitos em alguns aspetos ou para algumas finalidades, noutras atribuiu ao legislador expressamente uma competência de regulação geral da matéria que inclui poderes de restrição. Assim, no que respeita ao direito consagrado no artigo 35.º, n.º 4, a Constituição prevê expressamente a possibilidade da sua restrição, no inciso final «salvo em casos excecionais previstos na lei», mas não indica os seus pressupostos ou finalidades. Porém, a restrição terá de observar, para além da reserva de lei em sentido formal consagrada no artigo 165.º, n.º 1, alínea *b*), da Constituição, os limites impostos pelo artigo 18.º, n.os 2 e 3: proporcionalidade em sentido amplo; reserva de lei em sentido material; proibição de retroatividade; e inviolabilidade do conteúdo essencial. As dúvidas, neste caso, centram-se no respeito pelo princípio da proporcionalidade.

Tratando-se da restrição de direitos de defesa ou de conteúdo negativo — o direito a que o Estado não aceda a dados pessoais —, o problema que se coloca é o de saber se o legislador, na solução estipulada no artigo 3.º contextualizada no respetivo regime jurídico, violou a proibição do excesso.

A primeira etapa do juízo passa por identificar as razões que podem justificar a restrição dos direitos aqui envolvidos — razões que, nos termos do n.º 2 do artigo 18.º, se traduzem necessariamente num dever de proteção de outros direitos fundamentais ou na prossecução de interesses legítimos que a ordem constitucional confia ao poder público, mormente o legislativo. No que diz respeito ao artigo 3.º da Lei Orgânica n.º 4/2017, as finalidades da norma reconduzem-se ao valor constitucional da segurança, que agrega a dimensão positiva de um conjunto muito vasto de direitos fundamentais (v.g., vida, integridade, propriedade) e interesses coletivos como a independência nacional e a ordem pública. Trata-se, em suma, das alíneas *a*) (garantir a independência nacional), *b*) (garantir os direitos e liberdades fundamentais) e *c*) (defender a democracia política) do artigo 9.º da Constituição, que define as «tarefas fundamentais do Estado». O texto constitucional vai ao ponto de subjetivar a segurança, no artigo 27.º, n.º 1, *in fine*, tratando-a como um direito fundamental.

Na prática, as limitações de direitos fundamentais devem obedecer aos seguintes requisitos: *(a)* formulação de uma norma clara e previsível; *(b)* meio necessário para alcançar um objetivo de interesse geral ou para proteger direitos ou liberdades de outrem; *(c)* proporcionalidade em relação ao objetivo visado; *(d)* preservação do conteúdo essencial do direito fundamental.

Cabe, assim, determinar, a esta luz, se o acesso pelos «oficiais de informações do SIS e do SIED» a «dados de base e de localização de equipamento» é uma medida desproporcionada ou um meio excessivo para alcançar as finalidades — em si mesmas não apenas legítimas como constitucionalmente impostas ao poder público — a que se destina.

Antes de submeter a norma aos testes da adequação, da necessidade e da proporcionalidade em sentido estrito, compreendidos no princípio da proibição do excesso, é indispensável analisar o regime de acesso que a Lei Orgânica n.º 4/2017 consagra para esta categoria específica de dados, nomeadamente as finalidades, os critérios, as formas, os limites e as garantias nela previstas.

No que respeita às *finalidades,* a lei prevê (artigo 3.º) o acesso a dados de base e dados de localização exclusivamente «para efeitos de produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada». Ou seja, a defesa nacional e a segurança interna surgem, quer como bens jurídicos subjacentes a um elenco fechado de tipos criminais ou categorias de crimes, quer como razões residuais para aceder aos dados.

Quanto aos *critérios*, a lei exige (artigo 6.º) que o acesso seja adequado, necessário e proporcional em cada caso concreto — ou seja, que a diligência não se mostre excessiva, atentas todas as circunstâncias relevantes —, densificando esta exigência através do requisito de que a informação obtida diga respeito a um alvo ou um intermediário determinados (exigência de individuação) e de que seja impossível ou muito difícil obter a informação de outra forma ou em tempo útil (exigência de necessidade). O artigo 10.º, n.º 1, estabelece ainda que o acesso não compreende «todos os dados», mas apenas as «categorias de dados» que a diligência reclamar (exigência de restrição), ressalvando-se as «condições de proteção do segredo profissional».

Relativamente à *forma*, a lei determina que o acesso aos dados pelos oficiais de informações do SIS e do SIED seja objeto de autorização judicial «por uma formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções» (artigos 5.º e 8.º). O processo inicia-se com um pedido dos oficiais de informações sujeito a determinadas exigências de conteúdo (artigo 9.º), o qual é objeto de apreciação judicial fundamentada num prazo de 48 horas (artigo 10.º, n.º 3). Ainda que se entenda que esta formação, na prática, funciona, não como um tribunal, mas como uma entidade administrativa, tal entendimento não muda o equilíbrio de interesses constitucionalmente exigido entre a proteção da vida privada e os poderes-deveres do Estado na prevenção do terrorismo, pois nos termos do artigo 35.º, n.º 2, da Constituição, é suficiente que a garantia da proteção destes direitos seja levada a cabo por uma entidade independente.

No que concerne aos *limites*, destaca-se a proibição, contida no n.º 2 do artigo 6.º, de «interconexão em tempo real com as bases de dados dos operadores de telecomunicações e Internet para o acesso direto em linha aos dados requeridos» Significa isto que é permitido o acesso pelos oficiais de informações do SIS e do SIED apenas aos dados previamente armazenados pelos operadores de telecomunicações, como decorre da definição do objeto que consta do artigo 1.º, n.º 1.

Finalmente, quanto a *garantias*, para além da exigência de autorização judicial, a lei atribui à formação do Supremo Tribunal de Justiça competente para autorizar o acesso o poder de «determinar a todo o momento o cancelamento de procedimentos em curso de acesso a dados…obtidos de forma ilegal ou abusiva», que «violem o âmbito da autorização judicial prévia» ou que sejam «manifestamente estranhos ao processo» (artigo 12.º, n.º 3). Atribui a uma Comissão de Fiscalização de Dados do SIRP a competência para fiscalizar a atividade dos oficiais de informações, com o fito de garantir o «respeito pelos princípios e cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados obtidos» (artigo 15.º, n.º 1). Reconhece ainda poderes de fiscalização, neste domínio, ao Conselho de Fiscalização do SIRP (artigo 16.º). Por fim, o artigo 7.º prevê o agravamento das penas abstratamente aplicáveis aos vários tipos de crime que possam estar implicados no acesso ilegal a dados pessoais.

Todas estas medidas procuram assegurar a salvaguarda de uma esfera fundamentalíssima de privacidade e de autodeterminação informativa, limitando ao mínimo indispensável a ingerência estadual.

O acesso aos dados previstos e com os objetivos fixados no artigo 3.º da Lei Orgânica n.º 4/2017, dificilmente pode ser censurado no plano da adequação e da necessidade. Por um lado, é óbvio que a medida é um meio idóneo de produção de informações que se venham a revelar úteis na prevenção dos atos e na tutela dos interesses mencionados na lei. Por outro lado, não há evidência alguma de que existam meios menos lesivos que permitam, com igual eficácia, alcançar os objetivos a que o regime se destina, tanto mais que a lei faz depender a autorização de acesso e a sua manutenção da verificação da necessidade da diligência.

É na proporcionalidade em sentido estrito que se joga a conformidade constitucional da norma. Colocam-se aqui duas questões essenciais. A primeira é a de saber se um regime de acesso a «dados de base e de localização de equipamento» pelos oficiais de informações do SIRP, com o efeito inibidor da autodeterminação informativa dos cidadãos e com o risco de abuso da privacidade pessoal que a mera existência de um tal regime inevitavelmente implica, reprova no teste da proporcionalidade. Entendendo-se que não, surge-nos uma segunda questão: a de saber se o regime estabelecido na Lei Orgânica n.º 4/2017 limita o acesso aos dados pessoais a que respeita o seu artigo 3.º aos casos concretos em que, tudo visto e ponderado, tal acesso se justifica — ou, pelo menos, reduz a possibilidade de erro ou de abuso a um mínimo possível que se possa ajuizar constitucionalmente tolerável.

Quanto à primeira questão, deve entender-se que a existência de um regime desta natureza, pese embora o seu efeito restritivo de direitos fundamentais, é constitucionalmente admissível. O acesso a dados pessoais previsto no artigo 3.º da Lei Orgânica n.º 4/2017 destina-se ao cumprimento de deveres de proteção de direitos fundamentais e a tutela de interesses coletivos com elevada carga axiológica na ordem constitucional. Trata-se, como se viu, do desempenho pelo Estado de tarefas fundamentais definidas na Constituição, em circunstâncias em que a omissão de medidas desta natureza se pode razoavelmente reputar prejudicial para a salvaguarda dos valores constitucionais subjacentes àquelas tarefas.

Quanto à segunda questão, julga-se que o acesso para efeitos de prevenção de atos que integram os tipos ou categorias de crimes referidos no artigo 3.º, tal como se encontra regulado na lei, não é desproporcionado. A indeterminação dos critérios de acesso — que se consubstanciam num juízo de ponderação casuística, sujeito às exigências acima mencionadas de individuação, necessidade e restrição — traduzem a inevitável e desejável concordância prática entre os valores da privacidade e da segurança que relevam das circunstâncias. E o risco de abuso e de erro é fortemente limitado pelo controlo prévio da formação especial do Supremo Tribunal de Justiça: o risco de abuso é mitigado pela garantia estatutária de independência e imparcialidade dos juízes; o risco de erro é mitigado pela adequação funcional do poder judicial para fazer as ponderações reclamadas pela lei, as quais têm, de resto, uma grande afinidade com as que caracterizam a intervenção do juiz de instrução criminal na fase de inquérito.

Porém, semelhante juízo não se pode estender ao segmento da norma que permite o acesso aos dados para efeitos de salvaguarda imediata da defesa nacional e da segurança interna, sem a mediação de critérios de determinabilidade destes conceitos através de «elementos tipificadores limitadores da ação», na expressão do Tribunal Constitucional alemão (cf. *BVerfG*, 110, pp. 33, 57 e 60).

Os conceitos usados na norma questionada são demasiado vagos, por um lado, e são estranhos ao universo da judicatura, por outro; a exigência de autorização judicial não dá, no que a eles respeita, garantias suficientes de que a ingerência na privacidade dos cidadãos se cinge ao mínimo necessário e proporcional. Na verdade, pela sua própria natureza de conceitos de atribuições essenciais do SIRP, remetem para uma prerrogativa de avaliação do SIS e do SIED que frustra o equilíbrio que apenas o escrutínio judicial rigoroso de cada pedido de acesso pode assegurar. O legislador tem, assim, o ónus de concretizar, de forma rigorosa e precisa, quais os critérios suscetíveis de justificar, nos termos do artigo 3.º da Lei Orgânica n.º 4/2017, o acesso, por entidades públicas, aos dados de base e de localização de equipamento dos cidadãos.

Sendo assim, julga-se a norma constante do artigo 3.º da Lei Orgânica n.º 4/2017 inconstitucional, no segmento que confere aos oficiais de informação do SIS e do SIED acesso a dados de base e de localização de equipamento, para efeitos de produção de informações necessárias à salvaguarda da defesa nacional e da segurança interna, por violação dos artigos 26.º, n.º 1, e 35.º, n.ºs 1 e 4, em conjugação com o artigo 18.º, n.º 2, da Constituição.

**III — Decisão**

Pelo exposto, decide-se:

*a*) Declarar a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 3.º da Lei Orgânica n.º 4/2017, de 25 de agosto, na parte em que admite o acesso dos oficiais de informações do Serviço de Informações de Segurança (SIS) e do Serviço de Informações Estratégicas e de Defesa (SIED), relativamente a dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação, para efeitos de produção de informações necessárias à salvaguarda da defesa nacional e da segurança interna, por violação dos artigos 26.º, n.º 1, e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2, da Constituição da República Portuguesa;

*b*) Não declarar a inconstitucionalidade da norma constante do artigo 3.º da Lei Orgânica n.º 4/2017, de 25 de agosto, na parte em que admite o acesso dos oficiais de informações destes serviços no âmbito das respetivas atribuições, relativamente a dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação, para efeitos de produção de informações necessárias à prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada;

*c*) Declarar a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4.º da Lei Orgânica n.º 4/2017, de 25 de agosto, por violação do disposto no artigo 34.º, n.º 4, da Constituição, no que diz respeito ao acesso aos dados de tráfego que envolvem comunicação intersubjetiva, e por violação do disposto nos artigos 26.º, n.º 1 e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2, todos da Constituição, no que se refere ao acesso a dados de tráfego que não envolvem comunicação intersubjetiva.

Lisboa, 18 de setembro de 2019. — *Lino Rodrigues Ribeiro* [com declaração de voto quanto à alínea *a*) do dispositivo, que junto] — *Pedro Machete* [vencido quanto à alínea *b*) e com declaração quanto às alíneas *a*) e *c*)] — *João Pedro Caupers* (com declaração de voto) — *Fernando Vaz Ventura* [vencido quanto à alínea *b*) da decisão, conforme declaração de voto que junto] — *Claudio Monteiro* (vencido, nos termos da declaração de voto que junto) — *Joana Fernandes Costa* (parcialmente vencida nos termos da declaração conjunta apresentada) — *José Teles Pereira* (parcialmente vencido nos termos da declaração que apresentei) — *Maria de Fátima Mata-Mouros* (parcialmente vencida nos termos da declaração que junto) — *Gonçalo Almeida Ribeiro* (parcialmente vencido, nos termos da declaração conjunta apresentada) — *Maria José Rangel de Mesquita* [vencida parcialmente quanto à decisão da alínea *a*) e vencida quanto à decisão da alínea *c*), nos termos da declaração de voto que se apresenta] — *Manuel da Costa Andrade* [vencido quanto à alínea *b*) do dispositivo] — Tem votos de conformidade quanto às alíneas *a*) e *c*) do dispositivo e quanto à alínea *b*) votos de vencidas, da Conselheira *Catarina Sarmento e Castro* e *Maria Clara Sottomayor*, que não assinam por entretanto terem cessado funções. *Lino Rodrigues Ribeiro*

**Declaração de voto**

Votei vencido quanto à alínea *a*) da decisão constante do acórdão tirado nos presentes autos, pelos fundamentos que passo a expor.

A inconstitucionalidade do segmento da norma do artigo 3.º — «*produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna* [...]» — assenta exclusivamente na indeterminação dos conceitos «defesa nacional» e «segurança interna», os quais remetem para "prerrogativa de avaliação do SIS e do SIED que frustra o equilíbrio que apenas o escrutínio judicial rigoroso de cada pedido de acesso pode assegurar". De modo que, sem a mediação de critérios de determinabilidade desses conceitos através de «*elementos tipificadores limitadores da ação*», a norma não respeita o princípio da proporcionalidade, na vertente de proibição do excesso.

Ora, em meu entender, a norma extraída do referido artigo 3.º não atribui aos oficiais de informação do SIS e do SIED um poder irrestrito de aceder aos dados de base e aos dados de localização que não deem suporte a uma concreta comunicação. Com efeito, para além de explicitar a natureza do poder concedido e a respetiva titularidade, a norma demarca-lhe os limites através da explicitação do fim visado na concessão desse poder. É verdade que a descrição normativa do

fim integra conceitos jurídicos indeterminados — como os de «defesa nacional» e de «segurança interna» — cuja vagueza não permite autonomamente reconvertê-los em pressupostos do exercício do poder de aceder àquela categoria de dados. Mas não é menos certo que a norma do fim-interesse público que deve ser prosseguido através do acesso aos dados, não só vem acompanhada da explicitação, nos artigos 6.º e 9.º do mesmo diploma, das condições do exercício do poder, como a interpretação abstrata daqueles conceitos indeterminados exige o concurso das demais normas do sistema que regula a atividade dos Serviços de Informação.

De facto, para além do mínimo de conteúdo semântico que os enunciados «segurança interna» e «defesa nacional» possuem, é na Constituição — artigos 272.º e 273.º —, na Lei de Segurança Interna e na Lei de Defesa Nacional que se encontra o núcleo essencial do tipo de situações sobre o qual pode incidir o acesso à categoria de dados prevista no artigo 3.º da Lei Orgânica n.º 4/2017, de 25 de agosto. Assim, a «*segurança interna*» compreende a atividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade pública, em especial, «proteger a vida e a integridade das pessoas, a paz pública e a ordem democrática, designadamente contra o terrorismo, a criminalidade violenta ou altamente organizada, a sabotagem e a espionagem» (artigo 1.º, n.º 1 e 3 da Lei n.º 53/2008, de 29 de agosto); por sua vez, a «*defesa nacional*» abrange a atividade destinada a garantir a «soberania do Estado, independência nacional e a integridade territorial de Portugal, bem como assegurar a liberdade e a segurança das populações e a proteção de valores fundamentais da ordem constitucional contra qualquer agressão ou ameaça exterior» (n.º 1 do artigo 1.º da Lei Orgânica n.º 1-B/2009, de 7 de julho).

Deste modo, o acesso à categoria de dados coberta pelo artigo 3.º encontra-se limitado por finalidades mais pormenorizadas e especificadas que, não obstante a subsistente indeterminação, fornecem simultaneamente o quadro das circunstâncias em que a intromissão pode ter lugar. Tal como é necessário o recurso às normas do Código Penal e Legislação extravagante para determinar o que são «atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada» — casos que o Acórdão considerou, e bem, que «traduzem a inevitável e desejável concordância prática entre os valores da privacidade e da segurança que relevam das circunstâncias» —, também se torna necessário o concurso das normas que expressamente definem e enunciam os atos abrangidos pelas conceitos de «segurança nacional» e de «defesa nacional». E mesmo assim, considerando os Serviços de Informação abordam esses fenómenos por ângulos diferentes da investigação criminal, tem que se ter em conta que os conceitos usados no âmbito das informações têm um sentido funcional e teleológico não necessariamente coincidente com o significado jurídico-penal.

Pode, pois, afirmar-se que o núcleo essencial do tipo de situações capazes de justificar a acesso aos dados de base e de localização que não dão suporte a uma concreta comunicação esta normativamente estabelecido. Porém, o facto de estar assegurada a tipificação mínima das situações em que é possível aceder aos dados não exclui as diferentes possibilidades de ação que decorrem dos conceitos expressivos das normas. A margem de maleabilidade deixada pelos conceitos indeterminados que configuram normativamente os pressupostos do acesso aos dados confere aos Serviços de Informação e à autoridade independente que previamente autoriza o acesso o poder de livremente avaliar, em cada caso concreto, se ocorre o tipo de situações que o legislador previu. Na verdade, sendo a responsabilidade de produzir "informações de segurança" exclusiva daqueles serviços, apenas eles estão em condições de formular juízes de valor, muitos deles juízes de prognose, sobre a necessidade de aceder aos dados para salvaguarda de qualquer das situações que o legislador enquadrou no âmbito da segurança interna e defesa nacional.

A menor densidade normativa que resulta da utilização desses conceitos indeterminados apenas é tolerável, sem violação do princípio da segurança jurídica, perante o *menor grau de danosidade à privacidade* causada pela intromissão nessa específica categoria de dados. A Acórdão não deixa de reconhecer tal facto quando inicia a apreciação da constitucionalidade das normas sindicadas pelas questões suscitadas pelos dados de tráfego «*tendo em conta o seu maior grau de lesividade na intromissão nesse domínio*», referindo de seguida que «*o conhecimento destes dados pelos SIS e pelo SIED representa, necessariamente, uma mais intensa devassa da vida privada do que o acesso aos dados de base ou a dados de localização, previstos no artigo 3.º*», porém, sem que daí se tire quaisquer consequências. E de facto, o acesso a essa categoria de dados — de base e

de localização —, *quando dissociado de qualquer comunicação*, não apresenta o mesmo dano à privacidade dos respetivos titulares que o causado pela intromissão nos dados de tráfego.

Os dados de base — os dados informatizados relativos à conexão a uma rede de comunicações eletrónicas — limitam-se a descrever os elementos que fazem parte do objeto do "contrato de prestação de serviços" celebrado entre o utilizador e o operador do serviço de comunicações eletrónica, ou seja, são "dados contratuais" que subsistem enquanto durar o contrato e que se mostram indispensáveis, na perspetiva dos operadores, à faturação dos assinantes e pagamento de interligações, podendo ser tratados sem o consentimento do utilizador (alínea *a*) do artigo 6.º da Lei n.º 67/98, de 26 de outubro); e os dados de localização de equipamento de telecomunicações, quando não deem suporte a uma concreta comunicação, são uma categoria "meramente residual" — como se refere no Acórdão —, que não identificam a célula (cell ID) de origem e de destino de uma chamada telefónica numa rede móvel, para além desses equipamentos poderem conter dispositivos de desativação de serviços de localização que impedem ou dificultam a identificação do respetivo possuidor.

Não obstante o assinante poder declarar no ato de assinatura do contrato que pretende a confidencialidade dos dados contratuais, incluindo a não transmissão a terceiro, a verdade é que, para fins de investigação criminal, a lei não protege *na mesma medida* essas categorias de dados relativamente aos dados de tráfego. Com efeito, a Lei n.º 32/2008, de 17 de julho, sobre a conservação de dados gerados ou tratados no contexto de comunicações eletrónicas, considera bloqueados desde o início da sua conservação as categorias de dados indicadas no seu artigo 4.º, «com exceção dos dados relativos ao nome e endereço» (n.º 2 do artigo 7.º); a obrigação de conservação dos dados não abrange os dados de comunicação em que não foi estabelecida ligação telefónica (n.º 2 do artigo 5.º); o acesso e a transmissão de dados sobre localização celular são admissíveis sem autorização judicial (n.º 6 do artigo 9.º, que remete para o artigo 252.º-A do CPP); e o acesso aos dados de base também é possível sem prévia autorização judicial [artigos 187.º, 189.º, e 269.º, n.º 1, alínea *e*) do CPP].

Assim, estando proibida a interconexão em tempo real com as bases de dados dos operadores de telecomunicações e Internet para acesso direto em linha aos dados requeridos, assim como o acesso à totalidade dos dados previamente armazenados, através da aquisição em larga escala, por transferência integral dos registos existentes (artigos 6.º, n.º 2 e 9.º, n.º 3 da Lei Orgânica n.º 4/2017), a transmissão de dados contratuais dissociadas das comunicações efetivamente realizadas ou tentadas não pode ter o mesmo grau de proteção que o exigido para dados que revelam as circunstâncias de uma concreta comunicação, já que não colide com a *ratio* do regime de confidencialidade. O sigilo das telecomunicações não deverá ser sobrevalorizado ao ponto de impedir a prestação da "identificação" e "morada" para produção de informações de segurança relativas a uma "suspeita concreta e individualizada" (n.º 3 do artigo 9.º da Lei Orgânica n.º 4/2017).

É que essa categoria específica de dados — dados de identificação — também consta de registos administrativos que descrevem algumas características pessoais de um sujeito — designadamente o nome, a filiação, a nacionalidade, a residência, a data de nascimento, género — resultando a identificação de um sujeito do conjunto de documentos oficiais constantes daqueles registos. Não obstante ser o sujeito a determinar os elementos que o particularizam, traçando a sua história de vida, individualizando-se, e não o Estado a individualiza-lo segundo critérios próprios, a verdade é que a necessidade de identificação persiste no sistema jurídico sob uma perspetiva eminentemente publicista: o ato de atribuir signos distintivos à pessoa, como o nome, data de nascimento, estado civil e sexo, surgiu da necessidade estadual de individualizar os seus cidadãos para melhor se relacionar com eles (cobrança de impostos, repressão de delitos, etc.). Por isso, a *identificação* de uma pessoa, distinguindo-a das demais, tem um campo de abrangência bem mais restrito que a *identidade pessoal* protegida pelo artigo 26.º da CRP, que possui uma aceção mais substancial, sendo composta por uma série de elementos que a constituem, e que fazem com que a pessoa seja única.

Muitos e relevantes aspetos da identidade pessoal, como o conjunto de particularidades comportamentais que distingue uma pessoa das outras, não são atingidos pela intromissão nos dados de base. Os dados através dos quais o utilizador tem acesso a um serviço de comunicações são meros elementos estáticos da sua identidade que constam do contrato de prestação de serviços

de comunicações eletrónicas previsto no artigo 48.º da Lei n.º 5/2004, de 10 de fevereiro, mas que não permitem identificar, em tempo real ou *a posteriori*, os utilizadores, o relacionamento entre uns e outros através da rede, a localização, a frequência, a data, a hora e a duração da comunicação. Por isso, a recolha e informatização dessa categoria de dados por si só não fornece informação sobre o modo de ser do respetivo titular, o modo como constrói a sua vida e como expressa a sua individualidade e personalidade. Essa informação só é possível, incluindo a criação de perfis (*profiling*), através do acesso aos dados de tráfego, que engloba em si mesmo os dados de base. Mas neste caso, os dados de base não poderão dissociar-se dos dados de tráfego, pois quando se tem acesso à informação que estes últimos contêm, ter-se-á também acesso à informação relativas aos dados de base, e por isso não podem deixar de estar abrangidos pelo artigo 4.º da Lei Orgânica n.º 4/2017.

E quanto aos dados de localização previsto no artigo 3.º, na medida em que o acesso está vedado quando deem suporte a uma concreta e efetiva comunicação, não permitem o acesso à identificação da célula (*cell ID*) de origem e de destino de uma chamada telefónica numa rede móvel; e quando em posição de *stand-by*, isto é, ligado e apto a receber chamadas, podem permitir identificar a situação geográfica das células, mas não identificam, nem permitem identificar o possuidor do equipamento no momento da recolha de dados.

Ora, se os elementos mais substanciais e dinâmicos da identidade não são afetados através da intromissão nos dados de base e de localização que não pressupõem qualquer ato de comunicação, o tratamento desses dados pessoais é menos lesivo da esfera de personalidade e privacidade do respetivo titular que o tratamento dos dados segregados pela comunicação. Por isso, a menor danosidade à confidencialidade dos dados pessoais e à privacidade que lhe está subjacente pode justificar um grau menor de exigência correlativa à determinabilidade da norma que legitima o acesso a esses dados. Enquanto o acesso aos dados de tráfego, porque se revela tão intrusivo quanto o próprio conteúdo da comunicação em si mesma, impõe que o legislador tipifique com suficiente clareza e determinabilidade as situações em que, por razões de segurança, se justifica eliminar ou enfraquecer o direito à proteção dos dados, no tratamento dos dados de base e de localização que não deem suporte a uma comunicação pode aceitar-se e tolerar-se maior abertura da norma que fixa os pressupostos de acesso a tais dados.

É por isso que as normas do artigo 6.º da Lei Orgânica n.º 4/2017, se não revelam o grau mínimo de densidade dos pressupostos de acesso aos dados de tráfego, já que, como se refere no acórdão, dele «não resulta expresso que a recolha da informação tenha por *objeto notícias de factos suscetíveis de fundamentar suspeitas de perigo da prática de determinados crimes* contra um número circunscrito de bens jurídicos fundamentais para a comunidade», podem ter determinabilidade normativa suficiente para acesso aos dados que não pressupõem comunicações. Neste domínio, em que não há uma concreta comunicação, a intensidade do sacrífico do tratamento de dados pessoais assume contornos diversos e menos lesivos. Enquanto o acesso aos dados de tráfego, pela intensidade da lesão causada à autodeterminação informativa, só é tolerável numa "*situação de perigo*", em que existe probabilidade de ocorrência de um evento lesivo, não é excessivo ou desrazoável que o acesso aos dados de base se estenda a uma "*situação de risco*", em que possibilidade de ocorrência de um evento lesivo é incerta ou reduzida. Por variadas razões, que o legislador não pode prever, os serviços que compõem o SIRP, podem necessitar de produzir informações para prevenção de riscos à segurança interna e defesa nacional com recurso a "dados contratuais" de comunicações eletrónicas, sem que esse acesso possa ser configurado como intromissão na (tele)comunicação entre pessoas. Para esse efeito — avaliação e antecipação de riscos — as balizas de atuação do SIS e do SIED estão suficientemente traçadas nos artigos 6.º e 9.º da Lei Orgânica n.º 4/2017. Perante a incerteza que encerra a prevenção de riscos de atentados à segurança interna e à segurança nacional, o SIRP não pode estar constrangido a uma atuação baseada em pressupostos firmes, podendo aceitar-se espaços de ponderação valorativa que não podem estar presentes nas situações de perigo. Por isso, não estando em causa a confidencialidade das comunicações, o poder de intromissão naquela categoria específica de dados pessoais não fere intoleravelmente a esfera jurídica dos titulares dos dados. — *Lino Rodrigues Ribeiro*

**Declaração de voto**

[referente à decisão da alínea *b*) do dispositivo e à fundamentação das decisões das alíneas *a*) e *c*)]

**1** — A proteção constitucional dos dados pessoais deve ser perspetivada de modo integrado, pois todos os aspetos respeitantes ao seu tratamento — desde a sua recolha e conservação, a transmissão a terceiros e a utilização e conexão com outros dados —, embora autónomos, estão interligados não podendo ser analisados isoladamente. Com efeito, as diferentes expressões ou modos que pode assumir o tratamento de dados pessoais não autorizado pelo respetivo titular representam uma ou mais agressões aos seus direitos fundamentais, em particular ao direito à *autodeterminação informativa* e, caso estejam em causa comunicações interpessoais, também ao direito à *autodeterminação comunicativa*.

Por outro lado, resulta claramente da presente decisão que os dados no domínio das comunicações interpessoais que permitem a identificação das pessoas também são dados pessoais e que, por conseguinte, a tutela constitucional da autodeterminação comunicativa é *especial* relativamente à tutela constitucional em matéria de autodeterminação informativa (cf. os n.os 8, *in fine*, 9, *in fine*, e 11.2.1 do acórdão).

Com base nestas duas premissas, subscrevo integralmente a fundamentação do acórdão na parte respeitante à aplicação ao caso do artigo 34.º, n.º 4, da Constituição (v., em especial, os n.os 9 e 11.1).

Aliás, não poderia deixar de causar enorme perplexidade que, depois de uma pronúncia tão clara como a que consta do Acórdão n.º 403/2015, o Tribunal, a propósito da mesma matéria e com referência ao mesmo parâmetro, viesse a adotar um entendimento diferente. Onde a Constituição é clara por razões históricas, literais, sistemáticas e teleológicas, no sentido da defesa dos direitos fundamentais de liberdade perante os poderes públicos, não pode o Tribunal adotar uma hermenêutica constitucional em que tais direitos comecem por ser perspetivados enquanto fonte de deveres de proteção legitimadores de intervenções intrusivas no seu âmbito de aplicação. A prevenção de perigos para os direitos fundamentais é necessária e devida, mas apenas — e só — no quadro do respeito pelo Estado de direito democrático. Esse é, de resto, o caminho seguido em experiências constitucionais próximas da portuguesa, onde tais exigências conduzem frequentemente à introdução de modificações na Constituição. O que não se afigura admissível é contornar — ou considerar ultrapassados — os obstáculos colocados pelas referidas exigências sob a invocação de um consenso político alargado, mas que, todavia, não chegou a ser vertido nas formas próprias e devidas do quadro constitucional vigente.

Por concordar com o que na presente decisão é referido a propósito do sentido e alcance do artigo 34.º, n.º 4, da Constituição, as considerações que se seguem respeitam apenas à avaliação da proporcionalidade das soluções normativas analisadas à luz dos artigos 26.º, n.º 1, e 35.º, n.os 1 e 4, da Constituição respeitantes à autodeterminação informativa, matéria que é objeto dos n.os 10, 11.2 e 12 daquela decisão. De todo o modo, atento o mencionado caráter *geral* (e, por isso, também *subsidiário*) da tutela constitucional da autodeterminação informativa, tais considerações são transponíveis para o domínio da autodeterminação comunicativa, nomeadamente com referência aos dados de tráfego por ela tutelados, pelo que, se não fora a regra proibitiva consagrada no citado artigo 34.º, n.º 4, as mesmas considerações poderiam adquirir uma relevância autónoma a propósito da autodeterminação comunicativa.

Igualmente no tocante à aplicação do princípio da proporcionalidade neste domínio, não está em causa a inviabilização da defesa dos valores próprios do Estado de direito democrático. Bem pelo contrário, e como uma vez mais as experiências constitucionais próximas da nossa comprovam, são esses mesmos valores que impõem que a respetiva defesa, sem perda da eficácia, se faça ao abrigo de uma disciplina que assegure as garantias próprias de tal tipo de Estado.

**2** — A Lei Orgânica n.º 4/2017, de 25 de agosto, vem, ao abrigo da *concessão* prevista no artigo 15.º, n.º 1, da Diretiva n.º 2002/58/CE citada no acórdão, disciplinar o acesso por oficiais de informações do SIS e do SIED a certo tipo de dados de toda e qualquer pessoa singular ou coletiva que utilize as comunicações eletrónicas (note-se que é justamente por estar em causa a iniciativa legislativa de um Estado-Membro correspondente a uma *derrogação facultativa* de normas de direito

da União Europeia em domínio por este harmonizado, *permitida* pelo próprio direito da União, que o Tribunal Constitucional, apesar de as medidas legislativas nacionais em causa estarem abrangidas pela referida Diretiva — e, nessa medida, constituírem "aplicação de direito da União", nos termos e para os efeitos do disposto no artigo 51.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia [cf. a síntese formulada no Acórdão do Tribunal de Justiça de 2 de outubro de 2018, *Ministerio Fiscal*, C- 207/16, EU:C:2018:788, n.os 34 a 37] —, não pôde deixar de exercer a sua competência em matéria de fiscalização abstrata sucessiva da constitucionalidade, sem prejuízo da competência do Tribunal de Justiça relativamente à interpretação do direito da União que eventualmente possa ser considerada necessária para a apreciação e decisão sobre a aplicabilidade das normas nacionais em causa no âmbito do ordenamento português; cf. o n.º 6, alínea *b*), do acórdão). Os dados em causa, são, por determinação legal, recolhidos sistemática e generalizadamente e sem uma qualquer razão específica pelos prestadores de serviços de comunicações eletrónicas e conservados durante o período de um ano (cf. os artigos 4.º e 6.º da Lei n.º 32/2008, de 17 de julho). Os titulares desses dados não podem opor-se a tal conservação (cf. *ibidem*, o artigo 3.º, n.º 4). A razão de ser fundamental da imposição da obrigação dessa conservação de dados é possibilitar a posterior transmissão às autoridades de apenas *alguns* deles referentes a *certas pessoas*, tendo em vista a deteção e esclarecimento de situações indispensáveis à prevenção e repressão de uma criminalidade caracterizada pelo recurso cada vez mais frequente às comunicações eletrónicas, seja na fase de preparação, seja na fase de execução.

As exigências relativas ao acesso a esta "reserva cautelar de dados" por parte das referidas autoridades — em rigor, não se trata de uma única reserva, pois cada fornecedor de serviços de comunicações eletrónicas está obrigado à conservação dos dados de todos os seus clientes — têm de assegurar que os dados acedidos só sejam utilizados para as finalidades que estiveram na base da justificação da obrigação legal de conservação dos dados de todos os utilizadores sem uma razão determinada. De outro modo, por causa do caráter geral, sistemático e indiscriminado daquele armazenamento, podem surgir, a jusante, intrusões consequentes no âmbito de proteção do direito à autodeterminação informativa de qualquer um.

Na verdade, a falta de razões concretas para armazenar sistematicamente dados pessoais sem o consentimento dos seus titulares durante um certo período de tempo, além de constituir *per se* uma ingerência no âmbito de proteção daquele direito, potencia o risco de novas ingerências não antecipáveis pelos titulares dos dados. Recorde-se que o efeito protetor dos direitos fundamentais referentes ao tratamento de dados não se circunscreve ao primeiro acesso, estendendo-se igualmente a todo o processamento subsequente dos mesmos dados, o qual frequentemente também reveste caráter intrusivo (cf., por exemplo, e, respetivamente, as decisões do Tribunal Constitucional Federal alemão *Volkszählung*, de 15 de dezembro de 1983, a seguir referida como *BVerfGE* 65, 1 [46], e *Telekommunikationsüberwachung*, de 14 de julho de 1999, a seguir referida como *BVerfGE* 100, 313 [359]). Na verdade, as disposições que conferem poderes às autoridades públicas para acederem e utilizarem dados pessoais no domínio das comunicações criam, em regra, uma "cadeia de diferentes agressões baseadas umas nas outras" [*verschiedene, aufeinander aufbauende Eingriffe*] (assim, v. a decisão do Tribunal Constitucional Federal alemão *Zuordnung dynamischer IP-Adressen*, de 24 de janeiro de 2012, a seguir referida como *BVerfGE* 130, 151 [184]). Acresce a proteção específica proporcionada pelo direito à autodeterminação informativa contra os perigos para o direito ao desenvolvimento da personalidade, a liberdade geral de ação e o direito à reserva da intimidade da vida privada e familiar decorrentes do tratamento informatizado de dados (incluindo os dados publicamente acessíveis; cf. as decisões do Tribunal Constitucional Federal alemão *Online-Durchsuchungen*, de 27 de fevereiro de 2008, a seguir referida como *BVerfGE* 120, 378 [397 ff.], *BVerfGE* 130, 151 [183 f.] e *KfZ-Kennzeichenkontrollen 2*, de 18 de dezembro de 2018, a seguir referida como *1 BvR 142/15*, Rn. 37-39; salientando igualmente a projeção de ingerências no mencionado direito à autodeterminação informativa sobre outros direitos fundamentais, v. o Acórdão *Tele 2*, já citado no presente acórdão, n.os 92 e 93).

Deste modo, o tratamento de dados subsequente a uma agressão inicial ao direito à autodeterminação informativa — *in casu* consubstanciada na conservação sistemática de dados sem uma razão específica — tem igualmente de ser apreciado e avaliado com referência à proteção assegurada por tal direito. Desde logo, e no que ora releva, a transmissão dos dados armazenados

pelos prestadores de serviços de comunicações eletrónicas a autoridades públicas e a possibilidade de acesso destas aos mesmos a fim de os utilizarem na prossecução das respetivas atribuições. Ou seja, as normas legais aplicáveis a cada um destes modos de tratamento de dados constituem, por isso, *restrições legais* do direito à autodeterminação informativa. Daí a necessidade de um cuidado acrescido na conformação do regime legal de acesso e de utilização dos dados em causa pelas autoridades competentes, nomeadamente quanto à definição das condições de acesso e ao estabelecimento de garantias de que os dados, uma vez acedidos, não sejam utilizados para fins diferentes daqueles que justificaram o armazenamento inicial nem fiquem definitivamente "perdidos" para o seu titular (no sentido de este perder o seu rasto e de ficar impossibilitado não só de pedir a sua eliminação, como de conhecer a utilização que dos mesmos é feita, por quem e para quê).

O equilíbrio de tal regime, globalmente considerado, é que permite avaliar se as diversas agressões decorrentes da transmissão às autoridades dos dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas podem ser justificadas à luz do princípio da proporcionalidade.

**3** — Para além dos fundamentos que estão na base dos juízos positivos de inconstitucionalidade formulados no presente acórdão, nomeadamente nas alíneas *a*) e *c*) do seu dispositivo, com os quais concordo, entendo que *o regime de acesso aos dados* de telecomunicações e de *internet* — dados esses cuja sensibilidade resulta do que na sequência do seu tratamento automatizado podem revelar sobre cada um e, principalmente, de poderem ser utilizados na construção de perfis detalhados quanto à personalidade, à mobilidade, às interações e ao envolvimento sociais ou, no caso de entes coletivos, também aos respetivos procedimentos decisórios (cf. a decisão do Tribunal Constitucional Federal alemão *Vorratsdatenspeicherung*, de 2 de março de 2010, a seguir referida como *BVerfGE* 125, 260 [318 f.], e o Acórdão *Tele 2*, n.os 98 a 100) — por parte dos oficiais de informações do SIS e do SIED *consagrado nos artigos 3.º e 4.º da Lei Orgânica n.º 4/2017 é, todo ele* — incluindo, pois, a parte referida na alínea *b*) do dispositivo —, *desproporcionado* e, por isso, *incompatível com o direito à autodeterminação informativa* pelas seguintes razões:

*i*) A excessiva indeterminação normativa dos pressupostos de facto da competência para autorizar o acesso aos dados;

*ii*) A omissão de previsão do dever de notificar as pessoas cujos dados são transmitidos aos serviços de informações do facto dessa transmissão ter sido realizada;

*iii*) A omissão de previsão da garantia de que os dados pessoais acedidos pelos SIS e pelo SIED só possam ser transmitidos a terceiros, nomeadamente a serviços de Estados que não sejam membros da União Europeia ou a organizações internacionais, desde que se mostre assegurado um nível de proteção de dados equivalente àquele a que estão obrigados os serviços de informações nacionais.

**4** — O acesso de autoridades públicas a dados previamente armazenados tão sensíveis como os referidos na Lei Orgânica n.º 4/2017, devido à gravidade da agressão ao direito à autodeterminação informativa do titular dos dados que tal acesso representa, só pode ser legitimado pela eficácia da proteção preventiva relativamente a bens constitucionalmente muito importantes. Em vista deste fim, que em si mesmo é legítimo, o acesso em causa, além de *adequado* e *necessário* para a consecução do mesmo, deve estar submetido a condições fixadas por lei formal tão *precisa* e *clara* que permita aos titulares dos dados em causa antecipar ou prever tal acesso — evitando-o, se assim o entenderem, por via da omissão dos comportamentos que podem constituir pressuposto da autorização de acesso — e que forneça às entidades competentes uma medida legal, um critério, para autorizarem o acesso e para o controlarem (cf. o artigo 18.º, n.º 2, da Constituição, e, sobre a exigência de precisão ou determinabilidade das leis restritivas de direitos, liberdades e garantias enquanto condição necessária para aferir da respetiva proporcionalidade, v. os Acórdãos deste Tribunal n.os 285/92 [III, C), n.º 5], 474/2013 [n.º 12] e 225/2018 [n.º 53]; neste domínio específico do tratamento de dados, v. também, por exemplo, a decisão *BVerfGE* 120, 378 [407 f.] e a decisão do Tribunal Constitucional Federal alemão *Bundeskriminalamtsgesetz*, de 20 de abril de 2016, a seguir referida como *BVerfGE* 141, 220 [265], os Acórdãos *Digital Rights*, já citado na presente decisão, n.os 54 e 55, e *Tele 2*, n.os 109 e 117; v., por último, o Parecer n.º 1/15 do Tribunal de Justiça

[Grande Secção], de 26 de julho de 2017, n.º 141, que refere igualmente jurisprudência do Tribunal Europeu dos Direitos Humanos).

A razão legal justificativa do acesso tem, por isso, de corresponder a uma situação de facto concreta que circunscreva efetivamente a atuação possível das autoridades, tornando claros os limites da atuação permitida. Esta exigência torna-se ainda mais premente nos casos — como o presente — em que os dados de todos são conservados sem uma qualquer razão específica, justamente para efeitos de uma eventual posterior transmissão às autoridades públicas, a seu pedido, mediante um procedimento secreto e não observável pelas pessoas afetadas (cf. o artigo 14.º, n.º 5, da Lei Orgânica n.º 4/2017). Com efeito, tais circunstâncias, por poderem criar na generalidade das pessoas a sensação de estarem sob uma vigilância permanente por parte das autoridades, aumentam o grau de agressão ao direito à autodeterminação informativa: «as pessoas não sabem o que uma dada autoridade pública sabe sobre elas, mas sabem que as autoridades podem saber muito sobre elas, incluindo informações muito pessoais» (cf. a decisão *BVerfGE* 125, 260 [335]; no mesmo sentido, v. o Acórdão *Tele 2*, n.º 100).

Ora, a *cláusula de prevenção* de atos relacionados com certos crimes consagrada nos artigos 3.º e 4.º daquele diploma não satisfaz tal exigência.

**4.1** — Desde logo, porque não é unívoco em todos os casos previstos o crime concretamente visado e o alcance possível da sua prevenção.

Por exemplo, no que se refere ao «terrorismo», é visado apenas o crime homónimo previsto no artigo 4.º da Lei n.º 52/2003, de 22 de agosto, ou também os crimes de «organizações terroristas», «terrorismo internacional» e «financiamento do terrorismo» previstos, respetivamente, nos artigos 2.º e 3.º, 5.º e 5.º-A da mesma Lei? Note-se que, para efeitos do disposto no Código de Processo Penal, todos os citados crimes são considerados «terrorismo» (cf. o artigo 1.º, n.º 1, alínea *i*), deste Código). Em qualquer caso, e independentemente da punição dos atos preparatórios do crime de terrorismo estatuída no artigo 2.º, n.º 4, da Lei n.º 52/2003, a verdade é que a prevenção do terrorismo — mesmo que praticado por um só indivíduo — não pode deixar de abranger o seu financiamento e eventuais ajudas ou colaborações.

Os atos preparatórios do crime de «espionagem» também são punidos (cf. o artigo 344.º do Código Penal com referência ao artigo 317.º do mesmo diploma). Tal amplia muitíssimo o âmbito possível da prevenção: pense-se, por exemplo, na interação de alguém com acesso a documentos classificados como segredo de Estado com uma associação ou organização estrangeira. Ora, só em função do contexto concreto pode ser afastado o eventual caráter preparatório. Aliás, a simples ideia de prevenção pode, em tese, justificar a vigilância de todos os que tenham acesso a tal tipo de informação. Nesse caso, qual o *critério legal* para vigiar A, mas já não B?

A mesma amplitude quanto à prevenção pode ser replicada a propósito dos atos de «sabotagem» (cf. o artigo 329.º do Código Penal): perante a agitação académica ou social, qual o facto que justifica iniciar a vigilância tendo em vista prevenir greves "incómodas" e eventualmente lesivas de interesses importantes, protestos sob a forma de "fecho a cadeado" das portas de uma universidade ou o "corte" (temporário) de uma estrada?

Por outro lado, onde encontrar a definição relevante para efeitos do artigo 3.º da Lei Orgânica n.º 4/2017 da noção de «proliferação de armas de destruição maciça»? E a «criminalidade altamente organizada» corresponde apenas ao conceito homónimo definido no artigo 1.º, n.º 1, alínea *m*), do Código de Processo Penal, ou deverá ser entendida como um conceito indeterminado, à maneira dos «crimes graves» cuja investigação e repressão justifica a transmissão do mesmo tipo de dados dos que aqui estão em causa, nos termos da Lei n.º 32/2008, de 17 de julho (cf. o respetivo artigo 9.º, n.º 1)?

**4.2** — As aludidas imprecisões ganham maior acuidade em razão da natureza da atividade desenvolvida pelos serviços de informações, ou seja, as autoridades às quais os dados em causa podem ser transmitidos.

Diferentemente do que sucede com a transmissão de dados prevista no artigo 9.º da Lei n.º 32/2008 — a transmissão dos dados de telecomunicações e de *internet* previamente armazenados pode ser autorizada para fins de *investigação* e *repressão* de crimes graves («se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e

repressão de crimes graves» —, a Lei Orgânica n.º 4/2017 visa disciplinar a transmissão de dados para fins de mera *prevenção* de atos criminosos que ameacem bens jurídicos muito importantes. A *prevenção de perigos* implica juízos de prognose baseados em regras de experiência quanto à probabilidade de lesão de um dado bem jurídico — orienta-se, por conseguinte, objetivamente, em função da situação de perigo criada em relação a determinado bem; a *repressão criminal* parte da verificação de um ato danoso punível como crime e procura determinar as circunstâncias da sua produção e o responsável pela sua prática — a orientação aqui é referida essencialmente à pessoa do suspeito da prática do crime (cf. os desenvolvimentos constantes dos n.os 11.2.3 e 11.2.4 do presente acórdão).

As diferentes perspetivas coenvolvidas — respetivamente, análise de situações objetivas *ex ante* e a descoberta *ex post* e perseguição de suspeitos de terem praticado certos crimes — têm levado a considerar, neste domínio da intrusão no âmbito de proteção do direito à autodeterminação informativa, que a autorização de acesso a dados sensíveis com fins de mera prevenção por simples referência a um catálogo de crimes, tendo em vista evitar que os mesmos venham a ser cometidos e, consequentemente, lesados os bens por eles protegidos, não constitui a técnica normativa mais adequada, uma vez que não são claras as exigências e os critérios quanto à intensidade do perigo para os bens jurídicos a proteger e que é relevante para permitir a intrusão. Esta incerteza é agravada nos casos em que o perigo para tais bens já é, ele próprio, objeto de incriminação ou nos casos em que os atos preparatórios dos crimes do catálogo também são punidos (cf. a decisão *BVerfGE* 125, 260 [329]). Acresce, no que se refere especificamente aos *serviços de informações*, que a respetiva atuação neste domínio se deve submeter às exigências aplicáveis em matéria de prevenção: «as exigências constitucionais para a utilização de dados ordenada à prevenção de perigos [*Gefahrenabwehr*] valem para todas as habilitações de intrusão com fins preventivos. As mesmas valem assim também para o processamento de dados pelos serviços de informações [e não apenas para a atuação preventiva de cariz policial]» (cf. a decisão *BVerfGE* 125, 260 [331]).

Para superar estas dificuldades, deve o legislador, ao invés, tomar como referência imediata os próprios bens jurídicos cuja proteção justifica o acesso e posterior utilização dos dados em causa e determinar o grau de ameaça de lesão de tais bens a partir do qual se deve considerar verificado o pressuposto para autorizar o acesso aos dados. Uma solução normativa deste tipo é a que mais se ajusta à prevenção de perigos enquanto modo de proteção de bens jurídicos e garante uma conexão imediata ao fim justificativo da ingerência no âmbito de proteção do direito fundamental (cf. *ibidem*, pp. 329-330).

Em qualquer caso, a base legal habilitante da ingerência tem de conter indicações factuais e pontos de referência a identificar numa dada situação que indiciem um perigo suficientemente caracterizado para os bens jurídicos a proteger; ou, pelo menos, tais indicações devem levar a concluir que uma situação desse tipo poderá ocorrer num futuro próximo. As meras suspeitas ou suposições gerais baseadas na experiência são insuficientes. O mesmo se passa com conjeturas factualmente fundadas sobre possíveis perigos, em que a situação de facto se caracteriza por uma grande abertura quanto ao desenvolvimento futuro. Com efeito, as indicações factuais normativamente exigíveis devem permitir identificar situações concretas em que, com um grau variável de proximidade temporal, determinadas pessoas poderão lesar os bens jurídicos considerados (cf. as decisões *BVerfGE* 120, 274 [328 f.], 125, 260 [330 f.] e 141, 220 [271 ff.]) — revestindo tais bens, naturalmente, uma importância constitucional fundamental.

Especialmente em relação a formas de criminalidade muito complexas que ameacem bens especialmente importantes, pode o legislador alargar os limites da possibilidade de intervenção para além do "perigo concreto" típico da prevenção policial (uma situação em que, se nada se fizer no imediato ou a muito curto prazo, ocorrerá com grande probabilidade a lesão de um bem jurídico protegido), reduzindo as exigências quanto à previsibilidade da sequência causal e, portanto, fazendo recuar a intervenção a situações suscetíveis de serem integradas numa fase preparatória ainda relativamente longínqua — trata-se do "campo avançado" próprio da antecipação de perigos para bens jurídicos valiosos (cf. o n.º 11.1.2 do presente acórdão). Mas, também nesses casos, deve a verificação de factos concretos que suportem a prognose de um acontecimento que conduza à lesão dos bens protegidos por pessoas determinadas constar da previsão legal (cf. a exigência de "situações de *perigo suficientemente indiciadas*" referida no n.º 11.2.3 do acórdão). Por exemplo,

em relação à prevenção de atos de terrorismo, «frequentemente praticados na sequência de um longo planeamento, de modos muito diferenciados e em locais não previsíveis por indivíduos não condenados anteriormente em processos criminais, podem ser autorizadas medidas de vigilância, mesmo que não seja conhecido um acontecimento concreto e previsível, desde que o comportamento individual de certa pessoa funde a probabilidade concreta de que num futuro mais ou menos próximo irá praticar crimes dessa natureza» (cf. a decisão *BVerfGE* 141, 220 [272 f.]: o exemplo mencionado é o da entrada no país de uma pessoa que tenha estado num campo de treino para terroristas localizado no estrangeiro; porém, se o fundamento da intrusão se localizasse ainda mais a montante de uma situação de perigo não totalmente definido para os bens jurídicos protegidos, por hipótese, a atração intelectual por uma compreensão religiosa de cariz fundamentalista, o custo da ingerência consubstanciada na vigilância já provavelmente deixaria de ser compensado pelo valor dos fins intencionados).

**4.3** — Mas não é nada disso que se passa com as previsões dos artigos 3.º e 4.º da Lei Orgânica n.º 4/2017. Acompanhando e procurando reforçar o que se afirma no n.º 11.2.4 do acórdão — afirmações essas que considero transponíveis para o âmbito de aplicação do artigo 3.º da citada Lei —, verifico que nenhum daqueles dois preceitos contém uma medida clara e precisa quanto aos limites da intrusão. Consequentemente, os mesmos artigos, por si só ou em conjugação com outros elementos do regime em causa, não permitem assegurar que a lesão do direito fundamental à autodeterminação informativa, consubstanciada no acesso por parte dos oficiais do SIS e do SIED aos dados de telecomunicações e *internet* — revistam eles a natureza de *dados de base*, de *dados de localização de equipamento* ou de *dados de tráfego* (cf. o artigo 2.º, n.º 2, da Lei Orgânica n.º 4/2017) — previamente armazenados pelos prestadores de serviços de comunicações eletrónicas (o mesmo é dizer, a *carga coativa*) seja, em todos os casos, reduzida ao mínimo indispensável à proteção dos bens jurídicos que, enquanto interesse público fundamental, a legitima (o *ganho* ou *benefício para o interesse público*). A racionalidade e justa medida entre as vantagens (públicas) e desvantagens (privadas), entre benefícios e custos, não se mostra, por isso, suficientemente garantida.

Para que assim não fosse, seria indispensável determinar no amplíssimo campo da prevenção — que pode ir da mera possibilidade de dano, mais ou menos remota, até ao limiar do perigo concreto, passando pela precaução, pela suspeita de perigo e por várias outras situações em que a aproximação do dano pode surgir com maior ou menor definição e com maior ou menor urgência — um tipo de situação objetivamente comprovável a partir da qual a análise custos-benefícios, fundada na consistência da prognose relativamente ao dano do bem jurídico considerado, pudesse ser submetida a uma apreciação crítica.

Com efeito, a *cláusula de prevenção* daqueles dois artigos limita-se a remeter para as atribuições do SIS e do SIED. O primeiro é, justamente, «o organismo incumbido da produção de informações que contribuam para [...] a prevenção da sabotagem, do terrorismo, da espionagem e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido» (cf. o artigo 21.º da Lei-Quadro do Sistema de Informações da República — Lei n.º 30/84, de 5 de setembro). Nesse quadro, os «factos que suportam o pedido» de acesso aos dados, assim como as pessoas envolvidas em tais factos elegíveis como «alvo» ou «intermediário determinado» (cf. os artigos 6.º, n.º 1, alínea *a*), e 9.º, n.º 2, alíneas *b*) e *c*), ambos da Lei Orgânica n.º 4/2017), podem ser quaisquer indivíduos ou entidades que, no juízo do SIS ou do SIED, apresentem uma qualquer possibilidade de conexão — a lei nem sequer exige um risco mínimo — com a prática futura de um dos crimes do "catálogo" (crimes esses que, conforme mencionado, também não se encontram claramente identificados). Mais: o legislador até parece admitir que o acesso aos dados pessoais seja meramente instrumental «para a obtenção de informação» que nem sequer diga diretamente respeito ao titular dos dados [cf. o artigo 6.º, n.º 1, alínea *b*), da citada Lei: por hipótese, a ocupação de uma casa ou a utilização de um veículo ou computador). Em suma, nos termos legais, o fim da prevenção, tal como avaliada pelo SIS e pelo SIED, justifica sempre o acesso aos dados.

Deste modo, a prerrogativa de avaliação reconhecida aos serviços de informações no domínio da prevenção, torna a garantia do controlo *a priori* desenvolvido pela formação de conselheiros do Supremo Tribunal de Justiça, em larga medida, ineficaz. A proporcionalidade do pedido referida

no artigo 10.º, n.os 1 e 2, da Lei Orgânica n.º 4/2017 só pode ser medida em função dos próprios termos em que o pedido é formulado, designadamente das finalidades invocadas dentro do âmbito demasiado vago e indeterminado da prevenção: salvo *desvio de poder* ou *erro de facto manifesto*, não se vislumbram outros fundamentos legais para a denegação da autorização de acesso.

Por outro lado, é verdade que a mesma formação de conselheiros deve assegurar «a *ponderação* da relevância dos fundamentos do pedido e a salvaguarda dos direitos, liberdades e garantias constitucionalmente previstos», de acordo com o estatuído no artigo 5.º daquele diploma (itálico adicionado). Simplesmente, esta remissão para a decisão do caso concreto da solução do conflito entre os direitos dos titulares dos dados e o interesse público na prevenção é, por si só, insuficiente.

Desde logo, tal ponderação é sempre exigível, devendo, em todo o caso, assegurar-se aos órgãos de controlo a possibilidade da sua realização. O prazo de decisão e a possibilidade de determinar a todo o momento o cancelamento de procedimento em curso concorrem decerto nesse sentido (cf., respetivamente, os artigos 10.º, n.os 3 e 4, e 12.º, n.º 3, da Lei Orgânica n.º 4/2017). E o mesmo se diga quanto à fundamentação do pedido de acesso aos dados (cf. *ibidem*, o artigo 9.º, n.º 2).

Porém, no caso vertente, o que se discute é a localização das próprias balizas da prevenção constitucionalmente admissível, em função do direito fundamental a comprimir — o direito à autodeterminação informativa — e do *modus operandi* da referida compressão (a partir de uma "reserva de dados" conservados indiscriminadamente e sem uma razão específica, em segredo e sem que os titulares do direito comprimido tenham consciência de estarem sob observação). A simples devolução da resolução do aludido conflito para decisões concretas não resolve, por isso, o problema específico da agressão ao direito à autodeterminação informativa aqui em análise: as pessoas em geral, sabendo que os seus dados se encontram conservados e acessíveis às autoridades mas desconhecendo as condições objetivas em que tal acesso é permitido, podem considerar ser mais prudente absterem-se de exercer outros direitos que sejam expressão da sua autonomia pessoal (liberdade de expressão, liberdade de circulação, liberdade de associação, entre outros) em consequência do receio de estarem ou virem a estar sob vigilância.

Acresce, por fim, ser igualmente seguro que as restrições legalmente previstas de direitos de liberdade fundadas em preocupações de prevenção não poderem, sob pena de violação do princípio da proporcionalidade, deixar de ser limitadas ao plano avançado de defesa definido em função daquele *limiar de agressão* que, garantindo a eficácia da prevenção, menos se afaste das situações de perigo concreto.

**5** — No que se refere à omissão de previsão do dever de notificar as pessoas cujos dados são transmitidos aos serviços de informações do facto dessa transmissão ter sido realizada, cumpre começar por recordar que o artigo 35.º, n.º 1, da Constituição, reconhece o direito de acesso aos «dados informatizados» de cada um e o direito a conhecer a finalidade a que se destinam, em ambos os casos «nos termos da lei». Nesse sentido, a legislação aplicável, consagra o *princípio da transparência* em matéria de tratamento de dados pessoais, em função do qual aqueles direitos são concretizados e desenvolvidos (cf. o artigo 5.º, n.º 1, alínea *a*), do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 — o Regulamento Geral sobre a Proteção de Dados —, e os direitos de informação e acesso, retificação e destruição e limitação do tratamento consagrados nos seus artigos 12.º e ss.; cf. também os direitos dos titulares dos dados consagrados na legislação anterior, nomeadamente nos artigos 10.º e ss. da Lei n.º 67/98, de 26 de outubro — Lei de Proteção de Dados Pessoais).

O pressuposto do exercício de todos esses direitos — incluindo a possibilidade de recurso à via jurisdicional para defesa de interesses relacionados com o tratamento desses dados — é naturalmente o conhecimento de que os dados do próprio estão a ser ou foram objeto de tratamento. Daí a importância fundamental para a transparência e consequente equilíbrio do regime em matéria de tratamento e proteção de dados do dever de informar o titular dos dados em causa. A exigência de informação, nomeadamente sob a forma de uma notificação, surge reforçada nos casos em que dados pessoais sensíveis de todos são armazenados sistematicamente e sem uma razão específica por prestadores de serviços no cumprimento de uma obrigação legal para fins de posterior disponibilização às autoridades, caso estas venham a considerar o acesso a alguns desses dados necessário para a prossecução das suas atribuições (cf. as decisões *BVerfGE* 65,

1 [44 ff.], 100, 313 [361], 125, 260 [335] e 141, 220 [282]; v., num domínio próximo, o artigo 13.º, n.º 2, alínea *d*), da Diretiva (UE) 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados; e, apesar da transposição menos precisa no que se refere à disponibilização de informações sobre os dados em causa ao seu titular — e não apenas de informações gerais sobre dados —, o artigo 14.º, n.º 2, alínea *d*), da Lei n.º 59/2019, de 8 de agosto, que a transpôs). É evidente que, nos casos de vigilâncias encobertas legalmente autorizadas, a informação ao titular dos dados não pode comprometer a finalidade das medidas adotadas (cf., por analogia, o artigo 13.º, n.º 3, da citada Diretiva (UE) 2016/680, e o artigo 14.º, n.º 3, da Lei n.º 59/2019; recorde-se que este último diploma também inclui no seu âmbito de aplicação subjetivo o SIS, enquanto força de segurança — cf. o seu artigo 3.º, n.os 1, alínea *i*), e 3, e o artigo 25.º, n.º 2, alínea *e*), da Lei n.º 53/2008, de 29 de agosto, a Lei da Segurança Interna).

Todavia, e sem prejuízo de *exceções determinadas com base numa ponderação caso a caso e sujeitas a reavaliações periódicas*, designadamente no âmbito da prevenção e repressão da espionagem ou do terrorismo, o legislador deve prever, como regra, a *informação posterior* ao titular dos dados de que os mesmos: (i) foram acedidos e com que finalidade; (ii) constam ou constaram de uma base de dados; e, se for o caso (iii) em que data foram eliminados. Possibilita-se, desse modo, ao referido titular dos dados o exercício que ainda for possível ou que, em seu entender, se justificar dos direitos próprios da proteção de dados pessoais (cf. as decisões *BVerfGE* 125, 260 [336] e 141, 220 [283]; ver também os Acórdãos *Schrems*, n.º 95, e *Tele 2*, n.º 121 e, ainda, o Parecer n.º 1/15, n.os 218 a 220).

A Lei Orgânica n.º 4/2017, ao submeter o tratamento dos dados obtidos nos termos e para os fins mencionados nos seus artigos 3.º e 4.º, ao «regime especial de proteção de dados pessoais do SIRP» e ao «regime do segredo de Estado aplicável ao SIRP» (cf., respetivamente os n.os 3 e 5 do artigo 14.º da mesma Lei; sobre o mencionado «regime de segredo de Estado», cfr os artigos 32.º e 32.-A da Lei n.º 30/84, de 5 de setembro — Lei Quadro do SIRP), afasta de plano e sem a possibilidade de qualquer avaliação concreta — mesmo nos casos de recusa de validação pelo diretor do centro de dados de inserção dos dados ou de supressão dos dados (cf. os artigos 9.º, n.º 4, e 10.º, n.º 5, do regulamento aprovado em anexo à Resolução do Conselho de Ministros n.º 188/2017, de 5 de dezembro) — a notificação aos titulares dos dados de que estes foram acedidos pelos serviços de informações.

É certo que o artigo 15.º, n.º 6, daquela Lei prevê o «direito de acesso dos cidadãos aos dados processados ou conservados nos centros de dados do SIS e do SIED», a exercer «através da Comissão de Fiscalização de Dados do SIRP». Porém — e para lá das limitações à atuação desta Comissão referidas no n.º 11.1.2, alínea (*iv*), do presente acórdão — o conhecimento por parte do interessado que pode justificar um tal pedido de acesso é meramente *acidental*; não resulta do cumprimento de qualquer dever de notificação (cf. o artigo 27.º, n.º 2, da Lei Quadro do SIRP: «[q]uem, por ato de quaisquer funcionários ou agentes dos serviços de informações ou no decurso de processo judicial ou administrativo, tiver conhecimento de dados que lhe respeitem e que considere erróneos, irregularmente obtidos ou violadores dos seus direitos, liberdades e garantias pessoais pode, sem prejuízo de outras garantias legais, requerer à Comissão de Fiscalização de Dados que proceda às verificações necessárias e ordene o seu cancelamento ou a retificação dos que se mostrarem incompletos ou erróneos»). Consequentemente, o direito de acesso em causa não é suficiente para reequilibrar o regime em análise num sentido favorável ao titular de dados e, por essa via, compatibilizar o peso da ingerência associada à transmissão aos serviços de informações dos dados de telecomunicações e *internet* previamente armazenados pelos prestadores de serviços de comunicações eletrónicas com o princípio da proporcionalidade.

**6** — Finalmente, no que se refere à omissão de previsão da garantia de *continuidade do nível de proteção* em caso de transmissão a terceiras entidades, importa referir que tal garantia é relevante para assegurar os direitos dos titulares dos dados de acederem aos mesmos, de exigirem a sua retificação ou eliminação e, em geral, de controlarem o tratamento de que os mesmos são objeto, prevenindo que tais direitos sejam esvaziados ou inutilizados. De modo particular, a ga-

rantia em apreciação também se destina a evitar que os dados pessoais venham a ser utilizados para fins diferentes dos que justificaram o acesso inicial aos mesmos por parte das autoridades competentes.

Este princípio da continuidade do nível de proteção em caso de transmissão para países terceiros não-membros da União Europeia ou para organizações internacionais tem sido muito justamente destacado no âmbito do direito da União Europeia (v., por exemplo, o Acórdão *Schrems*, n.os 72 a 74, e o Parecer n.º 1/15, n.º 134; cf. também os considerandos n.os 64 e 65 da Diretiva (UE) 2016/680, aqui aplicáveis por analogia, assim como os seus artigos 35.º a 40.º; na Lei n.º 59/2019, cf. os artigos 37.º a 42.º). E o mesmo constitui, pelas razões antes mencionadas, um desenvolvimento consequente do direito à proteção de dados pessoais constitucionalmente consagrado.

Ora, o «regime especial de proteção de dados pessoais do SIRP», que, de acordo com o estatuído no artigo 14.º, n.º 3, da Lei Orgânica n.º 4/2017, disciplina o tratamento dos dados obtidos ao abrigo da mesma Lei não contém previsões específicas sobre esta matéria. Por outro lado, como decorre do artigo 7.º, alínea *b*), do Regulamento do Centro de Dados do SIED e do SIS, aprovado em anexo à Resolução do Conselho de Ministros n.º 188/2017, é certo que existem compromissos com serviços congéneres estrangeiros no que se refere à troca de informações e dados. Deste modo, a omissão de previsão da garantia de continuidade aqui em análise com referência aos dados a aceder pelo SIS e pelo SIED, nos termos dos artigos 3.º e 4.º da Lei Orgânica n.º 4/2017, torna tal acesso desproporcionado e por isso incompatível com o direito à autodeterminação informativa, uma vez que não acautela suficientemente nem os direitos dos titulares dos dados nem a vinculação às finalidades determinantes do acesso, em termos de os dados não poderem ser tratados posteriormente de uma forma incompatível com essas finalidades. — *Pedro Machete*

**Declaração de voto**

Recuperando uma antiga e breve memória, o meu exame oral de direito penal começou pelas razões que permitiam — e eram muitas — a aplicação de medidas de segurança restritivas da liberdade aos designados "vagabundos", sem explicitação de fundamentos e por tempo indeterminado. Era verdadeiramente o Estado contra o direito, por oposição ao nosso atual Estado de direito.

Compreenderão que eu tenha, também por essa memória e em consciência, sérias objeções a qualquer interpretação do artigo 34.º, n.º 4, da Constituição, de que resulte o alargamento da ingerência nas telecomunicações — nele inequivocamente limitada a "matéria de processo criminal" e nesse sentido interpretada pela doutrina constitucional nacional mais significativa —, a temáticas que a extravasem, cobrindo indefinições que tenho por perigosas, como a "proliferação de armas de destruição maciça" e, sobretudo, a "segurança interna". Por muito "unitária" que deva ser a interpretação do texto constitucional, repugna-me aceitar que ainda se considere "interpretação", isto é, busca do "sentido e alcance" da norma, um processo intelectual conducente a um resultado que não tem no texto interpretado "um mínimo de correspondência verbal". Não creio que as particularidades da interpretação constitucional — que têm sobretudo em conta que muitas normas constitucionais não são regras, mas princípios (padrões de otimização de comportamentos) ou, sendo regras, apresentam uma menor densidade do que o comum das normas legais — tenham lugar na interpretação daquele preceito constitucional, com o propósito e resultado de converter em "matéria de processo criminal" aquilo que não é matéria de processo criminal. Tal conversão exige a revisão da norma constitucional, não se bastando com leituras "expansivas" ou "atualistas" desta, com o propósito de nela incluir aquilo que o legislador constituinte não quis lá pôr.

Releve-se-me a franqueza, mas pouco me importa saber se tal operação se louva em peripécias histórico-parlamentares ou em construções doutrinais, norte-americanas, alemãs ou de qualquer outra origem, por muito sábias que sejam e por muito respeito que me mereçam os seus defensores. Recordo, ainda, que "matéria de processo criminal" não é, não pode ser, qualquer uma que o legislador ligue a um qualquer comportamento que ele tenha entendido penalizar, mas somente aquela em que se reflitam valores fundamentais indispensáveis à convivência humana, insuscetíveis de outra forma de proteção eficiente, como decorre, de resto, de jurisprudência constante deste tribunal.

E não me venham dizer que a intromissão dos serviços de informações prevista nos artigos 3.º e 4.º, limitando embora, em grau muito significativo, a minha liberdade, é indispensável para que o Estado possa defender a minha segurança. Já ouvi isso, noutros tempos e em outros contextos. Se tivesse de escolher entre defender a minha segurança ou proteger a minha liberdade — e não tenho, antes se impondo ao legislador um cuidado exercício de ponderação, suscetível de construir um justo equilíbrio entre ambos os valores —, optaria, sem hesitar, pela liberdade. Não me encerrem numa masmorra — ou numa torre de vidro — para me proteger. Como alguém disse, viver é sempre perigoso.

Dag Hammarskjöld, antigo Secretário-Geral das Nações Unidas, disse um dia que se poderia resumir toda a filosofia dos direitos humanos numa simples frase — ser livre do medo. Anos mais tarde, o seu compatriota, Olof Palme, quando Primeiro-Ministro da Suécia, partilhando da mesma convicção, dispensou a proteção policial a que tinha direito, para ir ao cinema — e foi assassinado na via pública. Mas foi sempre um homem livre.

Desta pré-compreensão decorre o meu claro e irreversível apoio ao juízo de inconstitucionalidade relativamente à totalidade dos artigos 3.º e 4.º da Lei Orgânica n.º 4/2017. Quanto à parte daquele que não foi objeto de juízo de inconstitucionalidade [alínea *b*)], fiquei, pois, vencido. — *João Pedro Caupers*

**Declaração de voto**

**1** — Encontro-me vencido quanto ao decidido na alínea *b*) da decisão, que não declarou inconstitucional a norma constante do n.º 3 da Lei Orgânica n.º 4/2017, na parte em que admite o acesso dos oficiais de informações do SIS e SIED a *dados de base* e de *localização de equipamento*, quando não dão suporte a uma concreta comunicação, para efeitos de produção de informações necessárias à prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada.

Importa indicar, sumariamente, os motivos para essa divergência.

**2** — Entendo que as ponderações que suportam o juízo de violação dos artigos 26.º, n.º 1, e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2, da Constituição, no que se refere a *dados de tráfego* que envolvem comunicação intersubjetiva, fundamento da declaração de inconstitucionalidade, com força obrigatória geral, constante da alínea *c*) do Acórdão, valem, por *identidade de razão*, para as categorias de dados previstas no artigo 3.º da Lei Orgânica n.º 4/2017, independentemente da finalidade a que se destine o respetivo acesso e tratamento.

Efetivamente, e como se reconhece na decisão, as categorias de dados previstos no artigo 3.º, sobretudo os *dados de localização de equipamento*, comportam o acesso a um manancial de informações sobre a vida privada do respetivo titular de forte relevo. É sabido que se tornou comum e generalizada a posse, por qualquer pessoa e a todo o tempo, de um qualquer equipamento móvel de ligação a redes de comunicações eletrónicas, hoje encarado como que se de uma outra peça de vestuário se tratasse, acompanhando o sujeito em permanência. Assim, o acesso à localização de equipamento de telecomunicações (o que compreende telemóveis, computadores portáteis, *tablets*, assim como qualquer outro dispositivo com capacidade de ligação a serviços telefónicos ou à internet), *dado pessoal* registado em permanência pelas redes de comunicações eletrónicas ou serviços de telecomunicações sempre que se trate de equipamento ativo (ligado), permite recolher todos os detalhes sobre a localização geográfica do sujeito. A forte devassa inerente ao verdadeiro *roteiro da vida de cada um*, no espaço e no tempo, que assim se tornou retrospetivamente viável, reclama, creio, um escrutínio intenso da proporcionalidade da restrição ao direito à reserva da intimidade da vida privada, assim como ao direito à autodeterminação informativa, comportada na norma do artigo 3.º da Lei n.º 4/2017, em todo o seu alcance objetivo. Sem dificuldade, podem encontrar-se situações de vida em que a informação sobre onde o sujeito estava (ou não estava) num dado momento ou período de tempo comporta um efeito intrusivo e repercussões na esfera jurídica individual pelo menos não inferiores ao que resulta do acesso a dados de tráfego respeitantes a uma comunicação intersubjetiva ou acesso *online* (pense-se, por exemplo, no plano laboral ou em regimes de residência de cidadãos estrangeiros). Donde, não encontro razões materialmente

fundadas para que a intensidade do controlo a exercer nessa vertente do objeto do presente processo seja inferior à que incide sobre a ingerência permitida pela norma do artigo 4.º, também em exame.

Não partilho, assim, a visão de que o acesso aos dados de tráfego que não envolvem uma comunicação intersubjetiva representa, *necessariamente*, uma mais intensa devassa da vida privada do que o acesso aos dados de base ou a dados de localização, sem suporte a uma concreta comunicação, previstos no artigo 3.º Para todas as tipologias em apreço, o tratamento de dados pessoais não consentido põe em causa a confiança dos cidadãos na segurança e reserva dos sistemas de comunicações eletrónicas; o interesse do titular dos dados em decidir, ele mesmo, acerca da utilização das suas informações pessoais; o interesse em não ser sujeito a decisões exclusivamente automatizadas dos seus dados; o interesse em conhecer, dispor, controlar, atualizar, corrigir ou apagar os dados pessoais que lhe digam respeito; o interesse em conhecer a finalidade do tratamento dos seus dados; e o interesse na não divulgação de dados objeto de tratamento. E, também, todo o acesso e tratamento de dados pessoais, previsto nos artigos 3.º e 4.º, decorre em ambiente oculto, coberto por estruturas reforçadas de segredo, sujeito a pressupostos comuns de admissibilidade, estipulados no artigo 6.º da Lei Orgânica n.º 4/20017.

**3** — Ora, tal como se entendeu relativamente aos dados de tráfego, também quanto à ação de prevenção prevista no artigo 3.º, articulada com as condições de admissibilidade previstas no artigo 6.º, ambos da Lei Orgânica 4/2017, a medida é modelada por critérios muito abertos, semanticamente maleáveis e insuficientemente determinados, valendo igualmente neste domínio todas as ponderações referidas nesse segmento da fundamentação e a conclusão pelo défice de densificação do regime jurídico e dos pressupostos nele formulados para a ingerência.

Do mesmo jeito, é inteiramente transponível para o acesso previsto no artigo 3.º o juízo sobre a insuficiência de mecanismos que permitam ao cidadão reagir contra intervenções ilícitas, incluindo quanto à conservação de dados para além do estritamente necessário à finalidade que justificou o acesso e tratamento, a que acresce a ausência de regulação que discipline a partilha de dados com serviços de informação congéneres, assegurando que a conservação dos dados permanece sujeita à jurisdição nacional (sobre tais aspetos, sublinhando a exigência de remédios ao dispor dos sujeitos afetados e que os dados em causa sejam conservados em território da União, vd. acórdão do TJUE, *Tele 2*, parágrafos 121 a 124; também com interesse, cf. a Opinião n.º 1/15, ECLI:EU:C:2017:592, relativa ao Acordo a sobre a transferência dos dados dos registos de identificação dos passageiros, entre a União Europeia e o Canadá, parágrafos 201 a 208).

Por tais razões, entendo que a norma do artigo 3.º, em *todo o respetivo âmbito objetivo* — e não apenas na parte relativa à produção de informações necessárias à salvaguarda da defesa nacional e da segurança interna —, não satisfaz o *teste* da proporcionalidade em sentido estrito, pelo que padece de inconstitucionalidade, por violação dos artigos 26.º, n.º 1, e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2, da Constituição. — *Fernando Vaz Ventura*

**Declaração de voto**

Votei vencido quanto à questão central decidida neste Acórdão, na alínea *c*) do seu conteúdo dispositivo, por entender que o artigo 4.º da Lei Orgânica n.º 4/2017 não viola o artigo 34.º, n.º 4, da Constituição, na medida em que dele não se extrai uma proibição de acesso dos serviços de informação aos designados metadados, para fins de prevenção criminal.

Antes de mais, não creio que, no plano constitucional, faça qualquer sentido distinguir os diferentes tipos de dados — de base, de localização e de tráfego — consoante os mesmos dão ou não suporte a uma concreta comunicação. O direito fundamental à inviolabilidade do domicílio e da correspondência consagrado no artigo 34.º deve ser tomado como um todo, e nessa medida abrange todas as comunicações eletrónicas privadas, qualquer que seja a sua natureza ou meio de transmissão. É, pois, à luz desse conceito amplo de comunicações eletrónicas privadas que se deve aferir o âmbito da proibição estabelecida no n.º 4 daquele artigo e, por maioria de razão também, o âmbito da permissão expressamente ressalvada na sua parte final.

Definido o seu âmbito de aplicação, é fácil de se alcançar que o n.º 4 do citado artigo proíbe todas e quaisquer ingerências das autoridades públicas nas comunicações privadas que não es-

tejam previstas na lei "*em matéria de processo criminal"*. A questão resume-se, pois, em saber se as restrições previstas na Lei Orgânica n.º 4/2017 se podem ou não considerar como restrições *"em matéria de processo criminal"*, não sendo sequer necessário, para se legitimar as ingerências previstas naquela lei, o recurso ao conceito de restrições constitucionais implícitas aos direitos fundamentais, o que neste caso, aliás, poderia suscitar algumas dúvidas, tendo em conta a taxatividade da proibição expressamente estabelecida na Constituição.

Isso não significa, como é óbvio, que não se deva fazer uma leitura atualizada do disposto na norma constitucional em análise, pois nenhuma das realidades que estão na origem da Lei Orgânica n.º 4/2017 existiam quando o artigo 34.º da Constituição foi escrito, em 1975. As comunicações não eram eletrónicas, e em qualquer caso os meios de comunicação não tinham a sofisticação tecnológica que tem hoje, nem a criminalidade então existente constituía um perigo para a paz social comparável aos riscos atualmente associados a atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada. E a este propósito não posso deixar de dizer que uma Constituição que, salvaguardadas as garantias processuais adequadas, não consinta a ingerência nas comunicações privadas para prevenir o terrorismo e a alta criminalidade, é uma Constituição que trai a sua própria Ideia de Direito, que tem na segurança dos cidadãos e na defesa dos seus direitos fundamentais uma das traves mestras do Estado de Direito.

Prova disso mesmo é o facto de as próprias leis "*em matéria de processo criminal"* terem evoluído muito desde 1975, e de ser hoje evidente que cabe ainda naquele conceito toda a atividade instrutória realizada pelas autoridades judiciárias para fins de prevenção criminal, desde que a estrutura dos seus procedimentos, e das suas garantias, sejam equivalentes à do processo criminal propriamente dito. Como melhor explica a Conselheira Maria de Fátima Mata-Mouros no seu voto de vencido, que nessa parte subscrevo inteiramente, os procedimentos e as garantias estabelecidas na Lei Orgânica n.º 4/2017 para o acesso dos Serviços de Informação aos Metadados, e em geral às comunicações eletrónicas privadas, não são substancialmente diferentes dos estabelecidos nas leis processuais penais para as mesmas ingerências, quando realizadas a solicitação do Ministério Público na fase de Inquérito. E não ocorre a ninguém suscitar a inconstitucionalidade dessas leis, que do mesmo modo implicam uma restrição ao direito fundamental à inviolabilidade do domicílio e da correspondência consagrado no artigo 34.º, sem que exista ainda, nessa fase, um processo criminal em sentido estrito, com arguidos constituídos e todas as suas garantias estabelecidas.

Seria, aliás, absurdo fazer-se depender a admissibilidade da restrição de um conceito formal de processo criminal, cuja definição cabe ao legislador, quando, o que releva para efeitos constitucionais, é a materialidade dos valores que a legitimam. Não é por acaso, aliás, que o n.º 4 do artigo 34.º ressalva *"os casos previstos na lei* ***em matéria*** *de processo criminal"*, e não os casos em que já exista um processo criminal em sentido estrito. O que releva, então, é que a restrição se justifique pela salvaguarda dos mesmos valores constitucionais, e que as ingerências aos direitos fundamentais, além de se realizarem por procedimentos que ofereçam o mesmo nível de garantias que na fase instrutória prévia ao processo criminal, sejam adequadas e proporcionais aos fins visados.

Ora, sendo inquestionável a identidade dos valores constitucionais que a Lei Orgânica n.º 4/2017 visa salvaguardar, na parte em que ela permite o acesso aos metadados para fins de prevenção criminal, é também inequívoco que as ingerências aos direitos fundamentais dos cidadãos nela previstas se realizam por procedimentos que oferecem o mesmo nível de garantias que oferece a fase instrutória prévia ao processo criminal, tendo em conta, nomeadamente, que o acesso aos dados é sujeito a controlo judicial e autorização prévia, reservada à competência de uma «formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções» (artigo 8.º da Lei Orgânica n.º 4/2017), e que o próprio Ministério Público pode intervir no processo (n.º 1 do artigo 1.º), podendo ainda, ou devendo mesmo, desencadear os processos criminais aplicáveis, dado que a autorização de acesso aos dados, a transmissão dos dados, o cancelamento de acesso aos dados, a sua destruição e a recolha de indícios da prática dos crimes de terrorismo e espionagem, são obrigatoriamente comunicados ao Procurador-Geral da República (n.º 2 do artigo 5.º, o n.º 1 do artigo 11.º, o n.º 4 do artigo 12.º e o artigo 13.º) «para os devidos efei-

tos». O que, tudo somado, constitui uma garantia mais do que suficiente da proporcionalidade e da adequação das medidas a adotar em cada caso concreto em que elas se revelarem necessárias.

Pelas exatas mesmas razões, acompanho a decisão, na sua alínea *a*), na parte em que ela não admite quaisquer ingerências nas comunicações privadas para fins que extravasam o âmbito estrito da prevenção criminal, expressamente ressalvado na parte final do preceito constitucional em análise. — *Claudio Ramos Monteiro*

**Declaração de voto**

Vencidos quanto à declaração de inconstitucionalidade, expressa na alínea *c*) da decisão, da norma constante do artigo 4.º da Lei Orgânica n.º 4/2017, de 25 de agosto.

**1** — A decisão repousa — parece-nos — em dois argumentos principais.

O *primeiro argumento* é o de que os dados relativos a «comunicações intersubjetivas» — definidas como um processo comunicativo consumado ou tentado *entre pessoas* — são objeto de uma *tutela constitucional reforçada* em relação a dados pessoais que não respeitam a um processo comunicativo, como os dados de localização de equipamento, ou dados de tráfego que respeitam ao que no acórdão se designa «comunicação» entre «pessoas e máquinas» ou «entre máquinas», como a navegação e a consulta de sítios na *internet*.

Os dados que integram o primeiro universo — diz-se — relevam da autodeterminação *comunicativa*, subsumindo-se no n.º 4 do artigo 34.º da Constituição, que delimita através de uma «reserva absoluta de processo criminal» a exceção ao direito fundamental à inviolabilidade das comunicações. Os dados que integram o segundo universo, por outro lado, relevam da autodeterminação *informativa*, situada fora do perímetro de tutela constitucional reforçada dispensada por aquele preceito, valendo em relação a eles a autorização genérica de restrição contida no inciso final do n.º 4 do artigo 35.º da Constituição.

Ora, como a Lei Orgânica n.º 4/2017 autoriza o acesso pelas autoridades do Sistema de Informações da República Portuguesa (SIRP), quer a dados de «comunicações intersubjetivas» — dados de «tráfego» *e* de «telecomunicações», segundo as definições estipulativas destes termos dadas nas alíneas *a*) do n.º 1 e *c*) do n.º 2 do artigo 2.º da Lei Orgânica n.º 4/2017 —, quer a dados estranhos a um processo comunicativo entre pessoas — dados de «base» e de «localização de equipamento» (alíneas *a*) e *b*) do n.º 2 do artigo 2.º) e dados «de tráfego» *e* «de *internet*» (alínea *b*) do n.º 1 e *c*) do n.º 2 do artigo 2.º) —, o juízo sobre a constitucionalidade das normas que integram o objeto do processo deve partir, segundo a maioria, de premissas *radicalmente distintas* num e no outro caso.

Assim, o acesso *extra delictum* aos dados de «comunicações intersubjetivas» — ou seja, fora do âmbito de um processo criminal pendente — é *categoricamente proibido* pelo regime *especial* da inviolabilidade das comunicações, estabelecido no artigo 34.º, n.º 4, da Constituição. O acesso aos demais dados abrangidos pela Lei Orgânica n.º 4/2017 é *genericamente permitido*, desde que observados os vários limites, entre os quais se destaca a proibição do excesso, decorrentes do regime *geral* das restrições aos direitos, liberdades e garantias, estabelecido no artigo 18.º, n.º 2, da Constituição.

**2** — O *segundo argumento* da decisão é o de que, no domínio em que a Lei Orgânica n.º 4/2017 autoriza o acesso pelas autoridades do SIRP a dados que *não* se encontram sob a incidência do regime especial da inviolabilidade das comunicações, impõe-se um juízo de proporcionalidade *diferenciado* das medidas, consoante se trate de dados de tráfego, por um lado, ou dados de base e de localização de equipamento, por outro — o mesmo é dizer, entre os dados cobertos pelo artigo 4.º, na medida em que não respeitem a «comunicações intersubjetivas», e os dados cobertos pelo artigo 3.º

Entende-se que o acesso a dados *de tráfego*, independentemente da circunstância de estes respeitarem ou não a uma «comunicação intersubjetiva», «representa… uma mais intensa devassa da vida privada do que o acesso aos dados de base ou a dados de localização». De tal modo que, quanto a tal acesso, se justifica uma maior «densidade de escrutínio a aplicar pela jurisdição constitucional», «similar ou equivalente» à reclamada pelo acesso a dados de tráfego de comunicações intersubjetivas, «apesar da diferença de parâmetros constitucionais.»

Daí se retira que o acesso a dados de tráfego no âmbito da prevenção de atos de espionagem e do terrorismo pelas autoridades do SIRP, regulada através de conceitos indeterminados, como os de «*"alvo determinado",* "*situação de urgência",* "*muito difícil de obter"*, "*tempo útil"*», que constam do n.º 1 do artigo 6.º da Lei Orgânica n.º 4/2017, não passa no crivo da proporcionalidade em sentido estrito, na medida em que não assegura que a lesão da autodeterminação informativa fique circunscrita a «situações de perigo suficientemente indiciadas», cuja ameaça assente em «circunstâncias de facto, normativamente descritas». Com efeito, considera-se no acórdão que o «princípio da proporcionalidade impõe que o Estado invoque uma situação de perigo previsível, concreta e de verificação altamente provável» para aceder aos dados cobertos pelo artigo 4.º da Lei Orgânica n.º 4/2017. De outra forma — conclui —, corre-se o risco «de, sob a capa da luta contra o terrorismo e a espionagem, os cidadãos serem reduzidos a *identidades digitalmente criadas* e *heteroconstruídas»,* «com a consequente desumanização das pessoas e estandardização dos seus comportamentos», assim acabando por se «perverter a democracia».

Pelo contrário, no que respeita aos dados de base e de localização de equipamento cobertos pelo artigo 3.º, afirma-se no acórdão que os «critérios de acesso… traduzem a inevitável e desejável concordância prática entre os valores da privacidade e da segurança que relevam das circunstâncias», salientando-se que o «risco de abuso e de erro é fortemente limitado pelo controlo prévio da formação especial do Supremo Tribunal de Justiça», isto apesar de continuar a ser substancialmente maior, mesmo em face do decaimento parcial da norma, o elenco legal dos fins que justificam o acesso.

**3** — Nenhum dos *argumentos principais* se nos afigura persuasivo.

Por um lado, dissentimos da interpretação que a maioria, reiterando o Acórdão n.º 403/2015, faz do n.º 4 do artigo 34.º da Constituição, e do corolário que dela inevitavelmente retira: o de que a ordem constitucional portuguesa concede uma tutela *especial*, *definitiva* e *absoluta* a todas as dimensões da autodeterminação comunicativa dos indivíduos fora do âmbito de *um* processo criminal, ao contrário do que sucede com a autodeterminação informativa, apesar de ambas relevarem de *radicais axiológicos comuns* — a reserva de intimidade da vida privada e o livre desenvolvimento da personalidade. Entendemos, por isso, que a apreciação da constitucionalidade das medidas de acesso previstas nos artigos 3.º e 4.º da Lei Orgânica n.º 4/2017 passa, no essencial, por um juízo de *proporcionalidade*.

Por outro lado, não cremos que os termos em que tal juízo de proporcionalidade deva ser feito variem substancialmente em função das *categorias de dados* abrangidas pelas normas sindicadas, nem aceitamos que seja exigível, viável, ou sequer desejável que o legislador «densifique» o regime de acesso aos dados de tráfego através da «identificação normativa da situação fáctica que está na origem do perigo» — seja qual for o exato sentido que se tenha pretendido dar a esta expressão — ou que o Estado careça de invocar para aquele efeito, mesmo perante a «incerteza de que se reveste o fenómeno do terrorismo», uma «situação de perigo… de verificação altamente provável». Pensamos ainda que a maioria, no seu juízo de inconstitucionalidade da dimensão do artigo 4.º que submeteu ao teste da proporcionalidade, não discerniu corretamente a *natureza* e a *relevância* do controlo prévio assegurado pela formação especial do Supremo Tribunal de Justiça, designadamente como garante da concordância prática entre bens constitucionais.

*A*) *Interpretação do Artigo 34.º, n.º 4, da Constituição*

**4** — Segundo a decisão, «o n.º 4 do artigo 34.º da CRP conduz à inevitável conclusão de que o legislador constitucional resolveu explicitamente, no texto da Constituição, o sentido no qual devem ser resolvidas as eventuais colisões entre os valores constitucionalmente protegidos, e os correspetivos direitos fundamentais (...). [O] legislador constituinte retirou ao intérprete constitucional o espaço para encontrar…solução distinta para a operação de concordância prática em questão.» Acrescenta-se ainda que, «as ponderações entre direitos e valores constitucionais potencialmente em conflito foram já levadas a cabo pelo legislador constituinte», no sentido da *prevalência absoluta* da autodeterminação comunicativa sobre a tutela estatal de bens jurídicos fora do âmbito de um processo criminal pendente. Assim, a jurisdição constitucional, como «garante de um determinado parâmetro», deve respeitar a «operação de concordância prática realizada pelo legislador», a qual exprime uma «opção do poder constituinte democraticamente legitimado».

Todo este raciocínio, no nosso juízo, se encontra inquinado pela incompreensão das distinções essenciais entre *constituição* e *lei* e entre *interpretação constitucional* e *interpretação da lei* — precisamente aquelas diferenças que justificaram, na tradição constitucional europeia, a instituição de uma jurisdição especializada com características singulares para a administração da justiça constitucional.

A maioria parte do pressuposto de que a Constituição é uma *lei de valor reforçado* que exprime os juízos ou acolhe as preferências políticas de um legislador com uma legitimidade robustecida. De onde se segue que a interpretação constitucional não se distingue *essencialmente* da interpretação da lei, uma vez que ambas se destinam a discernir um *pensamento legislativo* ou a determinar uma *vontade política*. E por ser comum a natureza da interpretação nos dois casos, torna-se evidente o recurso aos subsídios hermenêuticos destilados pela doutrina tradicional da interpretação das leis — para além do «elemento literal ou gramatical de interpretação (a letra da lei)», como se afirma na decisão, «[também o elemento] sistemático, o histórico e o teleológico».

**5** — Partimos de premissas bem diversas.

A lei democrática exprime a vontade da maioria conjuntural legitimada nas urnas. Os atos legislativos não traduzem a unidade política dos cidadãos; ao invés, refletem o *pluralismo* das suas conceções sobre a sociedade justa e o bem comum, e o imperativo de que a controvérsia política que daí resulta seja arbitrada periodicamente através dos processos eleitorais da democracia representativa. A Constituição, pelo contrário, consubstancia um *pacto de vida comum* entre cidadãos divididos por compromissos mundividenciais concorrentes, a forma através da qual a pluralidade irredutível que é a matéria da comunidade política se estrutura numa *unidade* estável.

Assim, pode dizer-se que, ao passo que a lei democrática é na sua essência *formal*, no sentido de que o seu conteúdo varia de acordo com o juízo político que através dela se procura em cada momento expressar, a ordem constitucional é fundamentalmente *material*, porque radicada nas normas constitutivas de uma comunidade política de pessoas livres e iguais. Não admira, por isso mesmo, que o artigo 16.º da Declaração dos Direitos do Homem e do Cidadão, de 26 de agosto de 1789, porventura o mais emblemático dos documentos do constitucionalismo, tenha dado do conceito de constituição uma definição material: «A sociedade em que não esteja assegurada a garantia dos direitos nem estabelecida a separação dos poderes não tem constituição.»

Se é assim, se a vontade *constituinte* não é uma vontade *arbitrária*, mas *vinculada* pela sua natureza de vontade de constituir uma unidade política entre iguais, a compreensão do texto constitucional *pressupõe* o conceito material de constituição do Estado de direito democrático e os princípios de interpretação por ele *postulados*. Por outras palavras, aquele conceito e estes princípios são condição da possibilidade de compreender o texto constitucional, não como uma lei de valor mais ou menos reforçado, mas como *fundamento* da ordem jurídica da comunidade — o mesmo é dizer, como verdadeira e própria *constituição*.

Os princípios são aqueles que a teoria da interpretação *constitucional*, reagindo precisamente contra a redução da constitucionalidade a uma espécie do género da legalidade, vem articulando, com variações de nomenclatura, há cerca de um século: (i) o *princípio da unidade*: a ordem constitucional que resulta da interpretação possui uma coerência axiológica intrínseca; (ii) o *princípio da concordância*: a ordem constitucional que resulta da interpretação estabelece uma proporção entre os valores, direitos e bens que se destina a salvaguardar; (iii) o *princípio da integração*: a ordem constitucional que resulta da interpretação integra a pluralidade, devolvendo ao método democrático a regulação do dissenso político; (iv) e o *princípio da estabilidade*: a ordem constitucional que resulta da interpretação preserva a força normativa intertemporal através da abertura ao devir histórico.

São estes, por assim dizer, os «elementos» racionais ou lógicos da interpretação constitucional, os caminhos de uma hermenêutica que imprime ao texto a dignidade de fonte de uma normatividade *fundamental*.

**6** — Ora, a interpretação que na decisão se faz do n.º 4 do artigo 34.º da Constituição viola *todos* os princípios da interpretação constitucional.

Vejamos.

**6.1** — Em primeiro lugar, viola o *princípio da unidade*, na medida em que dela resulta uma ordem constitucional que concede níveis de tutela arbitrariamente diferenciados a realidades que relevam de *radicais axiológicos* comuns.

É indefensável a ideia de que o acesso a dados de tráfego de uma comunicação consumada ou tentada entre pessoas constitui *a priori* uma lesão *mais intensa* da *privacidade* e da *liberdade* do que o acesso a dados de localização de equipamento, que permitem determinar os movimentos do titular, ou a dados de tráfego de *internet*, que permitem reconstruir a navegação *online* do visado. De resto, comparando estes últimos com os dados de tráfego de comunicações através de serviços *online*, o próprio acórdão reconhece que a distinção é inviável, afirmando que, «face à semelhança dos valores e interesses afetados pelo tratamento não consentido de ambas as categorias de dados de internet e ao equivalente grau de danosidade que ele pode causar ao utilizador, a densidade de escrutínio a aplicar pela jurisdição constitucional à avaliação da escolha legislativa não [pode] ser menor em alguns deles.»

E, no entanto, entende-se na mesma decisão que a ordem constitucional exclui *categoricamente* o acesso aos dados de tráfego de «comunicações intersubjetivas», por via do n.º 4 do artigo 34.º, ao mesmo tempo que permite genericamente, ao abrigo do n.º 4 do artigo 35.º, desde que respeitados os limites gerais sobre a restrição de direitos fundamentais, o acesso aos demais dados pessoais — chegando-se ao ponto de afirmar que a jurisdição constitucional é «garante de um determinado parâmetro», como se fosse possível determinar o conteúdo de *um* parâmetro sem considerar a *unidade axiológica* da Constituição. Ou, mesmo na lógica seguida pela maioria, como se o Tribunal, no controlo da constitucionalidade das leis, pudesse atuar na condição de guardião de *um* e não de *todos* os parâmetros da Constituição.

**6.2** — Em segundo lugar, a interpretação do n.º 4 do artigo 34.º acolhida na decisão viola o *princípio da concordância*.

A garantia dos direitos e liberdades é uma tarefa fundamental do Estado, consagrada na alínea *b*) do artigo 9.º da Constituição, preceito que ecoa o artigo 2.º da Declaração de 1789, que enunciava: «A finalidade de toda associação política é a conservação dos direitos naturais e imprescritíveis...»

Ora, os direitos fundamentais têm funções *negativas* ou de *defesa* e funções *positivas* ou de *crédito*: aquelas correlativas do dever estatal de não agredir a esfera individual, através da restrição de direitos ou de liberdades; estas correlativas do dever estatal de *proteger* os indivíduos de comportamentos de terceiros ou perigos que afetam o gozo de bens. Na sua vertente negativa, os direitos fundamentais estabelecem limites à atuação do poder público, proibindo a compressão *excessiva* de direitos e liberdades; na sua vertente positiva, os mesmos direitos justificam e impõem a atuação do poder público, proibindo a proteção *insuficiente* de bens. Na verdade, segurança e liberdade são duas faces da mesma moeda: a segurança sem a liberdade é *inútil*, a liberdade sem a segurança é *impossível*.

Pela sua própria natureza, pois, a ordem constitucional proscreve simultaneamente o abuso do poder e o défice de proteção. A expressão natural deste equilíbrio é o princípio da *proporcionalidade*. Porém, segundo a leitura da maioria, a Constituição proíbe, *em termos absolutos*, a violação do sigilo das comunicações fora do âmbito de *um* processo criminal, independentemente das circunstâncias em que tal possa ocorrer ou do peso concreto dos imperativos de proteção que o reclamem. A ordem constitucional que resulta de uma tal interpretação não procura de modo algum a concordância entre liberdade e segurança no domínio da prevenção de perigos — antes sacrifica *cegamente* um dos valores, empenhando o modo de vida de que depende a realização de ambos.

**6.3** — Em terceiro lugar, a interpretação proposta na decisão viola o *princípio da integração*.

Uma ordem constitucional que se arroga a *última palavra* sobre «as ponderações entre direitos e valores constitucionais potencialmente em conflito» — entre as quais se destaca a tensão matricial entre liberdade e segurança —, em vez de devolver ao processo político democrático a gestão do dissenso entre os cidadãos sobre a correta ponderação a fazer em cada domínio da vida em sociedade, compromete a sua capacidade de reunir a pluralidade numa *casa comum*. A partilha dos valores do Estado de direito democrático postulada pelo constitucionalismo não implica nenhuma ficção de que os cidadãos estão de acordo quanto à interpretação e ponderação desses valores; reclama, sim, o reconhecimento constitucional do *princípio democrático*, como património comum de uma pluralidade irredutível, e a consequente vinculação do poder constituinte a *organizar* democraticamente a vida política, através de normas constitucionais relativas aos órgãos, competências e processos de decisão coletivos.

Numa democracia constitucional, a generalidade das ponderações que dividem *razoavelmente* a comunidade são confiadas ao processo legislativo ordinário e submetidas ao controlo de uma jurisdição dotada de legitimidade democrática indireta e incumbida de escrutinar mais ou menos intensamente a razoabilidade das opções tomadas. A ordem constitucional democrática *habilita* este processo de autodeterminação coletiva através da representação *eleitoral* pela assembleia legislativa e da representação *argumentativa* pela jurisdição constitucional.

Por outro lado, o «legislador constituinte» não goza de uma legitimidade democrática robustecida para se *antecipar* ao legislador ordinário na ponderação de valores constitucionais. Pelo contrário, os textos constitucionais mais democráticos são aprovados por simples decisão maioritária de uma assembleia constituinte ou dos cidadãos em referendo, exigindo por regra mais votos para a sua alteração do que os que foram necessários para a sua aprovação e proibindo necessariamente, de forma expressa ou implícita, a subversão da identidade constitucional pelo poder de revisão. Este aparente paradoxo dissolve-se se atentarmos em que a legitimidade democrática da ordem constitucional *não* se encontra de modo algum na suposta aritmética reforçada do processo constituinte, mas na capacidade de o texto constitucional, *corretamente interpretado*, honrar a promessa, encerrada no conceito material de constituição, de *integração* da pluralidade.

**6.4** — Finalmente, a leitura da maioria viola o *princípio da estabilidade*.

Uma ordem constitucional duradoira não se vincula definitivamente a uma conjuntura histórica, comprometendo-se com pressupostos empíricos que não pode garantir, hipotecando o seu futuro ao horizonte de sucessivas revisões constitucionais, submetendo os problemas constitucionais aos ritmos da política ordinária, arriscando a abertura de um fosso imenso entre norma e realidade — e, por tudo isto, degradando irremediavelmente a sua *força normativa* e *autoridade simbólica*.

Ressalvada a sua parte organizativa, que se traduz essencialmente num sistema de regras, o direito constitucional tende a consubstanciar-se em *princípios*, porque só assim possui a ductilidade indispensável ao cumprimento da sua vocação de norma *intertemporal* que integra a pluralidade numa unidade política estável. É especialmente perversa — e, no limite, absurda — a ideia de a ordem constitucional poder excluir em termos absolutos, através de soluções fechadas ao devir histórico, o uso de *meios proporcionais* para a sua própria defesa perante ameaças inteiramente novas ou velhas ameaças que se revestem de formas cada vez mais sinistras e agressivas.

Extrair da Constituição uma proibição categórica de *defesa administrativa* da ordem constitucional, através do acesso a dados de tráfego de «comunicações intersubjetivas», mesmo perante ameaças, como o terrorismo e a espionagem, que pelo seu potencial lesivo e ressonância simbólica vulnerabilizam as instituições fundamentais da democracia constitucional e põem em crise aguda a função preventiva da repressão penal, precipita o impossível dilema entre a *impotência* do poder público e a *ineficácia* das normas constitucionais.

**7** — Tudo visto, o único argumento relevante que parece aproveitar ao entendimento expresso na decisão baseia-se no *elemento literal* — no inciso final, «*em matéria de processo criminal*».

Com efeito, apesar da singularidade dos seus pressupostos e critérios, a interpretação constitucional não deve fazer tábua rasa da forma *escrita* ou *documental* das normas constitucionais. Ora, serão decerto de difícil resolução os casos em que se verifica uma contradição insanável entre o texto constitucional e os princípios da interpretação, ou seja, em que é de todo em todo impossível reconciliar a forma com a matéria do direito constitucional. Mas de tais casos — hipóteses porventura académicas, tendo em consideração a textura avisadamente aberta da semântica constitucional — não temos de nos ocupar, pois a isso não nos condena, ao contrário do que se entende na decisão, o teor literal do n.º 4 do artigo 34.º da Constituição.

Ao considerar que, nos termos e para os efeitos previstos nesse preceito, apenas são qualificáveis como casos de ingerência *em matéria de processo criminal* aqueles que tiverem lugar no *âmbito de um processo criminal pendente*, a maioria incorre num duplo equívoco. Para além de não fugir a uma interpretação do texto constitucional à luz do direito ordinário — procurando e encontrando neste a *categoria* que traduz o sentido daquele —, o juízo que fez vencimento não consegue superar, pelo menos de forma convincente, as dificuldades que ele próprio cria quando faz assentar a justificação última do recorte da exceção prevista no segmento final do n.º 4 do artigo 34.º da Constituição nas *garantias constitucionais do arguido,* e estas na *existência de um processo penal formalizado*, com o sentido que lhe é dado pelo Código de Processo Penal.

Demonstra-o, desde logo, a circunstância de o acesso a *dados de conteúdo* no âmbito de um processo penal — domínio em que o potencial de lesão de autodeterminação comunicativa é da *máxima* intensidade — se não encontrar dependente da constituição, nem *prévia,* nem *ulterior,* do suspeito como arguido. Uma vez instaurado o inquérito — o que ocorre sempre que for adquirida a notícia do crime, independentemente do conhecimento da identidade dos seus agentes (artigo 262.º, n.º 1) —, o juiz de instrução pode autorizar, nos termos previstos na lei, tanto a apreensão de correspondência (artigo 179.º, n.º 1), como a interceção e a gravação de conversações ou comunicações telefónicas (artigo 187.º, n.º 1), ainda que, por ausência de suspeita fundada quanto à autoria, o visado nunca chegue a ser constituído arguido (artigo 68.º, n.º 1, *a contrario*) e o inquérito acabe por ser arquivado (artigo 277.º, n.º 2, segunda parte).

Aquilo que, por força da Constituição, não pode em caso algum ocorrer — e é essa, mas apenas essa, a tensão a que responde *o direito das proibições de prova* —, é a *responsabilização criminal* de certo agente pela prática de determinado ilícito com base em elementos de prova obtidos através do acesso a dados de conteúdo, ou a dados de tráfego respeitantes a uma comunicação intersubjetiva, à margem de um processo penal formalizado e sem que aí tenham sido asseguradas todas as garantias de defesa inerentes ao estatuto de arguido.

Em matéria de dados de comunicação, as garantias que a pendência de um processo penal proporciona são aquelas que se *explicam* e *justificam* a partir da *finalidade punitiva* do processo: é na medida em que os elementos a que se acedeu poderão servir como *meio de prova* para sustentar uma condenação que ao arguido é assegurado o direito de contestar a sua validade — e logo, a sua atendibilidade — ao longo das diversas fases em que é suposto tomá-los em conta. Trata-se, por isso, de garantias que se situam numa fase *posterior,* e não prévia, à ingerência nas comunicações.

As garantias que a existência de um processo penal assegura *ex ante* — e, mais do que isso, aquelas que é *suscetível* de assegurar — são unicamente as que resultam da verificação dos *pressupostos legais* que condicionam a admissibilidade do acesso — tipo de crime, pena aplicável e relevância ou indispensabilidade da ingerência do ponto de vista das finalidades que com ela se prosseguem —, da exigência de uma *intervenção judicial* e, finalmente, do *juízo de ponderação* que para ela se convoca. Em suma, garantias semelhantes, como veremos, àquelas de que a Lei Orgânica n.º 4/2017 faz depender o acesso pelas autoridades do SIRP a dados de tráfego que envolvem comunicações intersubjetivas, *exclusivamente* para os fins previstos no seu artigo 4.º (produção de informações necessárias à prevenção da espionagem e do terrorismo) e nunca como elementos de prova em processo criminal.

**8** — Excluída a base em que assenta a equivalência que o acórdão estabelece entre o conceito de «matéria de processo criminal» e o conceito de «processo criminal pendente», a pergunta a que se impõe responder é a seguinte: Qual é, então, o *conteúdo positivo* da restrição à proibição de ingerência nos dados de comunicação que a Constituição autoriza no inciso final do n.º 4 do artigo 34.º? Ou, dito de outro modo, o que é exatamente «matéria de processual criminal»?

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 *retrospetiva,* 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 excecional 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 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.

Tal finalidade — isso parece isento de dúvidas — é *comum* ao acesso aos dados de tráfego pelas autoridades do SIRP, previsto no artigo 4.º da Lei Orgânica n.º 4/2017. Trata-se, também aqui, de um acesso *funcionalizado* à defesa de bens fundamentais da vida em comunidade contra formas de agressão, não só penalmente relevantes — e também por isso subsumíveis num conceito *material* de «processo criminal» —, como singularmente destrutivas da ordem constitucional. As medidas de acesso contempladas no artigo 4.º da Lei Orgânica n.º 4/2007 mantêm-se, assim, no âmbito da autorização constitucional para restringir a proibição de inviolabilidade dos meios de comunicação intersubjetiva, a qual, tendo na «matéria de processo penal» o seu pressuposto e limite, não pode deixar de abranger aquilo que, na categorização seguida pelo Tribunal de Justiça da União Europeia, se poderia designar aqui por «procedimentos de prevenção, de deteção ou de uma ação penal» (Acórdão *Digital Rights Ireland,* de 8 de abril de 2014, ponto 62). E este, como vimos, é *o único resultado interpretativo* compatível com os princípios da unidade, da concordância, da integração e da estabilidade que orientam a interpretação *propriamente* constitucional.

Concluímos, assim, que a Constituição permite o acesso pelas autoridades do SIRP, para cumprimento das finalidades aí previstas, a todo o universo de dados pessoais coberto pelos artigos 3.º e 4.º da Lei Orgânica n.º 4/2017, desde que observados os limites que decorrem do *regime geral* das restrições aos direitos, liberdades e garantias, designadamente a proibição do excesso. Em suma, a constitucionalidade das medidas de acesso depende, no essencial, do juízo sobre a sua *proporcionalidade*.

*B*) *Proporcionalidade do Acesso aos Dados de Tráfego*

**9** — Como vimos, a decisão atribui grande relevância constitucional a duas distinções dentro do universo dos dados pessoais cobertos pelos artigos 3.º e 4.º da Lei Orgânica n.º 4/2007. Por um lado, a distinção entre os dados de tráfego de «comunicações intersubjetivas» e os demais dados — de tráfego, de localização e de base; esta distinção releva da interpretação que a maioria faz do n.º 4 do artigo 34.º da Constituição, que demonstrámos ser insustentável. Por outro lado, a distinção entre os dados de tráfego cobertos pelo artigo 4.º — abrangendo, quer as «comunicações intersubjetivas», quer os dados de *internet* estranhos a uma comunicação consumada ou tentada «entre pessoas» — e os dados de base e de localização de equipamento cobertos pelo artigo 3.º

Assim se explica que na decisão se alcancem juízos opostos sobre a proporcionalidade das medidas de acesso autorizadas por aqueles preceitos. Entende-se que o acesso a dados de tráfego implica uma *lesão mais intensa da privacidade* do que o acesso a dados de base e de localização de equipamento, na medida em que aquele «possibilita conhecer as escolhas, comportamentos, hábitos, inclinações, gostos, vivências e centros de interesse do titular dos dados, e com base neles, avaliar e tipificar o seu comportamento e as suas particularidades». Daí que, mesmo na hipótese de o n.º 4 do artigo 34.º poder ser interpretado em termos que não proibissem liminarmente o acesso a dados de tráfego de «comunicações intersubjetivas», uma «análise mais atenta» do «regime de acesso aos *dados de tráfego* de comunicações pelos serviços de informações», consagrado na Lei Orgânica n.º 4/2017, sempre conduziria a idêntica conclusão, dada a *insuficiência* dos *mecanismos de controlo* previstos na lei — com a importante diferença de esta ordem de razões se estender a todos os tipos de *dados de tráfego* cobertos pelo artigo 4.º

Antes de nos debruçarmos sobre a questão da suficiência dos «mecanismos de controlo» previstos na lei, temos de salientar que, do ponto de vista constitucional, não há razão alguma para se enveredar por esta densa floresta de distinções. Em parte, o caminho seguido pela decisão deve-se ao modo como a maioria interpreta o n.º 4 do artigo 34.º da Constituição, matéria que já esgotámos. Mas deve-se ainda a uma ideia que se nos afigura insólita: a de que o acesso a dados de tráfego constitui *a priori* ou *por natureza* uma lesão mais intensa da privacidade do que o acesso, não apenas aos chamados «dados de base» — o que parece exato —, mas *também* aos «dados de localização de equipamento». Não compreendemos como a determinação exaustiva dos movimentos do titular através dos dados de localização de equipamento não possibilita, ou possibilita em medida *substancialmente* menor do que o acesso a dados de tráfego, o conhecimento das «esco-

lhas, comportamentos, hábitos, inclinações, gostos, vivências e centros de interesse do titular dos dados». Pelo contrário, tendemos a crer que, exceção feita aos dados de conteúdo, que se situam fora do âmbito de incidência da Lei Orgânica n.º 4/2017, a conexão entre dados de localização (ainda que estranhos a uma comunicação) e invasão da privacidade é particularmente evidente. E o que daí retiramos é que se justifica um juízo *global* e *uniforme* sobre a proporcionalidade das medidas de acesso a dados de tráfego e de localização, precisamente o contrário da ideia de uma «densidade de escrutínio a aplicar pela jurisdição constitucional» que varia consoante as diversas categorias de dados em causa.

**10** — Para verificar se as medidas contempladas nos artigos 3.º e 4.º da Lei Orgânica n.º 4/2007 superam os testes inerentes a um controlo baseado no princípio da proibição do excesso, partimos da premissa de que o acesso pelas autoridades do SIRP, quer a dados de localização de equipamento (artigo 3.º), quer a dados de tráfego (artigo 4.º), constitui uma *restrição severa* dos direitos de reserva de intimidade da vida privada e do livre desenvolvimento da personalidade. É por isso que tal acesso apenas pode ser admitido na presença de um «fundamento, preciso e determinado, na lei», para a prossecução do qual consubstancie um meio *adequado*, *necessário* e *proporcional*, e sempre na dependência de um procedimento apto a assegurar, em cada caso, que a ingerência na privacidade se limite ao mínimo necessário para alcançar a finalidade prosseguida e se mostre, tudo visto e ponderado, justificada.

Atentando no regime de acesso consagrado na Lei Orgânica n.º 4/2017, verifica-se que o mesmo contém um conjunto de «elementos tipificadores limitadores da ação» que, do ponto de vista da «densidade da moldura legislativa», o distanciam radicalmente daquele que foi objeto de apreciação no Acórdão n.º 403/2015, denotando ainda, quando com este confrontado, o propósito de dotar o sistema de mecanismos suficientemente aptos e credíveis para assegurar a fiscalização da legalidade das medidas, a defesa dos direitos dos cidadãos e, em última instância, a prevenção de abusos.

Por força dos critérios estabelecidos na lei, a possibilidade de ingerência das autoridades do SIRP nos dados encontra-se previamente limitada por uma tripla via: limitada pela *finalidade* para a qual pode ser autorizada — somente para «prevenção de atos de espionagem e do terrorismo» ou, no caso dos dados de localização de equipamento, ainda da prevenção de atos de sabotagem, proliferação de armas de destruição maciça e criminalidade altamente organizada (para além da «salvaguarda da defesa nacional e da segurança interna», consideradas como finalidades *a se*, o que julgamos inconstitucional pelas razões aduzidas no acórdão); limitada pelos pressupostos de *admissibilidade* do pedido de acesso — que apenas pode ser autorizado quando a diligência em causa for necessária, adequada e proporcional «para a obtenção de informação sobre um alvo ou um intermediário determinado» ou que «seria muito difícil ou impossível de obter de outra forma ou em tempo útil para responder a situação de urgência»; e limitada pelos *requisitos* do pedido de acesso — que apenas pode ser formulado com base numa «suspeita concreta e individualizada» e mediante a descrição detalhada dos «factos que o suportam» e a «identificação da pessoa ou pessoas afetadas [...] pelas medidas pontuais de acesso».

É verdade que, na modelação do regime de acesso, o legislador não prescindiu do recurso a um conjunto de conceitos indeterminados, como seja *«alvo determinado*», «*situação de urgência*», «*muito difícil de obter*» e «*tempo útil*». Todavia, o nível de indeterminação que o recurso a tais conceitos introduz não só tem evidente paralelo no próprio processo criminal que o acórdão toma por paradigma (artigo 187.º, n.º 1, do Código de Processo Penal), como, à semelhança do que ali sucede, serve também aqui o irrenunciável propósito de devolver ao órgão decisor a tarefa de concordância prática de direitos e bens no *caso concreto* e perante uma *suspeita individualizada e circunstanciada*.

Ao contrário do que se entende no acórdão, a respeito do acesso aos dados de tráfego, não cremos que fosse exigível ao legislador que enfrentasse a «incerteza de que se reveste o fenómeno do terrorismo» mediante a enumeração das «situações de facto que estão na origem do perigo». Ainda que se admitisse a possibilidade — no mínimo, duvidosa — de o legislador conseguir satisfazer esse nível de exigência, temos por certo que o sistema de acesso perderia grande parte da eficácia preventiva que constitui a sua razão de ser. Na verdade, não só a *densificação da moldura legislativa* foi levada tão longe quanto o permitido pela natureza da matéria regulada, como chega

ao ponto de ser uma virtude do regime, na medida em que a abertura dos conceitos que regulam o acesso é o veículo que possibilita aquela *casuística fina* através da qual o órgão de controlo define a fronteira entre a ingerência legítima e o abuso de poder. Subscrevemos, assim, tudo o que no acórdão se diz para fundamentar o juízo de não inconstitucionalidade das medidas de acesso previstas no artigo 3.º da Lei Orgânica n.º 4/2017, e que nos parece perfeitamente aplicável ao artigo 4.º

**11** — Do ponto de vista dos direitos dos indivíduos visados pelo procedimento, a atribuição da competência para autorizar o acesso aos dados a «uma formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções», constitui inequivocamente uma garantia da maior relevância. No exercício dessa função, caberá a tal formação subsumir nos conceitos legais de *«alvo determinado»,* «*situação de urgência*», «*muito difícil de obter*» e «*tempo útil*» os factos que lhe sejam submetidos e, através do juízo de ponderação para que remetem, decidir se a suspeita concreta e individualizada invocada pelas autoridades do SIRP tem o *grau de concretização* e o *nível de seriedade* necessários para justificar a ingerência na privacidade individual.

Esta intervenção do Supremo Tribunal de Justiça não é, ao contrário do que supõe a maioria, de *natureza administrativa.* É certo que a distinção entre as funções administrativa e jurisdicional se vai esbatendo à medida que nos afastamos dos casos paradigmáticos, como é aliás comum na generalidade dos conceitos jurídicos, e que a competência de controlo prevista na Lei Orgânica n.º 4/2017 se situa numa zona de indefinição, que porventura reúne características típicas de uma e a outra função. Mas há boas razões para se entender que a formação especial do Supremo Tribunal de Justiça é *ainda* um órgão judicial incumbido de exercer uma função *jurisdicional*. Por um lado, a atividade de controlo é *materialmente homóloga* daquela que, no âmbito de um processo penal pendente, é desempenhada pelo juiz de instrução quanto ao acesso a dados de conteúdo (artigo 187.º do Código de Processo Penal) e de localização celular (n.º 2 do artigo 189.º), sem que ocorra negar-se-lhe natureza jurisdicional. Por outro lado, os membros da formação são juízes, beneficiando das garantias de independência, inamovibilidade e irresponsabilidade e vinculados aos deveres de imparcialidade, defesa dos direitos e realização da justiça — garantias e deveres estes que integram o *estatuto* dos magistrados judiciais e a definição constitucional dos *tribunais*, precisamente porque se adequam ao desempenho da *função jurisdicional*.

De resto, o acórdão não retira todas as ilações da suposta natureza administrativa da formação especial do Supremo Tribunal de Justiça. Se a atividade desta integra a administração pública em sentido material, as normas da Lei Orgânica n.º 4/2017 que lhe atribuem competência são inconstitucionais, por violação do n.º 3 do artigo 216.º da Constituição, preceito de que se extrai uma proibição absoluta de os juízes exercerem a função administrativa. Acresce que este órgão de controlo, no entendimento de que não é um verdadeiro tribunal, não pode recusar a aplicação de normas inconstitucionais ao abrigo do artigo 204.º da Constituição, podendo fazê-lo apenas nas condições, francamente estreitadas pelo princípio da legalidade, em que seja admissível a chamada «fiscalização administrativa da constitucionalidade». Assim, debilita-se artificialmente a garantia dos direitos fundamentais.

São estas, em suma, as razões pelas quais nos afastamos do juízo que fez vencimento, convictos de que os «ataques terroristas indiscriminados se destinam, pela sua própria natureza, a plantar o medo no coração de civis inocentes, a causar o caos e o pânico e a perturbar o normal funcionamento da vida quotidiana»; e, ainda que, «em tais circunstâncias, as ameaças à vida humana, liberdade e dignidade surgem não apenas das ações dos próprios terroristas, mas também da reação das autoridades diante de tais ameaças» (Tribunal Europeu dos Direitos Humanos, Acórdão proferido pela *Grand Chamber* no caso *Ibrahim and Others v. The United Kingdom*, em 13 de setembro de 2016, ponto 293). Daí a necessidade imperiosa de um quadro legal neste domínio, como o estabelecido pela Lei Orgânica n.º 4/2017, que faça concordar, na medida do possível, a liberdade individual com a segurança coletiva. — *Gonçalo de Almeida Ribeiro* e *Joana Fernandes Costa*

**Declaração de voto**

**1** — Votei vencido quanto à declaração de inconstitucionalidade do artigo 4.º da Lei Orgânica n.º 4/2017, de 25 de agosto [que doravante identificarei como LO 4/2017 ou pelas iniciais de Lei dos Metadados (LM)], expressa na alínea *c*) do dispositivo[1]. Com efeito, pelas razões que explicitarei na presente declaração, considero que, no quadro das atribuições funcionais exclusivas dos serviços de informações integrantes do Sistema de Informações da República Portuguesa (SIRP), o acesso a *dados de tráfego* (o tipo de dados definido no artigo 2.º, n.º 2, alínea *c*), da LO 4/2017) pelos oficiais de informações do Serviço de Informações de Segurança (SIS) e do Serviço de Informações Estratégicas e de Defesa (SIED), para produção de informações necessárias à prevenção de atos de espionagem e do terrorismo, não viola o artigo 34.º, n.º 4 da Constituição da República Portuguesa (CRP) — ou seja, entendo que esse acesso é interpretativamente compatível com o segmento final da norma constitucional limitativa da ingerência das autoridades públicas nos *meios de comunicação* "[*aos*] *casos previstos na lei em matéria de processo criminal*". E considero, ademais, que o mesmo artigo 4.º da LM não consubstancia uma restrição desproporcionada (artigo 18.º, n.º 2 da CRP) ao n.º 1 do artigo 26.º e aos n.os 1 e 4 do artigo 35.º da CRP.

Refere-se o ponto 3. desta declaração à minha divergência com a posição maioritária (nesta parte tangencial: 7-6), nos específicos fundamentos que agregaram o voto dos sete Colegas que formaram esta maioria.

**1.1** — Concordo com o mais decidido no Acórdão. Ou seja, (i) votei a declaração de inconstitucionalidade do segmento do artigo 3.º da LO 4/2017, referido na alínea *a*) do dispositivo[2] (ii) e a não inconstitucionalidade do segmento da mesma norma identificado na alínea *b*) do dispositivo[3].

**1.1.1** — No caso da alínea *a*), concordando com o pronunciamento do Tribunal (com o sentido da decisão, com os parâmetros de desconformidade constitucional indicados e, no essencial, com a fundamentação), pretendo, no que tem o sentido de uma *opinião concorrente*, explicitar as particularidades do meu entendimento quanto à necessidade de introdução de uma filtragem temática precisa (como sucede, quanto aos dados de tráfego, no artigo 4.º da LM) no acesso dos serviços de informações a dados de base e de localização de equipamento. A este respeito, o entendimento que expus no voto de vencido formulado no Acórdão n.º 403/2015 carece de ser compaginado com as especificidades do quadro legal resultante da LO 4/2017. É fundamentalmente o que farei no item 2., *infra*, sem prejuízo de considerações de âmbito mais geral que reputo imprescindíveis à compreensão da minha posição.

**1.2** — Preambularmente, sistematizando o meu entendimento sobre a questão de constitucionalidade ora colocada, considero útil descrever comparativamente, nas duas manifestações que confrontaram este Tribunal no espaço de três anos, a opção do legislador parlamentar (assumida primeiramente em 2015 e enfaticamente reiterada em 2017) de dotar os dois serviços de informações integrantes do SIRP de acesso aos chamados *metadados* — dados, diversos do conteúdo das comunicações, gerados e previamente armazenados pelos prestadores de serviços de comunicações eletrónicas —, relativamente a campos temáticos específicos da atividade de produção de informações. Tal opção, agora expressa na LO 4/2017, apresenta assinaláveis diferenças relativamente à anterior iniciativa legislativa, corporizada no artigo 78.º, n.º 2, do Decreto n.º 426/XII da Assembleia da República[4], que foi inviabilizada por este Tribunal em fiscalização preventiva, em agosto de 2015, através do Acórdão n.º 403/2015 (do qual fui o relator originário, tendo ficado vencido).

Estando em causa, em ambas as situações, propiciar o acesso dos serviços de informações a esse meio de recolha de informação de base, em vista do seu ulterior tratamento no quadro da atividade de produção de informações — objetivo que, nesse enquadramento temporal, sempre foi protagonizado por maiorias parlamentares expressivas e transversais, que em qualquer dos casos seriam aptas a preencher o requisito de número previsto no artigo 286.º, n.º 1 da Constituição —, apresentam os dois textos (o Decreto n.º 426/XII em 2015 e a LO 4/2017) assinaláveis diferenças que agruparei em cinco áreas temáticas:

**(1)** O acesso à informação e a informação acedida.

**(a)** No artigo 78.º, n.º 2, do Decreto n.º 426/XII, previa-se que "[...] os *oficiais de informações do SIS e do SIED* [poderiam] [...] *aceder* [...] *a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar*

*e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização* [...]".

Agora, **(b)** nos artigos 3.º e 4.º da LO 4/2017, prevê-se, diferenciando o que anteriormente não o era, que "[*o*]*s oficiais de informações do SIS e do SIED podem ter acesso a dados de base e de localização de equipamento* [...]" (artigo 3.º) "[e] *a dados de tráfego* [...]" (artigo 4.º). Note-se que a definição das referidas categorias é agora detalhada no artigo 2.º, n.º 2, alíneas *a*), *b*) e *c*), nos termos seguintes: "*a*) «*Dados de base», os dados para acesso à rede pelos utilizadores, compreendendo a identificação e morada destes, e o contrato de ligação à rede*"; "*b*) «*Dados de localização de equipamento», os dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de telecomunicações que indiquem a posição geográfica do equipamento terminal de um serviço de telecomunicações acessível ao público, quando não deem suporte a uma concreta comunicação*"; "*c*) «*Dados de tráfego», os dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou no âmbito de um serviço de telecomunicações, ou para efeitos da faturação da mesma* [...]".

Esta diferenciação projeta-se na LO 4/2017 numa legitimação diferenciada quanto ao acesso a cada tipo de dados.

**(2)** A finalidade do acesso.

**(a)** No artigo 78.º, n.º 2, do Decreto n.º 426/XII, previa-se que o acesso aos dados ali previstos ocorria "[...] *para efeitos do disposto na* alínea *c*) do *n.º 2 do artigo 4.º, e no seu exclusivo âmbito*". No artigo 4.º, n.º 2, alínea *c*), do Decreto n.º 426/XII, estabelecia-se que "[...] *os serviços de informações desenvolvem atividades de recolha, processamento, exploração e difusão de informações:* [*a*]*dequadas a prevenir a sabotagem, a espionagem, o terrorismo, e sua proliferação, a criminalidade altamente organizada de natureza transnacional e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido*".

**(b)** Da conjugação entre os artigos 1.º, n.º 1, 2.º, n.º 3, 3.º e 4.º, da LO 4/2017, resulta que a conservação e transmissão pelos prestadores de serviços de comunicações eletrónicas dos dados: **(i**) respeita, *em geral*, a dados que se mostrem estritamente necessários para a prossecução da atividade de produção de informações pelo SIRP relacionada com a segurança interna, a defesa, a segurança do Estado e a prevenção da espionagem e do terrorismo (artigo 1.º, n.º 1); **(ii**) relativamente aos *dados de base e de localização de equipamento*, o acesso destina-se apenas à produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada e no seu exclusivo âmbito (artigo 3.º); e **(iii**), relativamente aos *dados de tráfego*, o acesso destina-se apenas à produção de informações necessárias à prevenção de atos de espionagem e do terrorismo (artigos 4.º e 10.º, n.º 2). Por outro lado, nos termos do artigo 11.º, n.º 2, da LO 4/2017, "[*o*] *acesso do pessoal do SIRP a dados e informações conservados em arquivo nos centros de dados do SIS e do SIED é determinado pelo princípio da necessidade de conhecer e só é concedido mediante autorização superior, tendo em vista o bom exercício das funções que lhe forem cometidas*".

**(3)** Entidade de controlo.

**(a)** Da conjugação do disposto nos artigos 78.º, n.º 2, 35.º e 37.º, n.º 3, do Decreto n.º 426/XII, resultava que o acesso aos metadados carecia de autorização prévia e obrigatória da designada *Comissão de Controlo Prévio*, na sequência de pedido devidamente fundamentado, sendo tal comissão composta por três magistrados judiciais, designados pelo Conselho Superior da Magistratura, de entre juízes conselheiros do Supremo Tribunal de Justiça (STJ), com pelo menos três anos de serviço nessa qualidade. A decisão seria tomada pelo elemento a quem tivesse sido distribuído o pedido, podendo haver decisões do coletivo em matérias de particular complexidade. Tratava-se essa *Comissão de Controlo Prévio*, como a qualifiquei no ponto 11.3 do voto de vencido no Acórdão n.º 403/2015, de uma *entidade administrativa independente*.

**(b)** Diversamente, na LO 4/2017, conjugando os respetivos artigos 1.º, n.º 1, 5.º e 8.º, resulta que o acesso aos dados: **(i**) depende de autorização judicial prévia e obrigatória, por uma formação especializada, dentro das secções criminais do STJ [nesse sentido foi alterada a Lei n.º 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário)], constituída nos termos do artigo 8.º, que garanta a ponderação da relevância dos fundamentos do pedido e a salvaguarda dos direitos,

liberdades e garantias constitucionalmente previstos — esta formação é constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções; e **(ii**) o processo de autorização é sempre comunicado ao Procurador-Geral da República (artigo 5.º, n.º 2).

**(4)** Critério da autorização.

**(a)** O artigo 36.º, n.º 2 do Decreto n.º 426/XII, previa que "[*o*] *pedido para a concessão de autorização prévia* [seria] *decidido ponderando a relevância dos seus fundamentos e a salvaguarda dos direitos, liberdades e garantias constitucionalmente previstos*". Tal autorização seria concedida ou negada por despacho fundamentado, proferido em 72 horas, podendo ser reduzido a 24 horas no caso de urgência (artigo 37.º, n.os 4 e 5).

**(b)** Ora, comparando com o Decreto n.º 426/XII, o critério de autorização na LO 4/2017, apresenta-se substancialmente densificado, resultando da atuação concatenada de diversos fatores de limitação expressamente indicados na lei: **(i)** o pedido só pode ser autorizado quando houver razões para crer que a diligência é necessária, adequada e proporcional para a obtenção de informação sobre um alvo ou um intermediário determinado, ou para a obtenção de informação que seria muito difícil ou impossível de obter de outra forma ou em tempo útil para responder a situação de urgência (artigo 6.º, n.º 1); **(ii)** a apreciação judicial da necessidade, adequação e proporcionalidade do pedido, designadamente no que se refere à justa medida da espécie e da escala de informação obtida, compreende a definição das categorias de dados de telecomunicações e Internet a fornecer pelos operadores, segundo um juízo restritivo de proibição do excesso que interdita o acesso indiscriminado a todos os dados de telecomunicações e Internet de um determinado cidadão, bem como a definição das condições de proteção do segredo profissional (artigo 10.º, n.º 1); **(iii)** o acesso é determinado pelo *princípio da necessidade de conhecer* e só é concedido tendo em vista o bom exercício das funções que forem cometidas ao pessoal do SIRP [artigo 11.º, n.º 2]; e **(iv)** o controlo judicial pela formação das secções criminais do STJ visa garantir o respeito pelos direitos, liberdades e garantias e pelo princípio da legalidade da recolha, assegurando, nomeadamente, que os dados são: recolhidos para finalidades determinadas, explícitas e legítimas; e adequados, pertinentes e não excessivos relativamente às finalidades para as quais são recolhidos (artigo 12.º, n.º 1).

A autorização é concedida ou negada por despacho, proferido no prazo de 48 horas, que pode ser reduzido, no caso de urgência, ao mais breve possível (artigo 10.º, n.os 3 e 4).

**(5)** Elementos do pedido.

**(a)** O artigo 37.º, do Decreto n.º 426/XII, adjetivando o controlo prévio aí em causa, previa, no seu n.º 2, que o pedido de acesso contivesse: **(i)** a indicação concreta da ação operacional a realizar e das medidas requeridas; **(ii)** os factos que suportavam esse pedido, finalidades que o fundamentavam e as razões que aconselhavam a adoção das medidas requeridas; **(iii)** a identificação da pessoa ou pessoas, caso sejam conhecidas, envolvidas nos factos em causa no pedido de acesso e das pessoas afetadas pelas medidas, além da indicação do local onde as mesmas devessem ser realizadas; e **(iv)** a duração das medidas requeridas, que, em qualquer caso, não poderia exceder o prazo máximo de três meses, prorrogáveis mediante autorização expressa.

**(b)** No artigo 9.º, n.º 2, da LO 4/2017, retoma-se o regime que constava do Decreto n.º 426/XII, apenas com a seguinte alteração na alínea *d*), referente aos elementos necessários ao pedido de acesso: indicação da "[...] *duração das medidas pontuais de acesso requeridas, que não pode exceder o prazo máximo de três meses, renovável por um único período sujeito ao mesmo limite, mediante autorização expressa, desde que se verifiquem os respetivos requisitos de admissibilidade*". Adicionalmente — no que traduz um elemento central do regime introduzido em 2017 —, prevê-se no n.º 3 do mesmo artigo 9.º, constituírem, para efeitos da LO 4/2017, "[...] *«medidas pontuais de acesso» as providências de recolha de dados, por transferência autorizada e controlada caso a caso, com base numa suspeita concreta e individualizada, que não se prolongam no tempo, sendo a sua duração circunscrita, e que não se estendem à totalidade dos dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, não admitindo a aquisição de informação em larga escala, por transferência integral dos registos existentes, nem a ligação em tempo real às redes de comunicações eletrónicas*" (sublinhado acrescentado).

**1.2.1** — Para além de outras diferenças entre os dois textos no plano da proteção de dados (cf. o artigo 14.º da LO 4/2017, *vs.* artigos 29.º e ss. e 37.º, n.º 8, do Decreto n.º 426/XII) e quanto ao Conselho de Fiscalização do SIRP (artigo 15.º da LO 4/2017, *vs.* artigos 21.º e ss. do Decreto n.º 426/XII), merecem destaque, ainda, os seguintes preceitos da LO 4/2017: **(i)** é proibida a interconexão em tempo real com as bases de dados dos operadores de telecomunicações e Internet para o acesso direto em linha aos dados requeridos (artigo 6.º, n.º 2); **(ii)** a transmissão diferida dos dados de telecomunicações e Internet obtidos de acordo com o regime consagrado na lei processa-se mediante comunicação eletrónica, com conhecimento da formação judicial prevista no artigo 8.º e ao Procurador-Geral da República, nos termos das condições técnicas e de segurança fixadas em portaria do Primeiro-Ministro e dos membros do governo responsáveis pelas áreas das comunicações e da cibersegurança, que devem observar um grau de codificação e proteção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados, sem prejuízo da observância dos princípios e do cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados, previstos na Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto, e na Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto, que a republicou, sob fiscalização e controlo da Comissão de Fiscalização de Dados do SIRP, nos termos da presente lei (artigo 11.º, n.º 1; a Portaria aqui prevista foi, entretanto aprovada — trata-se da Portaria n.º 237-A/2018, de 28 de agosto); **(iii)** a formação das secções criminais do Supremo Tribunal de Justiça valida o tratamento pelo SIS ou pelo SIED dos dados de telecomunicações e internet considerados em conformidade com o disposto no artigo 12.º, n.º 1 (artigo 12.º, n.º 2); **(iv)** compete à mesma formação judicial determinar a todo o momento o cancelamento de procedimentos em curso de acesso a dados de telecomunicações e internet, bem como ordenar a destruição imediata de todos os dados obtidos de forma ilegal ou abusiva, ou que violem o âmbito da autorização judicial prévia, bem como os dados que sejam manifestamente estranhos ao processo, nomeadamente quando não tenham relação com o objeto ou finalidades do pedido ou cujo tratamento possa afetar gravemente direitos, liberdades e garantias (artigo 12.º, n.º 3); **(v)** o Procurador-Geral da República é notificado das decisões de cancelamento de acesso e de destruição dos dados, para efeitos do exercício das suas competências legais (artigo 12.º, n.º 4); e **(vi)** a Comissão de Fiscalização de Dados do SIRP é notificada das decisões de cancelamento de acesso e de destruição dos dados, para efeitos do exercício das suas competências legais em matéria de proteção dos dados pessoais (artigo 12.º, n.º 5).

**1.2.2** — Ora, pressupondo os elementos evidenciados pela perspetivação da atuação do Legislador nesta matéria desde 2015, em vista da concretização do firme propósito, que se intui da reiteração, de dotar os serviços de informações portugueses de um instrumento de trabalho considerado básico na prossecução da sua função, importa abordar as questões antes enunciadas nos itens 1. e 1.1.1., que correspondem aos problemas especificamente decorrentes do(s) julgamento(s) do Tribunal. Embora o meu posicionamento quanto ao decidido seja diverso relativamente a cada uma das normas consideradas, entendo que a questão de fundo — que é, desde de 2015, a viabilidade constitucional do acesso dos serviços de informações a metadados — perspetiva alguns argumentos comuns às duas situações, cuja consideração constará, indiferenciadamente, dos pontos 2. [*a inconstitucionalidade parcial do artigo 3.º da LO 4/20179*] e 3. [*a inconstitucionalidade (afirmada pela maioria*) d*o artigo 4.º da LO 4/2017*] do texto deste voto.

**A inconstitucionalidade parcial do artigo 3.º da LO 4/2017**

**2 —** Na alínea *a*) do dispositivo o Tribunal declarou — por uma maioria na qual me integro — a inconstitucionalidade parcial do artigo 3.º da LO 4/2017, relativa ao acesso dos serviços de informações a *dados de base* e *de localização de equipamento*, por referência à definição constante do artigo 2.º, n.º 2, alíneas *a*) e *b*), do mesmo diploma, quando a fundamentação da pretensão de acesso a esses dados se refira, sem mais, à *salvaguarda da defesa nacional* e da *segurança interna*; ou, dito de outro modo, implícito no pronunciamento do Tribunal, quando a pretensão de acesso não se baseie "[...] *numa suspeita concreta e individualizada* [...]" (artigo 9.º, n.º 3, da LM) referida à "[...] *prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada* [...]" (artigo 3.º, da LM).

Neste caso o Tribunal, retomando uma referência constante do Acórdão n.º 403/2015 (no antepenúltimo parágrafo do respetivo ponto 15[5]), excluiu que o artigo 34.º, n.º 4 da CRP constitua parâmetro válido de aferição da constitucionalidade da norma (cf., no presente Acórdão, o terceiro parágrafo do ponto 8 da fundamentação, depois repetido no primeiro parágrafo do ponto 12). Daí que os referentes de desconformidade constitucional desta vertente da decisão sejam, por via de um controlo de proporcionalidade, os artigos 26.º, n.º 1, e 35.º, n.os 1 e 4, da CRP: relativamente a estes — é o que resulta do pronunciamento do Tribunal —, o artigo 3.º da LM passa nos testes de proporcionalidade, estando em causa os âmbitos temáticos indicados na alínea *b*) do dispositivo, mas já não passa, concretamente numa *avaliação de proporcionalidade em sentido estrito*, nas referenciações temáticas genéricas indicadas na alínea *a*) do dispositivo.

**2.1** — Sublinha-se o sentido garantístico que este confinamento temático — no qual assenta a construção da permissão de acesso no artigo 4.º da LM — aporta à resolução da questão de constitucionalidade que nos interpela. Com efeito, correspondem as expressões-conceito *defesa nacional* e *segurança interna* (contrariamente ao que sucede com referenciações — como o terrorismo e a espionagem — cuja base de identificação tem correspondência em descrições típicas) a domínios demasiado genéricos e vagos de identificação do objeto da atividade dos serviços de informações, extravasando, quando tomadas (invocadas) isoladamente como fundamento de uma ação a desenvolver por esses organismos, do grau de precisão que a introdução do filtro das descrições penais, como referências mediatas, necessariamente propicia. Isto vale, pois, com o sentido de uma garantia acrescida contra um uso desviado desta atividade do Estado. Ou seja, o emprego destes meios pelos serviços de informações, por razões de contenção da interferência assim potenciada ao estritamente necessário, e de efetividade do controlo judicial estabelecido na LM (nos artigos 5.º, n.º 1, 8.º, 10.º e 12.º), não pode bastar-se com uma identificação muito genérica do espaço de atuação desses serviços, carecendo antes de uma delimitação temática mais precisa, dentro do seu espaço funcional geral, através da qual seja possível identificar elementos concretos demonstrativos da existência de uma relação equilibrada entre as vantagens alcançadas pela interferência e os desvalores induzidos por esta. É que, se essa aferição é possível quando apreciamos realidades cujos contornos existenciais estão previamente definidos — quando falamos de terrorismo, de espionagem, e de outros conteúdos típicos cujas manifestações, mesmo situadas numa fase larvar e ainda pouco precisa, são passíveis de identificação, desde logo nos seus atos percursores —, torna-se muito mais problemática quando tal aferição é referida a conceitos vagos naturalmente propensos à ambiguidade significativa.

**2.1.1** — Esta construção, induzindo um espaço temático de atuação dos serviços de informações que partilha referências da perseguição criminal, manifestando-se, não obstante, em momentos e planos muito distintos desta, traz à liça a questão da diferenciação funcional entre as estruturas que protagonizam as duas tarefas. Trata-se de um problema da maior importância, com indiscutível relevância constitucional, que nos situa no âmago da diferenciação entre a função estadual de produção de informações, adstrita aos serviços de informações, e a função de polícia, na sua referenciação à perseguição criminal, como atividade auxiliar da justiça penal.

Note-se que estamos, em qualquer caso, perante *mundos separados*, que atuam com base em racionalidades bem distintas e visando objetivos muito diferentes, embora, como *mundos paralelos* que não deixam de ser, designadamente ao lidarem com certos aspetos dos mesmos fenómenos[6], "[*comunguem*] *algumas dimensões* [...]"[7]. Tal paralelismo, sugerindo, à superfície, a existência de semelhanças, pode induzir algum enviesamento na diferenciação entre produção de informações e atividade policial, esquecendo que a essência da diferença, a despeito de uma ou de outra partilha de certos ambientes de trabalho, permanece inequívoca e tem nessa separação uma teleologia própria: evitar mútuas poluições de efeito espúrio, contendo a atividade de cada um dos organismos no espaço funcional que lhe é próprio e que justifica o acervo de meios de atuação respetivos.

A aproximação que aqui empreendemos a este problema — procurando o sentido dessa diferenciação — assentará na caracterização da função de produção de informações, captando o sentido finalístico desta atividade do Estado, daí sendo dedutível, quase por evidência, o quanto ela é diversa da perseguição criminal e da atividade de polícia, e, acrescente-se, o quanto ela, em termos das consequências que projeta, fica aquém da potencialidade de interferência com os direitos individuais presente na perseguição criminal.

**2.1.1.1** — Encetando esse percurso, procurando uma concetualização da atividade de produção de informações — a atividade protagonizada pelos serviços de informações aos quais (e em função da qual) a LO 4/2017 adjetiva o acesso a metadados — somos conduzidos a um conceito abrangente que gerou, no mundo anglo-saxónico, um termo genérico (*intelligence*, que entre nós vale para *produção de informações*). Através deste referencia-se o resultado, o *produto final* visado, decorrente da agregação intencional de um conjunto de atividades, numa dinâmica que se descreve como cíclica — correspondente ao que usualmente se designa como *ciclo de produção de informações*, envolvendo planificação, recolha de informação, análise e disseminação[8]. Estas atividades são conduzidas em segredo[9], visando um resultado expresso na manutenção ou melhoramento do ambiente de segurança, pela antecipação de fatores gerais ou já concretizados de risco e ameaça, visando possibilitar a implementação atempada (útil) de políticas ou de estratégias de prevenção, e mesmo a adoção de medidas concretas no âmbito de outros quadros funcionais[10], quando o produto informacional adquirido por via do processamento da informação (da análise) expresse incidências conducentes a uma resposta desse tipo. Esta, quando situada a um nível mais concreto, significará invariavelmente a saída da situação do domínio funcional da produção de informações (designadamente através da entrada em campo da adjetivação penal; é essa, aliás, a intencionalidade que se expressa na intervenção no processo de autorização de acesso a metadados do Procurador-Geral da República, prevista nos artigos 9.º, n.º 1, e 11.º, n.º 1 da LO 4/2017). Ou seja, podemos ver a produção de informações como expressão de uma prática social omnipresente na atividade dos Estados, combinando processos de aquisição sistematizada de conhecimento e de exercício do poder visando a gestão do risco, pela redução do fator incerteza[11].

Ora, ilustrando o campo de atuação próprio da produção de informações — e sublinhando à partida a evidente diferença estrutural com a perseguição criminal, que parte do conhecimento de uma realidade fática específica, expressa na existência ou indiciação de um crime em concreto, sendo desencadeada e orientada retrospetivamente por este, adjetivando um resultado consequencialmente previsto para essa ocorrência —, podemos caracterizar (recorrendo ao texto indicado na nota 8, *supra*) as alternativas e as gradações de complexidade que geram, num quadro que interiorize o fator precaução, a procura de respostas, situadas nesse domínio funcional da atividade do Estado ao qual chamamos produção de informações:

"[...]

*No caso em que a tomada de decisão ocorre num quadro de certeza, conhecemos o resultado das diferentes escolhas possíveis e o único desafio refere-se à clarificação das preferências. No caso do risco, conhecemos os resultados possíveis (os efeitos benéficos ou adversos) e a probabilidade de ocorrência dos vários resultados. No caso da incerteza, conhecemos os possíveis resultados, mas não dispomos de base objetiva para estimar a probabilidade respetiva. No caso da ignorância nem sequer são conhecidos que efeitos adversos antecipar, ou desconhecemos a sua magnitude ou relevância, e não dispomos de pistas quanto à probabilidade de ocorrência.*

*No primeiro caso não existe espaço para a 'produção de informações', como tal; nas restantes três situações a 'produção de informações' adquire crescente importância — e dificuldade.*

[...]" (sublinhados acrescentados)[12].

Pressupõe a função policial, quando direcionada à adjetivação penal, elementos factualmente expressos, indutores de uma objetivação comportamental que afastam o essencial dos elementos de incerteza e de fluidez na referenciação concreta que observamos nas situações indicadas (*risco*[13], *incerteza*, *ignorância*) como correspondendo ao espaço próprio da atividade de produção de informações e, consequentemente, de atuação dos serviços de informações. A entrada em cena da tutela penal não corresponde, obviamente, a um termo dessa escala, não expressando decisões num quadro que possamos identificar com o termo *certeza*, menos ainda um quadro que possamos definir como aberto a uma eleição de preferências. Expressa a tutela penal, todavia, na sua génese ativadora, um quadro consequencialmente condicionado por elementos pretéritos — um evento que se prefigure como criminalmente relevante — de significado suficientemente claro, nas suas incidências jurídicas, que (já) postula o recurso aos mecanismos aptos a alcançar, em última análise, a resposta reintegradora que só pode ser propiciada no quadro da tutela penal.

**2.1.1.2** — Por outro lado, sobrevaloriza-se na visão que tende a confundir produção de informações e atividade policial — a qual reputamos de inadequada a qualquer das duas atividades e estranha ao nosso modelo constitucional — a presença circunstancial do que qualificamos como "*pontos de contacto*" — áreas de proximidade — entre as duas funções. Com efeito, embora ocorram, em algumas situações, coincidências temáticas no material fáctico de base tratado pelas duas atividades, não afasta essa incidência, longe disso, a profunda diferença de lógicas e de objetivos visados por cada uma das funcionalidades e das estruturas que as protagonizam. Esta confusão entre serviços de informações e autoridades policiais, que é gerada por aparências enganadoras e, em grande medida, alimentada por mitos[14], deve ser esclarecida, descodificando-se o sentido que esses tais "*pontos de contacto*" apresentam numa democracia constitucional, cujo quadro referencial é absolutamente incompatível (diametralmente antitético) da (com *a*) confusão, ou apropriação funcional mútua.

Essa sobreposição de funções, que está bem além da mera proximidade e nega o paralelismo, corresponde, aliás, a um modelo conatural aos regimes totalitários, traduzindo-se frequentemente no que se designa como *polícia política*. Ora, não sendo esse, como é óbvio, o modelo e o concreto enquadramento legal dos serviços de informações portugueses, designadamente pressupondo o acesso por estes a metadados adjetivado na LO 4/2017, direi, recorrendo ao *exagero retórico* através do qual Richard Posner repudia a mesma ideia: "[*t*]*hey are intelligence agencies, operating by surveillance rather than by prosecution. Critics who say that an American equivalente of MI5 would be a Gestapo understand neither MI5 nor the Gestapo*"[15]. Esconjura-se, assim, por redução ao absurdo, a ideia muito presente neste tipo de debates, fruto de desconhecimento ou de preconceitos, segundo a qual uma estrutura policial, atuando no quadro da perseguição criminal, comportaria menos riscos relativamente à proteção dos direitos fundamentais do que a atuação de um serviço de informações, no seu espaço funcional legítimo num regime democrático. Esquece-se, porém, que reduzindo as coisas ao seu verdadeiro significado, o que subsiste na perseguição criminal, e se realiza na adjetivação penal (e que constitui atividade absolutamente estranha e totalmente vedada aos serviços de informações), corresponde à forma de atuação do Estado com maior potencial agressivo sobre os direitos individuais: a que conduz à aplicação de sanções criminais e pode envolver, *in itinere*, a sujeição a medidas de coação fortemente compressoras dos direitos individuais.

A afirmação dessa diferença, no quadro em que aqui nos movemos, é inequívoca, como decorre da caraterização da atividade de produção de informações traçada por Miguel Nogueira de Brito: "[...] *os serviços de informações* [...] *atuam num plano que antecede a atividade policial de controlo de perigos. O propósito da sua atuação não obedece ao objetivo direto de implementar medidas de controlo de perigos ou de investigação criminal. As informações por si reunidas visam antes fundar a avaliação e decisão políticas que depois se manifestarão de diversos modos, por exemplo, através da criação de procedimentos contra associações ou partidos contrários à Constituição ou do desenvolvimento de programas sociais destinados a pessoas sujeitas a extremismos de vária ordem. Compreende-se, assim, que os serviços de informações não tenham típicas competências de polícia, mas apenas a competência de mobilizar meios tendentes à captação e tratamento de informação*"[16].

Ora, uma correta abordagem da questão de constitucionalidade colocada na presente fiscalização abstrata deve assumir plenamente a distinção entre os dois domínios funcionais, projetando o sentido profundo dessa diferença na perspetivação da conformidade constitucional de quaisquer permissões de acesso a informação para ulterior processamento por parte dos serviços de informações. Estamos, pois, perante uma relevante questão, a qual, aliás, não é específica da nossa ordem jurídico-constitucional, importando esclarecê-la.

**2.1.1.3** — A separação substancial dos dois mundos (serviços de informações, autoridades policiais) tem um óbvio sentido, correspondendo o quadro geral de uma diferenciação inequívoca entre as duas funções a exigências de controlo e de contenção de cada um dos domínios funcionais da atividade do Estado dentro do respetivo enquadramento constitucional. Isto não invalida, porém, que uma completa estanquicidade comunicacional desses dois mundos possa corresponder, na sua exacerbação, a um exagero sem sentido, concretamente quando a diferenciação se manifeste na total ausência de mecanismos propiciadores de algum tipo de comunicação, gerando perdas

de eficiência em domínios tangenciais das duas funções, sempre que o custo deste efeito não corresponda à perversão do valor constitucional promovido com a separação entre produção de informações e a perseguição criminal.

O caráter estanque da separação — e estamos a ilustrar esta ideia com um exemplo —, assente, aliás, na existência de mecanismos de travagem ou de neutralização da comunicação interagências, vigorou incontestada no espaço norte-americano até ao início deste século, sendo aí identificada pela sugestiva expressão "*The Wall*"[17]. Esta descreve procedimentos específicos e a estruturação organizacional de uma barreira absoluta de comunicação entre a CIA e o FBI e, quanto a este último, entre as funções de *intelligence* e de *law enforcement* (que razões históricas muito específicas fizeram coincidir, embora em estruturas separadas, na mesma organização). Foi essa separação severamente criticada, na sequência dos ataques de 11 de setembro de 2001, pelo relatório da designada Comissão Nacional de Inquérito[18], que considerou essa separação um fator gerador da falta de antecipação desses eventos, isto num quadro em que existiam "pedaços" de informação relevante "dos dois lados do muro", que, separados por essa barreira, nunca se encontraram, perdendo assim toda a coerência significativa que — todavia "após o facto" visto como consequencial — adquiriram[19].

**2.1.1.4** — No espaço europeu — e estamos a caraterizar em traços muito largos um processo particularmente complexo —, a incidência do que se designa como *terrorismo internacional jihadista*[20] induziu uma cooperação reforçada entre serviços policiais e de informações, tanto ao nível nacional como transnacional (é este, aliás, o quadro motivacional do legislador português, na LO 4/2017, como já havia sucedido em 2015 com o Decreto n.º 426/XII). Ora, foi o ajustamento constitucional desse novo quadro relacional que gerou pronunciamentos do Tribunal Constitucional Federal Alemão — e centramo-nos num país cuja comunidade de informações assenta num modelo que apresenta similitudes à estrutura do SIRP — que consideramos importantes, mas cujo sentido deve ser devidamente esclarecido, obstando a um uso descontextualizado dessas decisões. Convém lembrar que a opção de propiciar acesso a metadados aos serviços de informações portugueses (um acesso que é, todavia, muito limitado) é tributária da perceção de uma deterioração crescente do ambiente de segurança internacional, relativamente à ameaça terrorista transnacional, que justifica, ponderadas as especificidades de cada país, um outro (um novo) olhar sobre a atividade de produção de informações.

Nesse enquadramento, em 2013, foi o *Bundesverfassungsgericht* confrontado com uma queixa constitucional dirigida à criação de uma Base de Dados tematicamente dedicada ao terrorismo internacional, gerida (alimentada) conjuntamente por serviços de cariz policial e serviços de informações[21] — referimo-nos ao recurso que originou a Sentença de 24/04/2013 (*1BvR*, *1215/07*). Sendo esse contexto decisório totalmente distinto do aqui em causa (não existe equivalente desse instrumento entre nós; as bases de dados dos dois serviços integrados no SIRP não são, em si mesmas, partilhadas com autoridades policiais, nem tão-pouco o são entre os dois serviços[22]), e não esquecendo que o Tribunal Constitucional alemão considerou a existência dessa base conjunta compatível, nos seus elementos essenciais, com a Constituição alemã[23], importa reter o equacionar pelo Tribunal, nesse contexto, das condições em que se deve processar a circulação de informação entre serviços de informações e estruturas policiais (pontos 111 a 123 do Acórdão). A este respeito, reconhecendo que a essência funcional dos serviços de informações, direcionada à recolha de informação antecipadamente à configuração de uma ameaça concreta, sendo esta deduzida da presença de fatores que reconhecidamente funcionam como precursores, considerou o Tribunal, no quadro de um controlo de proporcionalidade referido ao direito à autodeterminação informacional, como valor constitucional relativizado pela construção e funcionamento dessa base de dados, a necessidade de a circulação dos dados contidos na base projetar a licitude da aquisição destes no âmbito funcional do recetor, ficcionando a conformidade da aquisição por este, em função do respetivo conteúdo funcional e meios de atuação. Ficcionando, pois, uma "mudança do propósito" que presidiu originariamente à aquisição desses dados, do âmbito da produção de informações para o da perseguição criminal ou vice-versa, configurando uma "*hipotética recolha de dados*" (*hypothetische datenneuerhebung*) no quadro da outra função envolvida na partilha [cf. os pontos 116 a 119 do Acórdão de 2013, no essencial retomados nos pontos 320 e 286 da Sentença do mesmo Tribunal de 20/04/2016 (*1 BvR, 966/09 e 1 BvR 1140/09*)[24]].

Este modelo de análise, concretizado num controlo de proporcionalidade, projeta os valores inerentes à especificidade de cada uma das funções na sua expressão no nível confrontacional do direito à autodeterminação informacional que cada um deles envolve. Ora, neste balanceamento, o Tribunal Constitucional Federal Alemão ponderou a menor expressão das limitações legais aos poderes de aquisição de dados por parte dos serviços de informações (que constitui, todavia, uma especificidade alemã sem equivalente na nossa ordem jurídica), como interferência justificável pelo menor potencial agressivo da atividade de produção de informações, comparativamente à perseguição criminal, que conduz (é apta a conduzir) à aplicação de penas criminais (cf. os pontos 117 a 119 e 120 a 123 do Acórdão de 2013).

Importa precisar, desde logo — e trata-se de um aspeto relevante para a presente questão de constitucionalidade —, a estranheza das questões centrais tratadas nas duas decisões consideradas do *Bundesverfassungsgericht* à matéria que nos ocupa. Aqui, no contexto da LO 4/2017 (tanto no caso do artigo 3.º como do artigo 4.º), estamos perante autorizações judiciais individualizadas de acesso a metadados, especificamente concedidas aos serviços de informações, que são apreciadas e decididas nesse particular âmbito, visando especificamente o tratamento dessa concreta informação no quadro funcional desses serviços[25]. Estamos, pois — e configuraria uma outra questão, deslocalizada da LM, fazendo toda a diferença neste contexto —, fora de qualquer mecanismo de partilha de dados, sendo o afastamento dessa incidência controlado pela formação judicial autorizante, através da subsistente validação do tratamento dos dados cujo fornecimento foi autorizado, concomitantemente à incidência de outros níveis de controlo. Ora, para além de sublinhar essa radical diferença, vale a comparação das duas situações como ilustração da criteriosa preocupação do legislador português de reduzir o acesso dos serviços de informações a este tipo de dados a níveis mínimos de intrusividade.

**2.2** — Numa outra perspetiva da questão de constitucionalidade referida ao artigo 3.º da LM, inexistindo violação do artigo 34.º, n.º 4 da CRP — e, para mim, tanto não existe no caso do artigo 3.º como no do artigo 4.º do Diploma, por serem ambos interpretativamente compatíveis com o trecho final da norma constitucional: "[...] *casos previstos na lei em matéria de processo criminal*" —, subsiste desta norma constitucional, quando encaramos a atividade dos serviços de informações, uma indicação interpretativa de que a atuação destes só poderá consubstanciar uma exceção à proibição constitucional de ingerência das autoridades públicas nos meios de comunicação se expressar uma realidade — digamo-lo assim — de alguma forma compaginável com o sentido primordial da adjetivação penal. Situando o argumento interpretativo, relativo ao sentido do trecho final do n.º 4 do artigo 34.º da CRP, numa perspetiva histórica — que adiante aprofundarei e que deve ser compaginada com o elemento teleológico — creio ser esta a *mensagem normativa* que a subsistência desse trecho inculca no intérprete.

Isso mesmo referi — em termos que ora reitero — no voto de vencido no Acórdão n.º 403/2015 (cf. o respetivo item 6.), ao caraterizar a intencionalidade da função de produção de informações, no quadro do SIRP, quando instrumentada com o acesso a dados deste tipo, "[...] *como um sistema estruturado em vista do desencadear de mecanismos de alerta prévio, uma função sequencialmente referida ainda a um momento anterior ao da entrada em jogo — rectius, da adjetivação — da tutela penal, mas que, nem por isso, deixa de estar ligada aos valores específicos (aos tipos) abarcados pela lei penal, e de poder mesmo vir a entroncar na adjetivação penal*". Assim, a atividade dos serviços de informações que, "[...] *num espaço de legitimidade constitucional* [...]", disponha destes instrumentos — acesso a dados de base e de localização e, até mais ainda, a dados de tráfego — tenha de assentar em condicionalismos de densificação que propiciem a referenciação temática a um espaço situado "[...] *na antecâmara da tutela penal, numa fase ainda larvar desta,* [...] *onde os respetivos valores, mesmo que em termos difusos e ainda com um significado ambíguo, já estejam demonstravelmente presentes, já tenham, enfim, sido colocados nalgum tipo de insegurança existencial minimamente concretizada e individualizada* [, em que essa atividade] *incid*[*a*] *sobre condutas individuais ou coletivas que contenham uma potencialidade, não negligenciável de menoscabo, mesmo que embrionário, dos valores próprios de uma 'ordem fundamental livre e democrática', quando esse desvalor seja reportável* [...] *potencie, ou torne racionalmente expectável, uma evolução que, em última análise, nos conduza a condutas penalmente típicas, referenciáveis*

*aos valores estruturantes dessa* [*ordem*] *em particular o terrorismo* [a] *espionagem e outros dos crimes contra o Estado* [...]".

E, enfim, creio ser com este sentido que deve ser entendida a referência a "*criminalidade grave*" por parte do Tribunal de Justiça da União Europeia (TJUE), no contexto decisório do Acórdão de 21/12/2016 (processos n.os C-203/15 e C-698/15; *Tele2 Sveridge c. Post-och telestyrelsen* e *Secretary of State for the Home Department c. Tom Watson e outros*): "[*o*] *artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União*" [ponto 2) da decisão, com sublinhado acrescentado[26]]. Deve notar-se, porém, para uma exata compreensão do sentido da jurisprudência europeia sobre esta matéria — e adiante, no item 3., aprofundarei esta asserção —, que o TJUE fixou este entendimento [no que vale igualmente para o Acórdão de 08/04/2014, *Digital Rights Ireland Ltd.* (C-293/12), que invalidou a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações], apreciando e controlando situações de acesso pelas autoridades públicas, não filtrado e em massa (a chamada recolha de dados *em massa*, *bulk metadata collection*), às bases de dados das operadoras. Vale esta advertência como diferenciação das situações de acesso individualizado — sem acesso às bases de dados das operadoras e mediante controlo, protagonizado por uma estrutura exterior ao destinatário dos dados, dos pressupostos de acesso nessa situação específica — como aquelas em causa no quadro da LO 4/2017: este Diploma — o tipo de acesso a metadados nele adjetivado — sempre valerá com um sentido *ad minus*, relativamente ao mencionado acesso em massa apreciado pelo TJUE[27], sendo certo que todos os condicionalismos estabelecidos no *direito do caso* do TJUE estão salvaguardados na adjetivação estabelecida na LO 4/2017; e isto sem embargo de todos esses condicionalismos terem sido estabelecidos num contexto diametralmente oposto ao aqui em causa — na sua essência (que o caso *Ministerio Fiscal*, aludido na nota 26, *supra*, aliás, intui por uma espécie de *redução teleológica*) referem-se essas decisões a transferências de dados em massa das bases das operadoras para os serviços de informações, ou visando propiciar um acesso direto a essas bases, tudo consequências que a LO 4/2017 expressamente afasta.

**A inconstitucionalidade (afirmada pela maioria) do artigo 4.º da LO 4/2017**

**3 —** O Tribunal, na alínea *c*) do dispositivo, declarando a inconstitucionalidade do artigo 4.º da LM, inviabilizou o acesso dos serviços de informações a *dados de tráfego*. Esse pronunciamento decisório diferencia, na indicação dos parâmetros de desconformidade constitucional, a existência, ou não, de uma comunicação intersubjetiva, reportando a violação do artigo 34.º, n.º 4, da CRP, aos casos envolvendo esse circunstancialismo, e a violação dos artigos 26.º, n.º 1 e 35.º, n.os 1 e 4, por via do artigo 18.º, n.º 2, todos da CRP, às situações que não pressupõem comunicação intersubjetiva.

Constituem os *dados de tráfego* — e estamos sempre a pressupor as definições constantes da LM — um subgrupo dentro do grupo geral formado pelos "*dados de telecomunicações*" e pelos "*dados de internet*" (artigo 2.º, n.º 1, alíneas *a*) e *b*), da LM). Estes, agregados, correspondem aos "[...] *dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas* [...]" cujo acesso pelos serviços de informações a LO 4/2017 permite e regula (cf. o respetivo artigo 1.º, n.º 1), sendo diferenciados no artigo 2.º, n.º 2, alíneas *a*), *b*) e *c*), da mesma Lei, em vista da respetiva recondução à permissão de acesso do artigo 3.º (relativa a dados de base e de localização de equipamento) ou do artigo 4.º (respeitante a dados de tráfego), com distintas condições de acesso num e noutro caso. Vale isto por dizer, centrando-nos nos dados de tráfego — "[...] *os dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou no âmbito de um serviço de telecomunicações, ou para efeitos da faturação da*

*mesma*" (artigo 2.º, n.º 2, alínea *c*), da LM) —, que estes incluem "*dados de telecomunicações*" e "*dados de Internet*".

Independentemente da distinção criada pelo Tribunal entre dados de tráfego que envolvem, ou não, comunicação intersubjetiva, correspondendo ao meu entendimento que o artigo 34.º, n.º 4, da CRP, no seu trecho final limitativo — "[*aos*] *casos previstos na lei em matéria de processo criminal*" —, não é incompatível com o acesso dos serviços de informações ao tipo de dados de tráfego em qualquer caso visados no artigo 4.º da LO 4/2017, concretamente nas condições estabelecidas neste Diploma, apreciarei essa questão à margem da distinção introduzida pelo Tribunal[28].

Claro que, ultrapassada a questão do artigo 34.º, n.º 4, da CRP, que constituiu o elemento central da argumentação do Tribunal em 2015, surge, na indagação de conformidade constitucional do artigo 4.º da LO 4/2017, a necessidade de levar a cabo um controlo de proporcionalidade (artigo 18.º, n.º 2, da CRP) quanto ao acesso a dados de tráfego estabelecido nesse artigo 4.º, por referência ao âmbito de proteção dos artigos 26.º, n.º 1 e 35.º, n.ºs 1 e 4, da CRP.

Isolarei de seguida, na crítica à posição da maioria de rejeição do artigo 4.º da LM, essas duas dimensões.

**3.1** — À questão da compatibilização interpretativa do artigo 34.º, n.º 4 da CRP com o acesso a dados de tráfego pelos serviços de informações se referem os dois votos discrepantes formulados no Acórdão n.º 403/2015. No meu voto (cf. os pontos 10., 10.1. e 10.2) considerei — e estou a adaptar o que então escrevi — que a fidelidade ao sentido querido pelo legislador constitucional, atualizado por referência à realidade social do presente (tanto a de 2015 como a atual), reclama um ajustamento interpretativo do que a maioria formada a este respeito subsistentemente encara como uma inultrapassável proibição literal contida no n.º 4 do artigo 34.º da CRP. Configura-se este ajustamento como abertura ao que qualifiquei em 2015 como *redução teleológica*, retirando algo ao âmbito da proibição (observo agora que, em rigor, poderíamos até descrever a atuação desse ajustamento por via interpretativa como *ampliação teleológica*, acrescentando algo à permissão de interferência).

Confronta-nos esta questão com o contexto histórico que desencadeou o aparecimento na Constituição da República Portuguesa de 1976, desde a versão inicial elaborada pela Assembleia Constituinte — entre 2 de junho de 1975 e 2 de abril de 1976 —, de uma disposição restringindo aos "[...] *casos previstos na lei em matéria de processo criminal*" a exceção à proibição de "[...] *toda a ingerência das autoridades públicas na correspondência e nas telecomunicações* [...]", integrada no segmento final seguinte norma:

*Artigo 34.º*

***(Inviolabilidade do domicílio e da correspondência)***

*1 — O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis.*

*2 — A entrada no domicílio dos cidadãos contra a sua vontade só pode ser ordenada pela autoridade judicial competente, nos casos e segundo as formas previstos na lei.*

*3 — Ninguém pode entrar durante a noite no domicílio de qualquer pessoa sem o seu consentimento.*

***4 — É proibida toda a ingerência das autoridades públicas na correspondência e nas telecomunicações, salvo os casos previstos na lei em matéria de processo criminal.***

[após a revisão constitucional de 1997, correspondendo ao texto atual: *4. É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações* ***e nos demais meios de comunicação****, salvo os casos previstos na lei em matéria de processo criminal.*]

Na projeção desse contexto histórico, não é relevante — não é interpretativamente relevante — especular com a localização no tempo de um suposto *pensamento constituinte* referido (e limitado) àquilo que, nos anos setenta do século passado, existia e era previsível vir a existir em termos de meios de telecomunicações. Tratar-se-ia, com um indisfarçável pendor serôdio, de uma discussão aparentada à da natureza da eletricidade, para efeitos de integração do crime de furto.

Aliás, essa (suposta) questão foi tratada e solucionada pelo legislador constituinte no quadro da revisão de 1997, integrando no referido n.º 4 o inciso, já acima indicado, "[...] *e nos demais meios de comunicação* [...]", abrindo à evolução futura a cobertura constitucional da inviolabilidade dos meios de comunicação[29].

Coisa diferente já será ponderar se a particular natureza dos chamados metadados, como dados circunstanciais de uma comunicação, diversos do conteúdo desta, representam — todos eles — exatamente o mesmo, sem possibilidade de introdução de diferenciações. Note-se que a existência de espaço interpretativo no artigo 34.º, n.º 4 para a ponderação de considerações gradativas, quanto à potencialidade interferente dos diversos tipos de dados nele considerados, foi assumida pelo Tribunal Constitucional no Acórdão n.º 403/2015, e é repetida no presente Acórdão, embora, em qualquer dos casos, para negar a aplicação da referida disposição constitucional, tão-somente, aos dados de base e de localização (cf., no texto deste voto, o item 2. e respetiva nota 5).

E a isto acresce, correspondendo ao entendimento que expressei no voto de vencido de 2015, o sentido em que a diferenciação entre *dados de tráfego* e *dados de conteúdo* (de cujo acesso o legislador assumiu a opção de excluir os serviços de informações) é relevante, dando corpo, na compreensão do trecho final do n.º 4 do artigo 34.º, a uma distinta consideração dos *metadados*, enquanto *dados sobre dados*, no confronto com os *dados* em si mesmos (correspondentes aos *dados de conteúdo*): aqueles, dando algum contexto a estes últimos, expressam circunstâncias periféricas de uma realidade que em si mesma não revelam. É com esse particular sentido, visando determinar a potencialidade interferente dos *dados de tráfego*, que o entendimento do Tribunal Constitucional no Acórdão n.º 486/2009, adquire um valor subsistentemente persuasivo (remete-se de novo para o terceiro parágrafo do ponto 8 da fundamentação do presente Acórdão), nos termos que indiquei nesse voto de vencido (cf. o respetivo ponto 9.2.)[30]. Aí, referindo-me especificamente à atividade de produção de informações, objetei à ideia, agora reafirmada pela maioria de rejeição do artigo 4.º da LM, de não existência de qualquer espaço de tangibilidade das autoridades públicas nas *telecomunicações e nos demais meios de comunicação*, no quadro do n.º 4 do artigo 34.º da CRP, relativamente a um enquadramento funcional com a peculiaridade da atividade de produção de informações — cuja potencialidade agressiva dos valores nesse quadro tutelados é bastante atenuada relativamente à adjetivação penal —, quando essa atividade protagonizada pelos serviços de informações, se refere à *proteção da segurança e à preservação da própria ordem constitucional*[31], sendo tematicamente orientada para a deteção precoce, ou numa fase larvar, do tipo de fenómenos indicados no trecho final do artigo 4.º da LM: atos de espionagem e do terrorismo.

A sugestão da estrutura verbal de uma *regra*, presente no n.º 4 do artigo 34.º, da CRP, cujo espaço de realização seria — só seria — o *tudo ou nada* da efetiva existência de um concreto processo criminal, priva o legislador — não se limitando a orientar fortemente a sua atuação — de considerar valores constitucionais conflituantes, mesmo que de *primeiríssima grandeza*[32], desconsiderando que referir *matéria de processo criminal* pode não representar exatamente o mesmo que processo criminal, *tout court* [veja-se o n.º 3 do artigo 252.º-A, do Código de Processo Penal; a maioria consideraria este (ao prever uma intromissão sem processo) inconstitucional?].

Com efeito, considero que essa estrutura significativa não se adequa, salvo raras exceções, à projeção interpretativa de normas materialmente constitucionais. Estas, pela sua natureza identitária, expressa, desde logo, no caráter *único* da fonte pela qual se manifestam[33], postulam, na captação da *mensagem* (normativa) que o texto incorporada, uma aproximação que seja sensível à ponderação de fatores que revelem o contexto significativo da expressão verbal encontrada no momento constituinte, permitindo o seu (re)posicionamento no presente. É que (e cito de novo o meu voto de vencido de 2015), "[...] *a letra da lei — de qualquer lei, obviamente também a lei constitucional, que é, paradigmaticamente, uma lei interpretativamente aberta — é o primeiro passo na complexa tarefa de a interpretar, mas não simultaneamente o derradeiro passo nesse sentido* [...]*, poderá então o seu sentido literal sofrer ajustamentos reclamados por outras considerações (sistemáticas, desde logo, sem perder de vista a concreta realidade social que reclama a aplicação da norma*)".

**3.1.1** — Assim, é na perspetivação histórica da restrição da ingerência das autoridades públicas nas telecomunicações — e nos demais meios de comunicação — aos "[...] *casos previstos na lei em matéria de processo criminal*", no contexto do n.º 4 do artigo 34.º da CRP, que logramos alcançar o sentido atuante que, no presente, à distância de décadas, corresponde a essa limitação.

Com efeito, importa ter presente que uma Constituição, "[...] *reflete acontecimentos do passado, estabelece as fundações do presente, e dá forma ao futuro* [sendo]*, ao mesmo tempo, filosofia, política, sociedade e direito*"[34]. É esta peculiar natureza, sempre presente nas normas que a integram, que faz sobressair, no contexto interpretativo, o propósito ou a função visada com o texto, projetando essa intencionalidade, historicamente situada, no presente. A interpretação neste quadro abre, pois, "[...] *espaço à adaptação das expressões legais* [empregues] *à modificação das circunstâncias e à emergência de novos desafios, desde que o objetivo e a função* [daquelas] *não seja alterado pelo aplicador: nem toda a mudança de sentido requer uma revisão constitucional*"[35].

É relevante, contribuindo decisivamente para a compreensão da norma interpretanda, recordar o contexto em que ocorreu a aprovação desta na Assembleia Constituinte.

Está em causa a discussão e votação do que correspondeu, nos trabalhos da Assembleia Constituinte, ao *artigo 21.º* do projeto respeitante ao Título dos *Direitos, liberdades e garantias*[36], refletindo este o que veio a corresponder, no texto final da Constituição de 1976, exatamente ao artigo 34.º atual [este, ressalvada a alteração de 1997 antes referida (cf. nota 29, *supra* e texto ao qual se refere), mantém-se desde 2 de abril de 1976]. A redação utilizada como base da discussão então travada, apresentava o seguinte conteúdo:

*Artigo 21.º*

*1 — O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis.*

*2 — É proibida, designadamente, toda a ingerência das autoridades públicas na correspondência e nas telecomunicações, salvo os casos previstos na lei em matéria de processo penal.*

*3 — 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. Ninguém pode entrar durante a noite no domicílio senão com o consentimento da pessoa aí domiciliada.*

Este texto, cujo n.º 2 veio a corresponder ao n.º 4 do artigo 34.º, foi aprovado por unanimidade quanto aos n.os 1 e 2. Relativamente ao n.º 3, foi apresentada uma proposta de alteração pelo Deputado Américo dos Reis Duarte, da *UDP* (*União Democrática e Popular*, que elegeu um Deputado à Assembleia Constituinte), com o seguinte teor: "*3 —* [*a*] *entrada no domicílio dos cidadãos só pode ser ordenada por decisão de um tribunal popular ou de uma comissão de moradores, nos casos segundo as formas a decidir pelas assembleias populares*" (esta proposta foi rejeitada, recolhendo apenas o voto do proponente)[37].

Esta vicissitude particular, referindo-se a uma questão distinta da aqui diretamente relevante, revela uma parte do contexto histórico desta, sendo aqui indicada por ilustrar bem um dos polos motivacionais do legislador constituinte em 1975, na adoção do regime consubstanciado no artigo 34.º, com a limitação constante do n.º 4 (decorrente do n.º 2 do referido artigo 21.º).

Desde logo — correspondendo a um desses polos — valeu, no contexto limitador de ingerências das autoridades no domicílio, correspondência e nas telecomunicações, a memória traumática, então (em 1975) ainda bem presente, da PIDE/DGS, cuja atuação arbitrária nesses domínios constituía um elemento central da prática da polícia política do regime derrubado em 25 de Abril de 1974[38], coroando o novo texto constitucional a reversão dessa situação. Da mesma forma — e corresponde ao outro polo motivacional a considerar, ilustrado pelo episódio da Assembleia Constituinte acima relatado —, a recondução ao aparelho judicial comum da autorização de exceções às limitações de ingerência das autoridades nesses domínios, concretamente no das telecomunicações, visou materializar o afastamento das ditas "*legalidades revolucionárias*" — por oposição à legalidade democraticamente legitimada, pela eleição da Assembleia Constituinte — geradas no decurso do processo revolucionário de rutura com o regime derrubado em 25 de Abril de 1974. Refiro-me a factos históricos conhecidos e a um processo de institucionalização da democracia portuguesa no qual a Constituição de 1976 (e a Revisão Constitucional de 1982) constituíram marcos históricos referenciais[39]. Sendo esse o contexto histórico da opção constitucional que ora nos interpela, dela permanece — como realidade historicamente atual — a essência assumidamente limitadora — exigentemente limitadora e justificadamente desconfiada —, no plano que aqui nos

interessa, da ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação.

Essa essência, que permanece atual, deve, porém, ser historicamente situada no presente, abarcando os desafios deste e captando as novas circunstâncias que modelaram essa essência ao longo de mais de quatro décadas, até ao limite onde seja possível reconhecer a presença atuante daquela ideia fundamental. Note-se que o legislador, se perspetivarmos diacronicamente a sua atuação no plano temático que aqui nos interessa — o da perspetivação da função de produção de informações, designadamente quanto aos meios de atuação dos serviços de informações — foi cautelosamente sensível aos desafios que o confrontaram.

**3.1.1.2** — Com efeito, a sociedade portuguesa foi atingida nas décadas de 70/80 do século passado por diversos desafios à segurança interna, protagonizados pelo fenómeno do terrorismo, tanto internacional como de âmbito doméstico. Quanto à primeira dimensão (terrorismo internacional), cabe salientar, no final dos anos 70 e começo dos anos 80, de um ciclo de ações, iniciado em novembro de 1979 com um atentado, que causou vítimas mortais, ao Embaixador de Israel em Portugal, prolongando-se esse ciclo até julho de 1983, com o ataque por um grupo arménio à Embaixada da Turquia (que provocou 7 mortos)[40]. Configurando terrorismo doméstico — descontando os fenómenos anteriores a 1976 (rede bombista) —, foi a sociedade portuguesa atingida na década de 80 pela atuação de um grupo terrorista nacional, as designadas *Forças Populares 25 de Abril* (FP/25). Traduziu-se isso, como sempre sucede naquilo que usualmente se qualifica como "refluxo revolucionário", num desvio para a "ação direta" de alguns dos "perdedores" (a franja mais radical deles) do conturbado processo de transição democrática portuguesa, numa espécie de reprodução tardia de um fenómeno que nos anos 70 do século XX foi visível em Itália, nas "Brigadas Vermelhas", e na República Federal Alemã, com a "Fração do Exército Vermelho"[41].

Note-se que a criação do SIRP, e concretamente a instalação do SIS em 1984, como primeiro serviço de informações civil subsequente ao 25 de Abril (ultrapassando a produção de informações atinentes à segurança interna pelas estruturas militares, sem enquadramento legal), ocorreu, consequencialmente, a culminar a sucessão de eventos acabados de relatar. Todavia, porque as manifestações desse fenómeno sempre se traduziram na prática concreta de crimes, o elemento reativo passou, como não podia deixar de suceder, pela perseguição penal. A isto acresceu o caráter limitado desses fenómenos (episódicos e situados num espaço temporal pequeno) e a sua ultrapassagem, sem que eles revelassem uma necessidade imediata de configurar um plano de atuação diverso para os serviços de informações.

A necessidade de revisitar este cenário só teve lugar no início deste século (a partir de 2001), com o 11 de setembro e a perceção do caráter global da ameaça que esse evento patenteou. Embora se tenha revelado, nesse contexto, um fenómeno radicado no passado (na segunda metade dos anos 90), só então foi verdadeiramente induzida uma perceção do fenómeno do *terrorismo internacional jihadista* como ameaça à escala global, assente em vertentes de muito difícil perceção precoce, que justificaram (e justificam persistentemente) o investimento de meios na produção e troca de informações, no plano transnacional. Foi a compreensão deste desafio pelo legislador nacional que justificou, num plano de resposta mínima e cautelosa (adaptada à perceção de uma intensidade ainda não muito expressiva dessa ameaça em Portugal), as iniciativas legislativas que desde 2015 confrontam o Tribunal Constitucional, quanto ao acesso, muito limitado, dos serviços de informações ao tipo de material informacional de base, correspondente aos metadados comunicacionais.

**3.1.2** — Valeu para o legislador, no assumir desta opção, o que antes se descreveu como indicação do contexto que a história (que aqui abarca um período de quarenta anos) conferiu ao trecho final limitativo constante do n.º 4 do artigo 34.º, da CRP. Porque, como referimos, citando Dieter Grimm (cf. a nota 35), "[...] *nem toda a mudança de sentido requer uma revisão constitucional*", valendo as opções legislativas cuja essência atualize o sentido do que, em sede constitucional, se estabeleceu no passado. É assim que o entendimento atual que propugno relativamente ao trecho final do artigo 34.º, n.º 4 da CRP, não afeta a essência significativa que este, historicamente perspetivado no presente, conferiu, face a novos desafios, à proibição de ingerência das autoridades públicas nas telecomunicações e demais meios de comunicação, sendo o acesso limitado

e particularmente restritivo decorrente do artigo 4.º da LO 4/2017, interpretativamente compatível com esse segmento final da norma constitucional.

**3.2** — Ultrapassada esta questão, subsiste a necessidade de realizar, com base no artigo 18.º, n.º 2, da CRP, um controlo de proporcionalidade do acesso a dados de tráfego pelos serviços integrantes do SIRP, tendo presente a interferência que esse alcance implica relativamente ao direito à reserva da intimidade da vida privada (artigo 26.º, n.º 1, da CRP) e à proteção nesse âmbito contra o uso da informática, no plano do direito de acesso aos dados pessoais próprios e de restrição do acesso aos dados pessoais por terceiros (artigos 35.º, n.os 1 e 4, da CRP).

A exigência desse controlo decorre, desde logo, da previsão, no artigo 18.º, n.º 2, da CRP, do confinamento das medidas de restrição de direitos ao necessário à salvaguarda de outros direitos e interesses constitucionalmente protegidos, sendo essa exigência enfatizada, no plano do Direito da União, pelo TJUE no Acórdão *Tele2* (referido *supra* no ponto 2.2.), quando estão em causa, como aqui é evidente suceder, medidas nacionais que comportam algum grau de interferência e de relativização do princípio da confidencialidade das comunicações e dos correspondentes dados de tráfego (cf. os pontos 88 a 91 do Acórdão *Tele 2*).

Mesmo neste quadro [o decorrente do Direito da União (artigo 15.º, n.º 1, primeiro período da Diretiva 2002/58, na versão inicial recuperada pelo Acórdão *Digital Rights*) e especificamente referido aos direitos fundamentais reconhecidos na Carta dos Direitos Fundamentais da União Europeia] vale, por identidade de razão, um controlo de proporcionalidade integrado pelos testes da *adequação*, *necessidade* e *proporcionalidade em sentido estrito*, não esquecendo, aliás, que o acesso e controlo individualizado, como único tipo de acesso estabelecido na LO 4/2017, retira, projetando-se fortemente em qualquer apreciação da potencialidade interferente do acesso a dados de tráfego, como uma clara limitação a essa incidência desvaliosa, pela eliminação do efeito de *arrastão*, abstrato e desprovido de bases de suspeição concretas, como o induzido por um trabalho de pesquisa direto sobre grandes bases de dados, à margem de um controlo concreto, prévio, de pertinência e de necessidade de acesso à informação visada[42]. Tudo isto são perigos que o legislador nacional, à partida, esconjurou.

**3.2.1** — Quanto à incidência do primeiro teste de proporcionalidade, sendo evidente a adequação do acesso a dados de tráfego pelos serviços de informações, para um cabal desempenho da tarefa de produção de informações necessárias à prevenção de atos de espionagem e do terrorismo, podemos afirmar a integração desse elemento de controlo. Assim se afasta a existência — como corresponde à essência da ideia de adequação da restrição induzida — a existência, por via do acesso autorizado, de um ato lesivo sem contribuição alguma para a realização de um fim constitucionalmente relevante.

**3.2.2** — No plano do controlo da *necessidade* da medida, ficcionando alternativas que, proporcionando o mesmo grau de satisfação do interesse público, sejam menos restritivas dos interesses afetados, deparamo-nos, no caso dos metadados, com um nível de interferência diminuto com as comunicações eletrónicas, preservadas de qualquer possibilidade de acesso ao *núcleo duro* representado pelo conteúdo destas. Especificamente quanto aos dados de tráfego, observamos a utilidade destes num quadro em que o tratamento de informação visa, por via da ponderação de dados meramente circunstanciais, propiciar o conhecimento de elementos relacionais que objetivamente expressem uma relação objetivada com os fatores de ameaça pretendidos antecipar. Menos que isto, só pode significar o não acesso a metadados, em contraciclo com a totalidade dos serviços de informações europeus, que partilham o nosso espaço de referências constitucionais.

**3.2.3** — Finalmente, quanto à *proporcionalidade em sentido estrito*, cujas múltiplas manifestações de conformidade foram já referidas por diversas vezes ao longo deste voto, retemos aqui alguns pontos específicos, em vista da caraterização do acesso a dados de tráfego como expressão de uma relação equilibrada no balanço entre os valores em causa na prossecução do objetivo subjacente à opção legislativa assumida e o nível de restrição da posição afetada por essa opção.

Não vale neste quadro a descrição do acesso individualizado a dados de tráfego pelos serviços de informações, com base num exigente controlo judicial externo de pertinência, como "[*redução dos cidadãos*] *a identidades digitalmente criadas e heteroconstruídas, baseadas em perfis defini-*

*dos por terceiros, com a consequente desumanização das pessoas e estandartização dos seus comportamentos, aniquilando-se a privacidade e condicionando-se a liberdade, assim acabando por perverter a democracia*" (citei o penúltimo parágrafo do ponto 11.2.4. do texto do Acórdão). A descrição deste cenário *fantasmagórico* não tem a mais remota relação com o tipo de acesso individualizado estabelecido pelo legislador português relativamente a todo o tipo de metadados. Os *perfis* em causa — usando a terminologia do Acórdão —, são definidos por terceiros, no sentido em que o são os elementos típicos de um crime, aqui atuantes nos domínios temáticos referidos no artigo 4.º da LM, com um claro sentido de filtragem de referências muito abstratas, desviantes de um acesso propiciado pela referenciação concreta num quadro de proximidade à ameaça. A diferença, para referir o óbvio quanto ao suposto efeito de etiquetagem que o trecho acima transcrito parece pretender sugerir, é que a produção de informações não induz as graves consequências decorrentes da adjetivação penal.

De facto, faz toda a diferença relativamente ao cenário construído no Acórdão, a circunstância de o acesso se processar individualizadamente, com base numa construção particularmente restritiva, que afasta o perigo envolvido num acesso massificado e não filtrado pela instância de controlo. Esse perigo, que é real noutras ordens jurídicas[43] — e que dá sentido à jurisprudência do TJUE neste domínio —, é pura e simplesmente neutralizado pelo exigente ponto de equilíbrio estabelecido pelo legislador português, podendo afirmar-se que o regime constante da LO 4/2017 cumpre plenamente os critérios estabelecidos no Acórdão *Tele 2*: (i) a limitação do acesso ao âmbito da luta contra a *criminalidade grave*; (ii) a sujeição desse acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente; (iii) e a garantia de conservação dos dados em território da União.

**3.2.3.1** — Sendo evidente o preenchimento pela LM da primeira e da segunda condições, importa sublinhar, quanto à terceira condição, que os dados recebidos, sendo integrados na base de dados do serviço recetor, não são objeto de partilha. As bases em causa não são partilhadas (artigos 41.º a 43.º da Lei n.º 9/2007, de 19 de fevereiro) com qualquer outro serviço (nem com o serviço congénere nacional) e os dados concretos, sendo objeto de processamento pela análise, integram um produto final cuja partilha, sendo controlada pelas instâncias de fiscalização do SIRP, é por estas filtrada nos termos considerados conformes ao Direito nacional e ao Direito da União, designadamente, quanto a este último, o resultante do *direito do caso*. Todavia, a partilha do produto informacional final não tem o significado de transferência de dados, no sentido considerado no Acórdão *Tele 2*, que nunca se refere a essa incidência.

**3.2.3.2** — Também no plano da sobreposição entre o Direito nacional e o Direito da União, quanto ao designado direito de acesso aos dados próprios, sublinha-se que as instâncias de controlo do SIRP recebem e tramitam queixas relativas às situações objeto de fiscalização, averiguando da respetiva pertinência. É certo que não existe uma notificação aos afetados, que contraditaria (e inviabilizaria) a natureza própria do trabalho de produção de informações. Todavia, para além de estar em causa uma atividade cuja potencialidade interferente é substancialmente reduzida, comparativamente à perseguição criminal (como ponderou o Tribunal Constitucional Alemão nos Acórdãos referidos no item 2.1.2.4. do presente voto), sempre importará considerar, no plano do Direito da União, neste caso com o sentido, pelo menos, de *matéria harmonizada*[44] (ou mesmo, dada a natureza da fonte comunitária — um Regulamento —, de *direito uniforme*[45]), que o Regulamento Geral de Proteção de Dados (RGPD), permite expressamente a limitação do direito de informação dos interessados, no quadro de medidas nacionais de salvaguarda e de prevenção de ameaças à segurança pública (cf., para além do sentido do artigo 2.º, n.º 2, alínea *d*), especificamente o artigo 23.º, n.os 1 e 2, alínea *h*), do RGPD).

Trata-se, enfim, na LO 4/2017, comparando com a "*tentativa de legislar*" de 2015 sobre esta matéria, consubstanciada no Decreto n.º 426/XII, de uma previsão mais precisa da informação a que é possível aceder, com finalidades bem definidas e reconduzíveis a comportamentos identificados por referência a tipos criminais consensualmente correspondentes a criminalidade grave; acesso esse dependente de autorização judicial, protagonizada por uma formação específica de juízes do STJ; mediante critérios de estrita necessidade que ostentam a definição possível em matérias desta natureza; obrigando à formulação de um pedido fundamentado, com base em suspeita concreta e individualizada, sendo a recolha limitada por esse contexto; proibindo-se a interconexão em tempo

real com bases de dados dos operadores de telecomunicações; com validação do tratamento dos dados e possibilidade de cancelamento a todo o tempo; e, enfim, com a sobreposição de diversos controlos *a posteriori*.

Temos, pois, com o regime agora inviabilizado pelo Tribunal Constitucional num seu elemento essencial (os dados de tráfego), um enquadramento legal particularmente densificado, acentuando fortemente a restrição de acesso a qualquer tipo de metadados pelos serviços de informações, num quadro de ponderação que não hesito em qualificar de *exigentíssimo*. Com efeito, porque o acesso previsto em 2015 já correspondia, como referi no voto de vencido então apresentado, a uma *exigente* aplicação prática do princípio da proporcionalidade, observo que com a LO 4/2017 foi essa incidência aprofundada, projetada ao extremo da utilidade destes meios de aquisição de informação de base, justificando-se a qualificação do regime agora pretendido introduzir com o uso de um superlativo — *exigentíssimo* — referido ao quadro limitador desta ingerência das autoridades públicas no direito ao desenvolvimento da personalidade e à reserva da intimidade da vida privada (artigo 26.º, n.º 1, da CRP) e na redução do âmbito de incidência da proibição de acesso a dados pessoais (artigo 35.º, n.os 1 e 4, da CRP).

**4** — Considerei em 2015, avaliando o regime então pretendido introduzir, existir uma relação suficientemente equilibrada entre um objetivo constitucionalmente legítimo — a prestação de segurança pelo Estado (artigo 27.º, n.º 1, da CRP; cf. item 6. do meu voto de vencido) —, a ser alcançado por uma atuação do poder público interferente com o âmbito de proteção de direitos fundamentais, e os meios empregues para atingir esse objetivo. Está implícita nessa avaliação a asserção básica — que um texto posterior de Vitalino Canas resumiu de forma particularmente feliz — de incumbir "[...] *ao legislador* [a definição do] *nível de eficácia pretendido, não se excluindo que seja a mais elevada* [, *não estando*] *comandada a adoção do meio disponível menos interferente* [...]. *Prescreve-se apenas que seja* [o] *menos interferente entre as alternativas capazes de atingir o fim que o legislador elegeu, com a intensidade por ele pretendida* [...]", solução esta que decorre "[...] *do imperativo de preservar a liberdade de conformação do legislador*"[46].

Vale isto por dizer que, então (em 2015), como *agora* (com o diploma de 2017), o legislador escolheu, num espaço de legitimidade de atuação e de eleição entre alternativas diversas passíveis de ser configuradas, o quadro geral de intensidade e de adjetivação do tipo e forma de acesso dos serviços de informações a metadados. Ora, não cumpre ao juiz constitucional, em qualquer dos casos, em substituição do legislador democraticamente legitimado, impor alternativas de intensidade (ou supostas alternativas de perfeição), quando a escolha deste se refere a um quadro substantivo e adjetivo cujo potencial restritivo já expressa uma relação equilibrada de opções valorativas referidas a uma realidade contingente sobre a qual se pretende legitimamente atuar[47].

Sucede, todavia, que nem o esforço ora empreendido pelo legislador, no sentido da adaptação do fim visado até ao limite da utilidade prática, logrou a aceitação do Tribunal Constitucional. Antes referi as particularidades que a construção argumental da questão colocada apresenta, quanto ao parâmetro de aferição constitucional convocável: o artigo 34.º, n.º 4, ou os testes de proporcionalidade referidos à interferência do acesso a metadados, aqui propiciado aos serviços de informações, com o âmbito protetivo decorrente dos artigos 26.º, n.º 1 e 35.º, n.os 1 e 4 da CRP. Não obstante, admitindo, por hipótese, que a Assembleia da República decida no futuro eliminar a primeira variável do problema, assumindo, num processo formal de revisão constitucional, a ultrapassagem do argumento que a maioria de rejeição do artigo 4.º da LO 4/2017 encontra no inciso final — "[...] *em matéria de processo criminal*" — do n.º 4 do artigo 34.º da CRP, nem assim é certo que essa maioria considere possível, por referência aos fundamentos que agora esgrime, a concessão aos serviços de informações portugueses — em aberto contraste com todos os serviços europeus congéneres — de acesso a dados de tráfego.

Constitui esta eventualidade, induzida pelo presente julgamento, motivo sério de apreensão, revelando, como entendo que revela, certo descaso — porventura até alguma displicência — quanto à capacidade de reação do Estado português face aos evidentes fatores de perigo, persistentemente atuantes no dia a dia das nossas sociedades, induzidos pela ameaça global do terrorismo internacional e pela interferência exterior ilegítima dirigida ao normal funcionamento das instituições democráticas e contra os interesses estratégicos do país. Tudo isto justificaria um módico de abertura do Tribunal a considerar positivamente o esforço particularmente responsável que o

legislador parlamentar vem realizando numa matéria com os contornos de grande delicadeza que esta evidencia, cujas incidências o Tribunal Constitucional não está, porque não é essa a sua função, em condições de avaliar devidamente. Como *um de nós* já escreveu, e tem inteiro cabimento no presente contexto, considerações de *competência funcional*, ancoradas na ideia de legitimidade decisória do judiciário, apontam no sentido "[...] *de os tribunais* [comparativamente a outros órgãos de soberania] *estarem mal apetrechados para a realização de certo tipo de julgamentos, nomeadamente envolvendo avaliações empíricas ou prognoses muito complexas* [...] *ou referidos a opções sobre políticas que envolvem* [a ponderação de elementos contingentes respeitantes ao] *interesse público* [...]"[48]. Tudo seria diferente, obviamente, se as opções que ora nos confrontam, no quadro da intencionalidade que preside à regulamentação do acesso dos serviços de informações a metadados, expressassem escolhas que, num domínio de evidência, pudéssemos qualificar como fortemente intrusivas ou como totalmente desfasadas dos princípios constitucionais que nos regem. Estamos, porém, bem longe desse cenário — estamos, ostensivamente, perante opções legislativas que assumidamente procuraram (e logram alcançar) um muito reduzido impacto nos valores constitucionais potencialmente conflituantes. É neste contexto que divirjo profundamente da rejeição do artigo 4.º da LO 4/2017 ora afirmada pelo Tribunal. — *José António Teles Pereira*

**Declaração de voto**

**1** — Vencida.

Apesar de acompanhar a alínea *b*) da decisão, apenas com reservas acompanho a respetiva alínea *a*). Não acompanho a alínea *c*) da decisão.

As normas em apreciação inserem-se no regime de acesso a dados de tráfego consagrado na Lei Orgânica n.º 4/2017 — decorrendo dos artigos 3.º e 4.º da mesma Lei Orgânica. Esta lei surge na sequência do Acórdão n.º 403/2015, do Tribunal Constitucional, que se pronunciou pela inconstitucionalidade do regime que se encontrava previsto para o mesmo efeito no Decreto n.º 426/XII da Assembleia da República, por violação do n.º 4 do artigo 34.º da Constituição.

Gostaria de começar por fazer um ponto introdutório, relativo à relação entre esta matéria e o Direito da UE (UE), de seguida explicarei os motivos que me levaram a não acompanhar a maioria. Finalmente, exporei porque é que, face a uma declaração de inconstitucionalidade com força obrigatória geral, teria recorrido aos poderes atribuídos ao Tribunal Constitucional pelo artigo 282.º, n.º 4, da Constituição, restringindo os seus efeitos.

**2** — Como ponto introdutório, antes do mais, gostava de referir que creio que a questão central colocada no presente pedido de fiscalização se prende com a apreciação da constitucionalidade das referidas normas, em especial, face ao artigo 34.º, n.º 4, da Constituição. Nesse contexto, as considerações de Direito da UE não ocupam um lugar central, por diversos motivos.

Desde logo, cumpre notar que esta é uma matéria que, em princípio, se encontra reservada aos Estados-Membros e fora do âmbito do Direito da UE. Efetivamente, o artigo 4.º, n.º 2, do Tratado da União Europeia estabelece de forma clara que a segurança nacional — âmbito onde nos encontramos — «continua a ser da exclusiva responsabilidade de cada Estado-Membro».

Esta orientação é confirmada pelo direito derivado da UE (como não podia deixar de ser), nomeadamente pelo artigo 1.º, n.º 3, da Diretiva relativa à privacidade e às comunicações eletrónicas (Diretiva n.º 2002/58/CE), que estabelece, sem qualquer ambiguidade, que o seu regime «em caso algum é aplicável às atividades relacionadas com a segurança pública, a defesa, a segurança do Estado». É nesse sentido que deve ser entendido o artigo 15.º da mesma Diretiva — que estabelece a possibilidade de os Estados Membros adotarem medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.os 1 a 4 do artigo 8.º e no artigo 9.º da Diretiva, quando esta seja aplicável, sob várias condições. Uma exceção semelhante decorre do artigo 23.º, n.º 1, alíneas *a*) a *c*), do Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679, RGPD).

Na parte em que é atingido o âmbito do Direito da UE — de acordo com a tese sufragada no Acórdão — é de entender que a compatibilidade do regime objeto de fiscalização com este ordenamento decorre claramente da jurisprudência do Tribunal de Justiça da UE (TJUE), nomeadamente do Acórdão *Tele2* (ECLI:EU:C:2016:970). Conforme se decide nesse Acórdão, no que diz respeito

ao tratamento de dados: «O artigo 15.º, n.º 1, da Diretiva 2002/58, [...], lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União». Analisando estes pontos, é de referir, desde logo, *i*) que as atividades focadas pelas informações em causa se enquadram no domínio da prevenção da criminalidade grave e organizada. Por outro lado, *ii*) existe um controlo prévio, nos termos aqui previstos. Relativamente à *iii*) permanência dos dados no território da UE, esta decorre implicitamente do regime previsto na Lei Orgânica e na Portaria que a regulamenta, nomeadamente porque o Sistema de Acesso ou Pedido de Dados aos Prestadores de Serviços de Comunicações Eletrónicas, (SAPDOC) é desenvolvido e gerido pelo Instituto de Gestão Financeira e Equipamentos da Justiça, I. P. (IGFEJ, I. P.), a quem caberá também a função de gestão do sistema e da respetiva credenciação de acesso.

**3** — Quanto ao pedido de fiscalização propriamente dito, entendeu a maioria que a norma do artigo 4.º da Lei Orgânica n.º 4/2017 viola o artigo 34.º, n.º 4, da Constituição no que diz respeito ao acesso aos dados de tráfego que envolvem comunicação intersubjetiva. Não acompanho esta decisão.

Tal como referido no Acórdão n.º 403/2015, a parte final do n.º 4 do artigo 34.º consiste numa autorização constitucional expressa para a restrição do direito fundamental à inviolabilidade das comunicações, nos «*casos previstos na lei em matéria de processo criminal*».

Diferentemente da tese sustentada no Acórdão, entendo que o procedimento previsto para o acesso aos dados de tráfego estabelecido na Lei Orgânica n.º 4/2017 se aproxima de tal modo do estabelecido no processo penal (mais precisamente, da prática dos atos do inquérito que são reservados à competência do juiz de instrução) que pode ter-se por materialmente equivalente aos procedimentos que caracterizam uma estrutura processual penal num Estado de Direito democrático nos termos exigidos na Constituição.

A referida autorização constitucional é completada com a discriminação dos *fins e interesses* a prosseguir com a lei restritiva ou com o *critério* que deve balizar a intervenção do legislador ordinário.

Relativamente aos fins e interesses a prosseguir, é de referir que as informações facultadas aos oficiais de informações nos termos da Lei Orgânica n.º 4/2017 se inserem no domínio da prevenção do terrorismo, da espionagem, da sabotagem, proliferação de armas de destruição maciça e da criminalidade altamente organizada. Visam reunir informações destinadas a prevenir a ocorrência de factos previstos e punidos na lei penal, designadamente em matéria de criminalidade grave e organizada, cabendo, por conseguinte, ainda no âmbito da autorização constitucional expressa para a restrição do direito fundamental à inviolabilidade das comunicações prevista no artigo 34.º, n.º 4, da Constituição («*em matéria de processo criminal*»). Uma tal autorização está, aliás, em consonância com outros preceitos constitucionais como o que prevê a possibilidade de realização de buscas noturnas em casos de criminalidade especialmente violenta ou altamente organizada, incluindo o terrorismo e o tráfico de pessoas, de armas e de estupefacientes, nos termos previstos na lei (artigo 34.º, n.º 3, da Constituição).

Compreende-se que assim seja. A par da liberdade, também a segurança constitui um valor protegido pela Constituição (artigo 27.º, n.º 1, da Constituição), tendo o Estado uma obrigação de defesa da ordem constitucional democrática.

**4** — Para além disso, a Lei Orgânica n.º 4/2017 veio corrigir os problemas de constitucionalidade identificados no Acórdão n.º 403/2015, definindo todo um procedimento de acesso aos dados de telecomunicações e de Internet sujeito a controlo judicial e autorização prévia, reservada à competência de uma «formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções» (artigo 8.º da Lei Orgânica n.º 4/2017). Esta formação específica do Supremo foi também expressamente consagrada no artigo 47.º, n.º 4, da Lei da Organização do

Sistema Judiciário (Lei n.º 62/2013, de 26 de agosto), na redação que lhe foi dada pelo artigo 17.º da Lei Orgânica n.º 4/2017 — sendo, assim, expressamente considerada pelo legislador democraticamente legitimado como integrando o sistema judiciário português.

Cabe a esta formação do Supremo Tribunal de Justiça garantir «a ponderação da relevância dos fundamentos do pedido e a salvaguarda dos direitos, liberdades e garantias constitucionalmente previstos» (n.º 1 do artigo 5.º da Lei Orgânica), competindo-lhe apreciar a necessidade, adequação e proporcionalidade do pedido apresentado pelos Serviços de Informações. Cabe-lhe ainda a definição «das categorias de dados de telecomunicações e Internet a fornecer pelos operadores segundo um juízo restritivo de proibição do excesso que interdite o acesso indiscriminado a todos os dados de telecomunicações e Internet», bem como a definição «das condições de proteção do segredo profissional» (n.º 1 do artigo 10.º).

Além da sujeição a autorização judicial prévia, que deve ser fundamentada, o procedimento fica sujeito ao acompanhamento permanente dos juízes no que respeita à transmissão dos dados em obediência a exigentes condições técnicas e de segurança (n.º 1 do artigo 11.º), controlo da validade do tratamento dos dados feito pelos Serviços de Informações (n.os 1 e 2 do artigo 12.º) e contempla a possibilidade do cancelamento a todo o momento bem como a destruição de todos os dados obtidos de forma ilegal ou abusiva, ou que violem o âmbito da autorização judicial concedida ou que sejam manifestamente estranhos ao processo (n.º 3 do artigo 12.º).

O presente Acórdão classifica o processo de autorização do acesso aos dados como «uma atuação de natureza administrativa e não judicial» (ponto 11.1.2, (ii)), daqui retirando que, apesar de representar uma evolução positiva «a transferência da discricionariedade decisória em matéria de acesso aos dados, de órgãos do SIRP para magistrados» permanece «coartada a possibilidade de defesa dos cidadãos contra a ingerência do Estado na sua esfera privada». Uma tal afirmação ignora, porém, que a razão de ser da atribuição da competência aos juízes reside precisamente na tutela preventiva dos direitos dos visados pelas medidas de ingerência em direitos fundamentais, na impossibilidade de estabelecer o contraditório, tal como acontece no inquérito criminal, em obediência à garantia constitucional prevista no artigo 32.º, n.º 4, da Constituição. Trata-se de permitir a realização de diligências de ingerência em direitos fundamentais que, de outro modo, seriam consideradas intoleráveis num Estado de Direito. Mesmo quando estejam em causa atos que não revistam natureza estritamente jurisdicional, a razão de ser da atribuição das decisões que afetam direitos fundamentais à competência do juiz reside nas garantias de independência pessoal e objetiva que o seu estatuto lhe confere e que asseguram um modo de pensar específico do juiz («*spezifisch richterlicher Denkweise*», na designação do Tribunal Constitucional alemão) que nunca deverá perder de vista o princípio da adequação entre meios e fins bem como a proibição do excesso.

**5** — Todavia, a dimensão orgânico-funcional de jurisdição não dispensa um procedimento específico regulado e dirigido à prolação de uma decisão vinculativa e independente. Por conseguinte, verdadeiramente decisivo será — isso sim — averiguar se o regime jurídico previsto concretiza as exigências constitucionais que importa assegurar em ordem a garantir a proteção adequada dos direitos dos visados. Ora, na Lei Orgânica em análise, o legislador definiu todo um procedimento para a concessão do acesso aos dados pelo Sistema de Informações da República Portuguesa, onde estabelece os critérios de decisão que o decisor tem de respeitar.

O acesso aos dados encontra-se definido de forma detalhada no artigo 11.º, com as garantias decorrentes da sujeição a controlo judicial (artigo 12.º) e regulando o artigo 14.º a forma como o tratamento dos dados comunicados deve ocorrer. O pedido destinado a obter autorização judicial deve precisar a «identificação da pessoa ou pessoas, caso sejam conhecidas, envolvidas nos factos referidos [...] e afetadas pelas medidas pontuais de acesso requeridas» (alínea *c*) do n.º 2) do artigo 9.º). As providências de recolha de dados só podem ser feitas «com base numa suspeita concreta e individualizada» (n.º 3 do artigo 9.º).

Os fins da concessão do acesso aos dados de tráfego encontram-se expressamente delimitados, destinando-se exclusivamente a prevenir categorias específicas de crimes — a espionagem e o terrorismo (artigo 4.º e n.º 2 do artigo 10.º) no que respeita aos dados e tráfego, e, no que respeita aos dados de base e de localização, à salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de

destruição maciça e criminalidade altamente organizada, no âmbito das atribuições do SIS e do SIED (artigo 3.º).

As condições de acesso estão legalmente determinadas através de critérios específicos para aferir a necessidade, em cada caso concreto, do acesso aos dados (o n.º 1 do artigo 6.º dispõe que o pedido de acesso só pode ser autorizado quando houver razões para crer que a diligência é necessária, adequada e proporcional «para a obtenção de informação sobre um alvo ou um intermediário determinado», na sua alínea *a*), ou «para a obtenção de informação que seria muito difícil ou impossível de obter de outra forma ou em tempo útil para responder a situação de urgência», na sua alínea *b*)).

A duração do acesso é determinável e limitada, pois a possibilidade de prorrogação do prazo máximo inicial de 3 meses apenas pode ocorrer uma única vez e encontra-se sujeita ao mesmo limite temporal do prazo inicial (alínea *d*) do n.º 2 do artigo 9.º). A Lei contempla ainda a existência de um prazo para a manutenção ou eliminação obrigatória dos dados recolhidos, embora remeta a determinação desse prazo para regulamento administrativo (n.º 4 do artigo 14.º).

**6** — É de assinalar que o recurso a conceitos indeterminados na previsão das normas que estabelecem o procedimento de autorização do acesso aos dados visados pelo Sistema de Informações da República Portuguesa replica a técnica usada nas normas que habilitam a realização no inquérito criminal de medidas de obtenção de prova que configuram ingerência em direitos fundamentais, o que corrobora as semelhanças entre os dois procedimentos (cf., por exemplo, o regime em análise com o artigo 187.º, n.º 1, do CPP: «A interceção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter»). Pode concluir-se que os parâmetros legais estabelecidos para a autorização judicial de uma medida restritiva de direitos fundamentais no âmbito de um inquérito no contexto do processo penal se caracterizam por alguma indeterminação. O que não pode é afirmar-se — sem incorrer em flagrante incoerência — que essa indeterminação é aceitável aos olhos da Constituição para o controlo judicial que é confiado ao juiz de instrução no inquérito criminal, mas já não é no procedimento equivalente estabelecido nas normas da Lei Orgânica em apreciação. Afasto-me, por isso, da posição do Acórdão.

A verdade é que também na base da autorização ou validação judicial de qualquer medida de investigação restritiva de direitos realizada no inquérito criminal encontramos apenas uma informação unilateral fornecida pelo próprio requerente da medida — o Ministério Público — que, nesse caso, acumula a condição de direta ou indiretamente ser o responsável pela investigação.

**7** — A Lei Orgânica assegura a *intervenção do Ministério Público* durante o processo (n.º 1 do artigo 1.º) — não como seu responsável, mas sim como terceiro imparcial, fiscal da legalidade e detentor da ação penal, numa lógica de equilíbrio de *checks and balances*. É neste contexto que a autorização de acesso aos dados, a transmissão dos dados, o cancelamento de acesso aos dados, a sua destruição e a recolha de indícios da prática dos crimes de terrorismo e espionagem, devem ser obrigatoriamente comunicados ao Procurador-Geral da República «para os devidos efeitos» (n.º 2 do artigo 5.º, o n.º 1 do artigo 11.º, o n.º 4 do artigo 12.º e o artigo 13.º).

Não se compreende, por conseguinte, a crítica apontada no Acórdão à escassez de definição dos poderes do MP.

**8** — O Acórdão espraia-se numa argumentação circular que não consegue ultrapassar a mera petição de princípio quando afirma que o presente procedimento não pode ter-se por materialmente equivalente ao processo penal porque «não se destina a investigação ou produção de prova no âmbito de um processo penal em curso» (ponto 11.1.2.) ou porque tem lugar «fora de um processo criminal devidamente formalizado» (ponto 11.2.3.). Na verdade, os únicos elementos caracterizadores do regime do processo penal que o Acórdão identifica para justificar aquilo que considera constituir uma distância irredutível para o procedimento de acesso aos dados pelos Serviços de Informações da República Portuguesa previsto no regime em análise saldam-se, afinal, na regra da publicidade do processo penal e nas garantias constitucionais do arguido.

Todavia, como o próprio Acórdão admite, na fase inicial do inquérito criminal inexiste arguido, sendo que é precisamente nesta fase que decorre à revelia do arguido — e, por conseguinte, sem o seu conhecimento — que têm lugar a os métodos de ocultos de obtenção de prova onde se insere

a possibilidade de acesso a dados de telecomunicações e Internet. Ou seja, em ambos os casos o acesso aos dados ocorre sem a constituição como arguido da pessoa em causa. Assim, longe de evidenciarem qualquer diferença inultrapassável, aqueles elementos caracterizadores demonstram a semelhança substancial que aproxima os dois procedimentos.

Não se ignora que a subsequente constituição de arguido no inquérito criminal é obrigatória diante da recolha de fundadas suspeitas, de crime, proporcionando — em regra — a partir desse momento o acesso aos autos bem como um leque de direitos e deveres processuais, designadamente, o direito de intervenção no inquérito e na instrução e o direito a recorrer de decisões desfavoráveis. Porém, e diferentemente do que vem sustentado no Acórdão, a constituição do arguido no processo penal não assegura a tutela jurídica efetiva e integral de todos os afetados pela restrição de direitos fundamentais que o acesso aos dados de comunicações necessariamente comporta. Desde logo, porque o lesado pela medida pode nunca vir a ser constituído arguido no processo. Seja como for, certo é que não está ao alcance dos visados pelas medidas ocultas de obtenção de prova que implicam ingerências em direitos fundamentais realizadas no inquérito criminal qualquer meio de tutela especificada que vise a sua revogação, cancelamento ou que garanta sequer o seu conhecimento. A proibição de prova tem uma incidência marcadamente processual; não constitui meio de tutela direta ou imediata dos direitos sacrificados por medidas de investigação.

De todo o modo, cumpre ainda assinalar que mesmo o já referido RGPD, diretamente aplicável na nossa ordem jurídica, quando prevê os requisitos das medidas legislativas que limitem o alcance das obrigações e dos direitos nele previstos, designadamente para fins de segurança do Estado, defesa, segurança pública ou prevenção, investigação, deteção ou repressão de infrações penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública (artigo 23.º, n.º 1, alíneas. *a*), b*, c*) e *d*), do RGPD), prevê como exceção ao direito dos titulares dos dados serem informados do acesso as situações em que tal possa prejudicar o objetivo da limitação (artigo 23.º, n.º 2, alínea *h*), do RGPD). Claramente que esta exceção seria aplicável no âmbito do regime em análise, tendo em conta os fins prosseguidos. Assim, neste caso, existe a possibilidade de afastamento do direito de ser informado.

**9** — Diferentemente do Acórdão, concluí, pois, que em todos os domínios relevantes se verifica uma equivalência clara entre o regime objeto de fiscalização (do procedimento de acesso aos dados de tráfego pelos oficiais do SIS e do SIED) e o regime de recolha de prova através dos métodos ocultos de obtenção de prova que têm lugar na fase de investigação prévia à constituição de arguido em inquérito criminal. Ora, cabe dentro do âmbito da autorização constitucional de restrição do direito fundamental à inviolabilidade das comunicações, prevista no artigo 34.º, n.º 4, da Constituição, um regime preventivo paralelo ao processo penal, o qual, inserindo-se no âmbito da prevenção de crimes graves, assegura garantias que oferecem o mesmo nível de exigência e eficácia das que existem naquele processo. Consequentemente, votei a não inconstitucionalidade da norma.

A discordância relativamente a esta conclusão do Acórdão reflete-se inevitavelmente nos demais pontos da fundamentação e da decisão.

Com efeito, considerando assente que nos encontramos dentro do âmbito da autorização constitucional para restringir o sigilo das telecomunicações, para efeitos de prevenção de criminalidade grave e organizada, ponderando os direitos e valores constitucionais em confronto, entendo não merecer a menor dúvida que a medida prevista no artigo 4.º da Lei Orgânica respeita os testes do princípio da proporcionalidade impostos pelo artigo 18.º da Constituição (adequação, necessidade e proibição do excesso). Nesta ponderação releva a circunstância de as informações visadas não poderem abranger dados de conteúdo e restringirem-se a dados pretéritos.

**10** — O juízo de respeito pelo princípio da proporcionalidade referente aos dados gerados no âmbito de comunicações intersubjetivas não pode deixar de estender-se aos dados de tráfego de Internet gerados fora do âmbito daquelas comunicações, bem como — por maioria de razão — aos dados de base e localização. É, portanto, de concluir também pelo respeito do princípio da proporcionalidade da restrição que o acesso a estes dados gera do direito à autodeterminação informativa. Efetivamente, como se salientou no Acórdão n.º 43/2015 (ponto 16) «o tipo de restrições ao direito à inviolabilidade das comunicações que é admitido pelo n.º 4 do artigo 34.º da CRP é muito

mais exigente do que as restrições toleradas por outros direitos fundamentais em que se protegem os mesmos bens jurídicos (dignidade da pessoa, desenvolvimento da personalidade, garantia da privacidade, autodeterminação comunicativa)».

No entanto, surpreendentemente, o presente Acórdão veio, porém, considerar que «a intensidade de escrutínio exigida, apesar da diferença dos parâmetros constitucionais em causa, não pode deixar de ser similar ou equivalente» (ponto 11.2.1.). Não consigo compreender como se pode considerar a intensidade de escrutínio equivalente, face ao afirmado carácter «muito mais exigente» do n.º 4 do artigo 34.º da CRP. Esta nova tese, além de incompreensível, revela-se ainda dificilmente conciliável com a ideia anteriormente expressa de que apenas no que respeita à inviolabilidade das comunicações garantida no artigo 34.º, n.º 4, o legislador constitucional resolveu explicitamente o sentido no qual devem ser resolvidas as eventuais colisões entre os valores constitucionalmente protegidos por reconhecer que só em matéria de processo penal vale uma *preferência abstrata* pelo valor da segurança em prejuízo da privacidade das comunicações (ponto 9.2.). Se — como pretende o Acórdão — as dimensões da privacidade e da proteção de dados pessoais dos utilizadores eventualmente em causa não têm menor merecimento constitucional do que aquelas que também podem ser lesadas no âmbito das comunicações, por que razão a Constituição as distinguiria?

**11** — Resta referir que, numa interpretação sistemática e integrada da Lei Orgânica, as referências à "defesa nacional" e à "segurança interna" constantes do seu artigo 3.º não têm de ser consideradas como fins inscritos na norma, a par da prevenção de atos que de seguida o preceito identifica por referência a tipos de ilícito penal, mas antes como a limitação do acesso aos dados para a prevenção daqueles crimes ao âmbito das atribuições dos Serviços de Informações definidas por lei. De acordo com esta interpretação, nenhum problema de constitucionalidade colocaria também esta norma. Os problemas de inconstitucionalidade identificados no Acórdão no que respeita ao artigo 3.º pressupõem a recondução das atribuições dos Serviços a fins autónomos que podem justificar o acesso a dados de base e localização o que, todavia, não me parece constituir a única — ou sequer uma rigorosa — interpretação do aludido preceito, que não deve prescindir de uma compreensão integrada e sistematizada de todo o diploma. Foi, portanto, com esta reserva que acompanhei a decisão da alínea *a*) da decisão.

**12** — Finalmente, tendo o Tribunal Constitucional decidido declarar a inconstitucionalidade, com força obrigatória geral da referida norma, penso que se impunha limitar os efeitos desta declaração.

Nos termos do artigo 282.º, n.º 4, da Constituição, o Tribunal Constitucional tem o poder-dever de, após deliberar uma declaração de inconstitucionalidade com força obrigatória geral, ponderar os efeitos da sua decisão face à possibilidade da sua restrição. Esta competência permite-lhe manipular os efeitos da declaração de inconstitucionalidade, de forma a alcançar um efeito mais restrito ou menos oneroso do que a eficácia normal desta declaração, prevista no artigo 282.º, n.os 1 e 2, da Constituição. Trata-se, pois, de um juízo que incide já não sobre a inconstitucionalidade da norma em causa, mas sobre os efeitos da declaração de inconstitucionalidade que devem ser ponderados face a exigências de segurança jurídica, equidade ou interesse público de especial relevo. A Constituição admite, pois, expressamente, que pode existir a necessidade de restringir os efeitos da declaração — e que o Tribunal Constitucional deve, por isso, ponderar essa possibilidade e sobre ela decidir.

No presente caso, creio que duas causas surgem que justificam a manipulação de efeitos da presente declaração de inconstitucionalidade — que deveria apenas produzir efeitos a partir da publicação do presente acórdão no *Diário da República.* Por um lado, existe um interesse público de especial relevo — a segurança interna nacional — que está em causa e que justifica esta restrição. Por outro lado, e relacionado com este interesse, também manifestas exigências de segurança jurídica justificam esta manipulação. Tendo em conta o tempo decorrido desde a entrada em vigor do regime, é preferível consolidar os atos e atividades entretanto produzidos, de forma a salvaguardar este interesse. A possível repercussão face às obrigações da República Portuguesa no quadro da cooperação internacional contra o terrorismo e criminalidade internacional também impõe esta limitação. Estas razões são substancialmente agravadas, neste caso, pela refutação — expressa no Acórdão — da natureza jurisdicional das decisões eventualmente já proferidas pela formação de juízes do Supremo Tribunal de Justiça, o que afasta necessariamente qualquer dúvida que pudesse

subsistir sobre a possibilidade de acautelamento da segurança jurídica através da ressalva dos casos julgados face aos efeitos da declaração de inconstitucionalidade, nos termos do artigo 282.º, n.º 3, da Constituição.

A fixação da produção de efeitos da declaração de inconstitucionalidade apenas para o futuro é um claro imperativo de segurança jurídica e de segurança nacional, a que o Tribunal Constitucional não se deveria eximir. — *Maria de Fátima Mata-Mouros*

**Declaração de voto**

**1 —** Vencida parcialmente quanto à decisão constante da alínea *a*) da fórmula decisória do Acórdão — na qual se declara a *inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 3.º da Lei Orgânica n.º 4/2017, de 25 de agosto, na parte em que admite o acesso dos oficiais de informações do Serviço de Informações de Segurança (SIS), e do Serviço de Informações Estratégicas e de Defesa (SIED), relativamente a dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação, para efeitos de produção de informações necessárias à salvaguarda da defesa nacional e da segurança interna, por violação dos artigos 26.º, n.º 1, e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2.º da Constituição da República Portuguesa* (cf. III — Decisão, alínea *a*)) — e vencida quanto à decisão constante da alínea *c*) da fórmula decisória — na qual se declara a *inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4.º da Lei Orgânica n.º 4/2017, de 25 de agosto, por violação do disposto no artigo 34.º, n.º 4, da Constituição, no que diz respeito ao acesso aos dados de tráfego que envolvem comunicação intersubjetiva, e por violação do disposto nos artigos 26.º, n.º 1 e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2, todos da Constituição, no que se refere ao acesso a dados de tráfego que não envolvem comunicação intersubjetiva* (cf. III — Decisão, alínea *c*)) — e respetiva fundamentação.

Isto, pelas razões que, de modo sucinto, de seguida se explicitam, não sem previamente se fazer referência ao enquadramento das normas sindicadas, quer no regime jurídico de direito nacional em que se inserem, quer na ótica do Direito da União Europeia, na medida em que se afigura relevante para alcançar o juízo de não inconstitucionalidade que subscrevemos.

**A**) **O enquadramento das normas sindicadas**

**A1. O enquadramento das normas sindicadas no regime aprovado pela Lei Orgânica n.º 4/2017, de 25 de agosto**

**2 —** As normas sindicadas nos autos — artigo 3.º («Acesso a dados de base e de localização de equipamento») e artigo 4.º («Acesso a dados de tráfego») da Lei Orgânica n.º 4/2017, de 25 de agosto (doravante LO n.º 4/2017) — inserem-se em diploma que «Aprova e regula o procedimento especial de acesso a dados de telecomunicações e *Internet* pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa e procede à segunda alteração à Lei n.º 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário)».

A LO n.º 4/2017 regula assim «o procedimento especial de acesso a dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas que se mostrem estritamente necessários para a prossecução da atividade de produção de informações pelo Sistema de Informações da República Portuguesa (SIRP) relacionadas com a segurança interna, a defesa, a segurança do Estado e a prevenção da espionagem e do terrorismo (...)» (art. 1.º, n.º 1). E, da compaginação do n.º 1 do artigo 1.º («Objeto») com os subsequentes artigos 2.º a 4.º («Definições», «Acesso a dados de base e de localização de equipamento» e «Acesso a dados de tráfego»), resulta que o regime instituído visa: *i*) o acesso a *certas categorias* de dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas — *dados de telecomunicações* e *dados de Internet* (tal como definidos nas alíneas *a*) e *b*) do n.º 1 do artigo 2.º), abrangendo os mesmos *dados de base*, *dados de localização de equipamento* e *dados de tráfego* (tal como definidos nas alíneas *a*) a *c*) do n.º 2 do artigo 2.º, os últimos «quando não deem suporte a uma concreta comunicação»); *ii*) apenas para *certos fins* — dados de base e de localização de equipamento

previamente armazenados «para efeitos de produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, de espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada e *no seu exclusivo âmbito*» (art. 3.º, itálicos acrescentados) e *dados de tráfego* previamente armazenados «*apenas* (...) para efeitos de produção de informações necessárias à prevenção de atos de espionagem e do terrorismo» (art. 4.º, itálico acrescentado); e *iii*) apenas quando tal acesso se mostre «estritamente necessário» para a prossecução de tais fins (art. 1.º, n.º 1), reiterando-se a ideia de (estrita) n*ecessidade* de acesso quer no artigo 3.º («Acesso a dados de base e de localização de equipamento»), quer nos artigos 6.º, n.º 1 e 10.º, n.º 1 («Admissibilidade do pedido» e «Apreciação judicial») e, ainda, no artigo 11.º, n.º 2 («Acesso aos dados autorizados» por parte do pessoal do SIRP, o qual é determinado pelo «princípio da necessidade de conhecer» e tendo em vista o bom exercício das funções que lhe forem cometidas). Deste modo, tais específicas temáticas ou específicos domínios, no âmbito da específica finalidade de «produção de informações» pelo SIRP que justifica o acesso dos oficiais de informações do Serviço de Informações de Segurança (SIS) e do Serviço de Informações Estratégicas de Defesa (SIED) às categorias de dados de telecomunicações e de *Internet* em causa elencados nos artigos 3.º e 4.º da LO n.º 4/2017, acompanham no essencial o enunciado genérico das temáticas ou domínios elencados no n.º 1 do artigo 1.º: «acesso a dados (...) que se mostrem estritamente necessários para a prossecução da atividade de produção de informações pelo (...) SIRP e relacionadas com a *segurança interna*, a *defesa*, a *segurança do Estado* e a *prevenção da espionagem* e do *terrorismo* (...)» — pese embora a não inteira coincidência de domínios no que respeita à segurança do Estado (apenas mencionada no artigo 1.º, n.º 1) e à prevenção de atos de sabotagem, proliferação de armas de destruição maciça e criminalidade altamente organizada (estes apenas mencionados no artigo 3.º).

Tendo presentes o objeto e as finalidades do acesso a dados previamente armazenados acima enunciados, tal como definidos pela LO n.º 4/2017, há que considerar que a mesma, aprovada após a prolação do Acórdão n.º 403/2015 (Plenário), não deixou de revelar a intenção do legislador de superar os vícios de inconstitucionalidade que aquele aresto, em sede de apreciação preventiva da constitucionalidade, apontou ao artigo 78.º, n.º 2, do Decreto n.º 426/XII da Assembleia da República (doravante Decreto) — como se explica no presente Acórdão a partir da Exposição de motivos da Proposta de Lei n.º 79/XIII e das normas que preveem os pressupostos de admissibilidade de acesso aos dados (cf., respetivamente, II — Fundamentos, 6. Enquadramento, *a*) As normas questionadas no quadro do novo sistema de acesso aos *metadados* e o parâmetro invocado, pp. 11, e 10. A questão de constitucionalidade do artigo 4.º da Lei Orgânica n.º 4/2017, 10.1. O acesso a dados de tráfego que envolvem comunicação intersubjetiva, 10.1.1, p. 47).

Ora, o presente Acórdão faz referência, em várias passagens, a (outras) normas do diploma em que se inserem as normas sindicadas: em relação ao sentido prescritivo dos preceitos normativos acessórios em relação às normas sindicadas (cf. em especial, II, 6, *a*), quanto aos artigos 5.º a 8.º da Lei Orgânica n.º 4/2017 e também ao artigo 1.º da Portaria n.º 237-A/2018, de 28 de agosto); às normas que preveem vários pressupostos de admissibilidade do acesso dos oficiais do SIS e do SIED aos *metadados,* incluindo *dados de tráfego* (cf. II, 11.1.1); às normas que, na perspetiva da maioria que fez vencimento quanto ao artigo 4.º, não permitem aproximar ou equiparar o procedimento de acesso a dados de comunicação e de *Internet* em causa ao processo penal, quer do ponto de vista formal quer material e garantístico, incluindo as normas que denotam segundo a maioria, uma insuficiência de mecanismos de controlo (cf. II, 11.1.2, em especial *i*) a iv); e, finalmente, no quadro dos traços do regime de acesso consagrado na LO n.º 4/2017, às normas que consagram as suas finalidades, os critérios, as formas, os limites e as garantias nela previstas (cf. II, 12. A questão de constitucionalidade do artigo 3.º da Lei Orgânica n.º 4/2017).

Sem prejuízo das várias e significativas diferenças que se podem apontar entre o regime de acesso constante do Decreto n.º 426/XII (cujo artigo 78.º, n.º 2, foi apreciado em sede de fiscalização preventiva da constitucionalidade pelo Acórdão n.º 403/2015, no sentido da inconstitucionalidade) e o regime consagrado pela LO n.º 4/2017, de 25 de agosto (tal como regulamentada pela Portaria n.º 237-A/2018, de 28 de agosto), alguns dos traços do regime instituído por esta Lei que o distanciam do regime constante do referido Decreto, por se afigurarem centrais para a análise das questões de constitucionalidade e, em particular, para o juízo de proporcionalidade das medidas

(restritivas) de acesso aos dados em causa, merecem uma referência adicional e prévia: *i*) os que decorrem do disposto no artigo 9.º (Iniciativa), em especial quanto aos fundamentos do pedido e seu objeto — «medidas pontuais de acesso» (as "exigências de conteúdo" a que o Acórdão se refere em II, 12.); ii) os que decorrem do artigo 8.º («Controlo judicial e autorização prévia»); iii) os que decorrem do artigo 10.º («Apreciação judicial»); iv) os que decorrem do regime de garantias instituído pelos artigos 12.º, 14.º, 15.º e 16.º

*i*) No que respeita à *iniciativa*, na vertente da *fundamentação do pedido e seu objeto*, o regime do artigo 9.º, n.os 2 e 3 da LO n.º 4/2017, apresenta três traços essenciais que o distinguem do constante do referido Decreto (cf. art. 37.º, n.º 2): a exigência de fundamentação do pedido e de modo detalhado e circunstanciado incluindo a indicação dos elementos enunciados na lei — em especial a indicação da ação operacional concreta a realizar e a indicação das medidas de acesso, os factos que suportam o pedido, finalidades que o fundamentam e razões que aconselham adoção de tais medidas e, ainda, a identificação da pessoa ou pessoas, caso sejam conhecidas, envolvidas naqueles factos e afetadas pelas medidas de acesso (art. 9.º, n.º 2, alíneas *a*) a *d*)); a caracterização das medidas requeridas como «medidas *pontuais* de acesso» definidas pelo legislador como «as providências de recolha de dados, por transferência autorizada e controlada caso a caso, com base numa *suspeita concreta e individualizada,* que não se prolongam no tempo, sendo a sua duração circunscrita, e que não se estendem à totalidade dos dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, não admitindo a aquisição de informação em larga escala, por transferência integral dos registos existentes, nem a ligação em tempo real às redes de comunicações eletrónicas» (art. 9.º, n.º 2, alíneas *a*) a *c*) e n.º 3); a limitação da renovação do período máximo de duração das medidas requeridas (3 meses), a um único período sujeito ao mesmo limite (também sujeito a autorização a autorização prévia) e desde que se verifiquem os respetivos requisitos de admissibilidade (art. 9.º, n.º 2, alínea *d*)).

*ii*) No que respeita ao *controlo judicial e autorização prévia*, a LO n.º 4/2017 reserva os mesmos agora a «uma formação das secções criminais do Supremo Tribunal de Justiça (STJ), constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior de Magistratura de entre os mais antigos destas secções» (art. 8.º e, também art. 5.º, n.º 1) — tendo a Lei de Organização do Sistema Judiciário sido alterada para contemplar tal específica formação das secções criminais (arts. 1.º, n.º 2 e 17.º da LO 4/2017). Assim, diversamente da Comissão de Controlo Prévio prevista no Decreto (cf. artigo 35.º), a formação em causa é configurada como uma (específica) formação das secções criminais do Supremo Tribunal de Justiça (e organicamente emanada destas) — constituída apenas por juízes das secções criminais do mesmo Supremo Tribunal (os presidentes das seções criminais e um juiz, de entre os mais antigos destas secções, designado pelo Conselho Superior de Magistratura). Deste modo, no exercício das competências que são lhe cometidas pela LO n.º 4/2017 — autorização prévia e controlo —, não deixa a formação (específica) em causa, e bem assim os magistrados que a integram, de comungar, em especial, da independência que constitui atributo próprio dos tribunais e da magistratura judicial, o que se revela particularmente relevante num domínio em que estão em causa direitos fundamentais e eventuais restrições aos mesmos. No mesmo sentido parece apontar o artigo 5.º, n.º 1, na parte em que se refere à obrigatoriedade de «autorização judicial prévia» por aquela formação específica das secções criminais do STJ — segundo o qual essa mesma formação (e a autorização pela mesma obrigatoriamente concedida) constitui «garante [d]a ponderação da relevância dos fundamentos do pedido e a salvaguarda dos direitos, liberdades e garantias constitucionalmente previstos».

*iii*) No que respeita aos traços de regime respeitantes à *apreciação judicial* (resultantes do art. 10.º), a LO n.º 4/2017 — para além dos traços que reproduzem o teor do artigo 4.º (art. 10.º, n.º 2) e regulam os prazos de decisão (art. 10.º, n.º 3, 1.ª parte, e n.º 4) — relevam em particular os termos dessa apreciação judicial, tendo o legislador cometido à formação judicial *supra* referida a apreciação da necessidade, adequação e proporcionalidade do pedido e estipulando que tal apreciação, designadamente no que se refere à «justa medida da espécie e da escala de informação obtida», «compreende a definição das categorias de dados de telecomunicações e *Internet* a fornecer pelos operadores, segundo um juízo restritivo de proibição do excesso que interdite o acesso indiscriminado a todos os dados de telecomunicações e *Internet* de um determinado cidadão, bem como a definição das condições de proteção do segredo profissional» (art. 10.º,

n.º 1). Estipula ainda o mesmo preceito que a decisão judicial, sob a forma de despacho, deve ser «fundamentado com base em informações claras e completas, nomeadamente quanto aos objetivos do processamento» (art. 10.º, n.º 3, 2.ª parte). Deste modo o legislador, não só reitera — em consonância com o *supra* referido conceito de «medidas pontuais de acesso» — a interdição de acesso indiscriminado a todos os dados em causa do visado (assim circunscrevendo o acesso a tais dados a um acesso efetuado de modo *seletivo*), bem como impõe — em consonância com as exigências da fundamentação do pedido constante do artigo 9.º, n.º 2 — que a fundamentação da decisão judicial leve em conta informações claras e completas, designadamente quanto aos objetivos do processamento (dos dados cujo acesso estiver em causa).

*iv*) Por último, no que respeita aos traços de regime relativos às garantias instituído pelos artigos 12.º, 14.º 15.º e 16.º, resulta destes preceitos — bem como da sua conjugação com o n.º 1, parte final, do artigo 1.º e o artigo 8.º — que, para além do «controlo» exercido pela formação das secções criminais do STJ no momento da apreciação da admissibilidade do pedido e da decisão de autorização (judicial) prévia, são previstas outras formas de controlo — e correspondentes garantias — em fase posterior à autorização, i.e, durante o período em que se processa (e mantém) o acesso aos dados, quer cometidas à referida formação do STJ (art. 1.º, n.º 1, parte final e 12.º), quer cometidas à Comissão de Fiscalização de Dados do SIRP (art. 15.º) e ao Conselho de Fiscalização do SIRP (art. 16.º).

Por um lado, após a comunicação eletrónica através da qual se processa (com especiais cautelas) a transmissão diferida dos dados de telecomunicações e *Internet* — obtidos ao abrigo da LO n.º 4/2017 (cf. art. 11.º, n.º 1) e, assim, cujo acesso foi autorizado, nos termos da mesma — a formação do STJ que decide da concessão (ou não) de autorização de acesso, valida, nos termos do n.º 2 do artigo 12.º, o tratamento dos mesmos pelo SIS ou pelo SIED em conformidade com o disposto no n.º 1 do mesmo artigo — i.e., com vista a garantir o respeito pelos direitos, liberdades e garantias e pelo princípio da legalidade, assegurando, nomeadamente, que tais dados são recolhidos para finalidades determinadas, explícitas e legítimas e são adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos (art. 12.º, n.º 1, alíneas *a*) e *b*)); e, em razão de tal controlo, pode determinar a todo o momento o cancelamento de procedimentos em curso de acesso aos dados em causa, bem como ordenar a destruição imediata de todos os dados obtidos de forma ilegal ou abusiva, ou que violem o âmbito da autorização judicial prévia, bem como os dados que sejam manifestamente estranhos ao processo, nomeadamente quando não tenham relação com o objeto ou finalidades do pedido ou cujo tratamento possa afetar gravemente direitos, liberdades e garantias (art. 12.º, n.º 3).

Por outro lado, à Comissão de Fiscalização de Dados do SIRP (art. 15.º) e ao Conselho de Fiscalização do SIRP (art. 16.º) são cometidas também competências de controlo.

A Comissão de Fiscalização de Dados do SIRP — à qual compete a fiscalização do respeito pelos princípios e cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados obtidos nos termos da LO n.º 4/2017 — detém (para além dos poderes de fiscalização previstos no regime geral aplicável aos centros de dados do SIS e do SIED — cf. arts. 7.º, alínea *c*), 26.º e 27.º da Lei n.º 34/84, de 5 de setembro, que estabelece as bases gerais do SIRP), em especial, poderes de fiscalização oficiosa, por referência nominativa, dos dados de telecomunicações e *Internet* obtidos nos termos da mesma Lei, dando conhecimento ao Conselho de Fiscalização do SIRP das irregularidades ou violações verificadas, detendo igualmente poderes para ordenar o cancelamento ou retificação dos dados recolhidos que envolvam violação dos direitos, liberdades e garantias consignados na Constituição e na lei e, se for caso disso, exercer a correspondente ação penal (cf. art. 15.º, n.º 7, da LO n.º 4/2017 — à semelhança do disposto, respetivamente, no n.º 3 do art. 27.º e do n.º 6 do art. 26.º, ambos da referida Lei n.º 30/84). Ademais, é através da mesma Comissão que se exerce o «direito de acesso dos cidadãos aos dados processados ou conservados nos centros de dados do SIS e do SIED», segundo o procedimento previsto no regime geral aplicável aos centros de dados do SIS e do SIED quanto à fiscalização mediante participação (este regulado no artigo 26.º, n.º 5, da mencionada Lei n.º 30/84, de 5 de setembro, segundo o qual a fiscalização pela Comissão de Fiscalização de Dados do SIRP, com a composição prevista no n.º 2 do mesmo artigo, se exerce, além de verificações periódicas dos programas, dados e informações por amostragem, fornecidos sem referência nominativa, igualmente

pelo acesso a dados e informações com referência nominativa, particularmente quando a mesma Comissão «entenda estar perante denúncia ou suspeita fundamentada da sua recolha ilegítima ou infundada»).

O Conselho de Fiscalização do SIRP detém também poderes de fiscalização relativamente ao procedimento de acesso e aos dados de telecomunicações e *Internet* obtidos nos termos da LO n.º 4/2017, podendo solicitar e obter esclarecimentos e informações complementares que considere necessários e adequados ao exercício das suas funções de fiscalização (cf. art. 16.º, n.º 2, parte final, da LO n.º 4/2017- à semelhança do disposto no art. 9.º, n.º 1, e n.º 2, alínea *e*), da Lei n.º 30/84, de 5 de setembro).

Para além das garantias que decorram do regime de proteção de dados consagrado nos artigos 12.º, 15.º e 16.º da LO n.º 4/2017, o artigo 14.º consagra igualmente garantias inerentes ao regime de proteção de dados (cf. em especial n.º 1 e n.º 2, alíneas *a*) a *d*)), sendo aplicável ao tratamento dos dados de telecomunicações e de *Internet* obtidos ao abrigo da LO n.º 4/2017 o regime especial de proteção de dados pessoais do SIRP (assim, n.º 3 e n.º 4 do art. 14.º [cf. Regulamento dos Centros de Dados do SIED e do SIS, aprovado em anexo à Resolução do Conselho de Ministros n.º 188/2017, de 23/11/2017, em especial arts. 4.º, alíneas *a*) e *b*), e 6.º, n.º 3, quanto à competência dos diretores dos centros de dados]) e o regime de segredo de Estado aplicável ao SIRP (cf. n.º 5 do art. 14.º — regime esse aprovado pela Lei n.º 6/94, de 7 de abril).

**3** — Os traços de regime que acima se referenciam — parcial e fragmentariamente abordados na fundamentação que fez maioria quanto à declaração de inconstitucionalidade constante da alínea *c*) da Decisão — não podem deixar de se levar em consideração, em especial, para efeitos da posterior análise — uma vez afastada a violação do parâmetro constante do artigo 34.º, n.º 4, da Constituição —, da proporcionalidade (art. 18.º, n.º 2, da Constituição) das medidas de acesso a dados de tráfego previstas no artigo 4.º da LO n.º 4/2017, à luz dos direitos fundamentais (pelas mesmas restringidos) consagrados nos artigos 26.º, n.º 1, e 35.º, n.ºs 1 e 4, da Constituição. Tal análise será efetuada após a explicitação do vencimento parcial quanto à decisão, constante da alínea *a*) da fórmula decisória do Acórdão, de declaração de inconstitucionalidade com força obrigatória geral do segmento do artigo 3.º da LO n.º 4/2017 que prevê o acesso a dados de base e de localização de equipamento para efeitos de produção de informações necessárias à salvaguarda da *defesa nacional* e da *segurança interna*.

**A2. O enquadramento das normas sindicadas à luz do Direito da União Europeia**

**4 —** No que respeita ao enquadramento das normas sindicadas à luz do Direito da União Europeia, o Acórdão faz referência ao quadro europeu relevante (cf. II — Fundamentos, 6. Enquadramento, *b*) O quadro europeu, e *c*) a jurisprudência europeia em matéria de proteção da privacidade das comunicações eletrónicas, i. *A Carta dos Direitos Fundamentais da UE*). Não obstante, afiguram-se ainda pertinentes algumas referências (e precisões) no tocante ao enquadramento de Direito da União Europeia, na medida em que igualmente relevam, na perspetiva que se adota, para alcançar o juízo de não inconstitucionalidade das normas sindicadas que subscrevemos: *i*) quanto ao *âmbito de aplicação* do Direito da União Europeia; ii) quanto às *especificidades de regime* resultantes do Direito da União Europeia; e, por fim, iii) quanto ao *alcance* da jurisprudência do TJUE (e do TEDH) mencionada no Acórdão.

*i*) Em primeiro lugar, quanto ao *âmbito de aplicação do Direito da União*, verifica-se, como mencionado no Acórdão (cf. em especial II, 6., *b*)), que a matéria relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas é objeto de regulação pelo Direito da União Europeia, em especial por atos de direito derivado com vista à harmonização das legislações dos Estados membros, pelo que o disposto no artigo 1.º, n.º 4, da Lei n.º 41/2004, de 18 de agosto ("Lei da Privacidade nas Comunicações Eletrónicas", que transpõe o Direito da União para a ordem jurídica interna), segundo o qual a definição das exceções (e respetivo regime jurídico) à aplicação da mesma «que se mostrem estritamente necessárias para a proteção de atividades relacionadas com a segurança pública, a defesa, a segurança do Estado e a prevenção, investigação e repressão de infrações penais são definidas em legislação especial» se justifica e compreende à luz do previsto nos artigos 1.º, n.º 3, e 15.º, n.º 1, da Diretiva 2002/58/CEE — assim

retomando aquele art. 1.º, n.º 4 (acrescente-se) as atividades excluídas do âmbito de aplicação da Diretiva 2002/57/CE pelo respetivo art. 1.º, n.º 3.

Sendo a regra, no que respeita ao âmbito de aplicação da Diretiva em causa (Diretiva 2002/58/CEE, na redação decorrente da Diretiva 2009/136/CE), tal como previsto no n.º 3 do seu artigo 1.º, que a mesma não se aplica a «atividades fora do âmbito do Tratado que instituiu a Comunidade Europeia», tais como as abrangidas pelos Títulos V e VI do TUE [à data (i.e., anteriormente à entrada em vigor do Tratado de Lisboa) D*isposições relativas à Política Externa e de Segurança Comum* (arts. 11.º-28.º do TUE) e *Disposições relativas à cooperação policial e judiciária em matéria penal* (arts. 29.º-42.º do TUE), respetivamente] e, «em caso algum, é aplicável às atividades relacionadas com a *segurança pública, a defesa, a segurança do Estado* (incluindo o bem-estar económico do Estado quando as atividades se relacionem com matérias de segurança do Estado) e as atividades do Estado em *matéria de direito penal*» (itálicos acrescentados), a mesma regra deve ser entendida à luz do disposto em duas outras fontes de Direito da União.

Por um lado, à luz do disposto no artigo 4.º, n.º 2, segundo parágrafo, *in fine,* e terceiro parágrafo, do TUE, segundo os quais, por um lado, a União respeita as funções essenciais do Estado, nomeadamente as que se destinam a garantir a integridade territorial, a manter a ordem pública e a *salvaguardar a segurança nacional* e, por outro lado, «Em especial, a *segurança nacional* continua a ser da *exclusiva responsabilidade* de cada Estado membro» (itálicos acrescentados) — assim afastando a inclusão da segurança nacional nas atribuições (partilhadas ou destinadas a apoiar, coordenar ou completar a ação dos Estados membros) da União Europeia.

Por outro lado, à luz do disposto no Regulamento Geral de Proteção de Dados (RGPD), aprovado pelo Regulamento (UE) n.º 2016/679 — o qual (como é referido no Acórdão) revogou a Diretiva n.º 95/46/CE (transposta pela Lei n.º 67/98, de 26 de outubro, "Lei de Proteção de Dados Pessoais") que a referida Diretiva n.º 2002/58/CE visou especificar e complementar (cf. art. 94.º e 95.º do RGPD). Com efeito, tal como disposto no artigo 1.º («Âmbito e objetivos»), n.º 3, da Diretiva 2002/58/CE, também o artigo 2.º, n.º 2, do RGPD («Âmbito de aplicação material») — que constitui, diversamente das Diretivas citadas, direito uniforme diretamente aplicável nos Estados membros — dispõe que o mesmo não se aplica ao tratamento de dados pessoais: *a*) Efetuada no exercício de atividades não sujeitas à aplicação do Direito da União; *b*) Efetuado pelos Estados membros no exercício de atividades abrangidas pelo âmbito de aplicação do Título V, capítulo 2, do TUE (ou seja, depois da entrada em vigor do Tratado de Lisboa, as *Disposições específicas relativas à Política Externa e de Segurança Comum* [Secção 1 — Disposições Comuns, arts. 23.º-41.º e Secção 2, Disposições relativas à Política Comum de Segurança e Defesa, arts. 42.º-46.º, todos do TUE]); *d*)Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública (note-se, aliás, que a delimitação negativa do âmbito de aplicação do RGPD é retomado no artigo 2.º, n.º 2, alíneas *a*)*, b*) e *d*) da *Proposta de Regulamento relativo à privacidade e às comunicações eletrónicas* — COM(2017) 10 final de 10/1/2017).

Pese embora a não exata coincidência entre o elenco de domínios subtraídos ao âmbito de aplicação do direito derivado da União — por um lado, atividades fora do âmbito do [então] Tratado que instituiu a Comunidade Europeia [hoje, Tratado sobre o Funcionamento da União Europeia (TFUE)], atividades relacionadas com a segurança pública, a defesa, a segurança do Estado e as atividades do Estado em matéria de direito penal, por um lado (segundo o direito harmonizado); e, por outro lado, as atividades não sujeitas à aplicação do Direito da União, as atividades abrangidas pelo âmbito de aplicação das *Disposições específicas relativas à Política Externa e de Segurança Comum* e as atividades relacionadas com a prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública (segundo o direito uniforme) — resulta daqueles vários preceitos a ideia essencial de que há um conjunto de domínios materiais (e correspondentes fins do Estado) à partida subtraído ao âmbito de aplicação do Direito da União — e relativamente aos quais, sendo possível aos Estados membros (e à União, como resultou da aprovação da Diretiva n.º 2006/24/CE e durante a sua vigência) usar da faculdade de aprovar medidas legislativas excecionais (e restritivas dos direitos consagrados também pelo ordenamento da União), as mesmas se encontrarem sujeitas, apenas nesse caso, a um regime que, ainda que seja objeto de uma harmonização mínima (como

disposto no art. 15.º, n.º 1, da Diretiva n.º 2002/58/CE), comporta ainda, por força da natureza de tais fins, *especificidades* resultantes de tal natureza.

*ii*) Assim, e em segundo lugar, quanto às e*specificidades* decorrentes do regime de Direito da União aplicável no caso aprovação, a título facultativo, das referidas medidas legislativas restritivas do âmbito dos direitos e obrigações decorrentes do mesmo Direito, não releva apenas o disposto no n.º 1 do art. 15.º da Diretiva n.º 2002/58/CE (*Aplicação de determinadas disposições da Diretiva 95/46/CE* — a qual, recorde-se, foi revogada pelo art. 94.º do RGPD) — que estabelece os *fins* (dos Estados membros) passíveis de justificar a adoção, a título facultativo, de medidas restritivas pelos mesmos Estados membros (salvaguarda da segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas) e os *limites* a observar na adoção de tais medidas («medida necessária, adequada e proporcionada numa sociedade democrática», para a salvaguarda de tais fins e, ainda, conformidade das mesmas com os «princípios gerais do direito comunitário, incluindo os mencionados nos [à data] n.os 1 e 2 do artigo 6.º do Tratado da União Europeia» [após a entrada em vigor do Tratado de Lisboa, no art. 2.º e no art. 6.º do TUE]) — mas igualmente o que hoje se dispõe no artigo 23.º do RGPD (que, por constar de ato de direito derivado com aplicabilidade direta, tem precedência sobre o disposto em atos de harmonização já que estes convocam necessariamente a transposição respetiva por ato legislativo nacional), preceito que não mereceu, todavia, qualquer referência na Fundamentação do Acórdão.

O artigo 23.º do RGPD, com a epígrafe «*Limitações*»*,* prevê, no que relevará para o juízo de não inconstitucionalidade que se adota, que o Direito da União ou dos Estados membros pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º (todos do RGPD), na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 12.º a 22.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar os fins previstos nas respetivas (além das demais) alíneas *a*), *b*)*, c*) e *d*), que correspondem aos domínios à partida *subtraídos* ao âmbito de aplicação do próprio RGPD (i.e., do Direito da União) — a *segurança do Estado*, a *defesa*, a *segurança pública* e a *prevenção, investigação, deteção ou repressão de infrações penais, ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública* (previsão retomada no art. 11.º, n.º 1, da referida Proposta de Regulamento relativo à privacidade e às comunicações eletrónicas, que igualmente prevê que os prestadores de serviços de telecomunicações eletrónicas devem prever procedimentos internos para dar resposta ao pedido de acesso aos dados nos termos das referidas medidas legislativas, da União ou nacionais). Neste ponto, o conteúdo do n.º 1 do artigo 23.º do RGPD não se distancia, no essencial, da previsão anterior contida no n.º 1 do artigo 15.º da Diretiva n.º 2002/58/CE. Todavia, o n.º 2 do artigo 23.º do RGPD prevê — de modo *inovatório* face aquele artigo — que as medidas legislativas adotadas ao abrigo do n.º 1 e para os fins neste previstos, incluem, quando for relevante, «disposições explícitas» pelo menos relativas a um conjunto de itens (previstos nas alíneas *a*) a *h*) do mesmo n.º 2), incluindo ao direito dos titulares dos dados a serem informados da limitação, mas com uma *ressalva* que se afigura essencial para os presentes autos e omitida no Acórdão — «a menos que tal possa prejudicar o objetivo da limitação».

Pese embora a aplicabilidade direta do RGPD, a Lei n.º 58/2019, de 8 de agosto, que «assegura a execução, na ordem jurídica nacional» daquele RGPD, dispõe expressamente, que a lei «não se aplica aos ficheiros de dados pessoais constituídos e mantidos sob a responsabilidade do Sistema de Informações da República Portuguesa, que se rege por disposições específicas, nos termos da lei» — em consonância com o âmbito de aplicação material do RGPD fixado (negativamente) no seu artigo 2.º, n.º 2, e com as limitações enunciadas no artigo 23.º do mesmo Regulamento — sendo a «lei» para que aquele preceito remete, entre outras, a LO n.º 4/2017 em que se inserem as normas sindicadas nos presentes autos.

*iii*) Por último, e em terceiro lugar, quanto ao exato *alcance* da jurisprudência do TJUE mencionada no Acórdão e factualidade subjacente, em especial a jurisprudência prolatada no caso *Tele2/Watson* (referida em II, 6., *b*), e *c*), i.) e no caso *Digital Ireland e.o.* (referida em II, 6., *c*), *i*),

cumpre precisar um aspeto essencial (omisso no Acórdão) que distingue os casos e as normas nacionais apreciados no acórdão *Tele2/Watson* das normas sindicadas nos presentes autos.

Não obstante estarem em causa naqueles casos apreciados pelo TJUE — tal como nos presentes autos —, medidas legislativas (nacionais) previstas no art. 15.º, n.º 1, da Diretiva 2002/58/CE, que derrogam (a exceção) o princípio da confidencialidade das comunicações e dos correspondentes dados de tráfego (a regra), as medidas que estiveram na origem da pronúncia prejudicial do TJUE — *diversamente* das sindicadas nos presentes autos — previam, para efeitos de luta contra a criminalidade, «uma conservação generalizada e indiferenciada de todos os dados de tráfego e dos dados de localização de todos os assinantes e utilizadores registados relativos a todos os meios de comunicação eletrónica e que obriga os prestadores de serviços de comunicações eletrónicas a conservarem esses dados de forma sistemática, contínua e sem nenhuma exceção» (cf. n.º 97, quanto às medidas em causa no caso *Tele2 Sverige AB*, C-203/15) — respondendo o TJUE à primeira questão prejudicial colocada pelo órgão jurisdicional nacional da Suécia no sentido de a interpretação das normas de Direito da União em causa (art. 15.º, n.º 1, da Diretiva 2002/58/CE, lido à luz dos arts. 7.º, 8.º e 11.º e 52.º n.º 1, da Carta) se opõe a tal regulamentação nacional (cf. n.º 112 e, n.º 134, 1), da fórmula decisória, do acórdão).

Como resulta da decisão de colocação da questão prejudicial, as categorias de dados visados pela legislação nacional da Suécia correspondiam, em substância, àquelas cuja conservação estava prevista na Diretiva 2006/24/CE — que, relembre-se, até ser julgada inválida pelo TJUE no caso *Digital Ireland*, visava harmonizar o direito dos Estados membros relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas (publicamente disponíveis ou de um rede pública de comunicações) em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de *investigação, de deteção e de repressão de crimes graves* (tal como definidos no direito nacional de cada Estado membro) —, assim subtraindo ao âmbito de aplicação do n.º 1 do art. 15.º da Diretiva 2002/58/CE os dados em causa, cuja conservação decorria do regime da Diretiva 2006/24/CE e para os referidos fins em causa (cf. art. 11.º da Diretiva 2006/24/CE, que introduziu um novo n.º 1-A na Diretiva 2002/58/CE).

O acórdão *Tele2/Watson,* ainda que apenas na fundamentação*,* não deixa aliás de admitir expressamente que as disposições de Direito da União aí interpretadas *não se opõem* a que um Estado adote regulamentação que permita, a título preventivo, a *conservação seletiva* dos dados de tráfego e de localização, para efeitos de luta contra a criminalidade *grave*, desde que a conservação dos dados observe um conjunto de requisitos (cf. n.º 108) — conservação limitada ao estritamente necessário no que se refere às categorias de dados a conservar, aos equipamentos de comunicação visados, às pessoas em causa e à duração de conservação fixada — para cujo cumprimento o TJUE indica de seguida diversas condições (cf. n.os 108 a 111). E, entre tais condições, indica o TJUE que no que respeita à delimitação de uma medida quanto ao público e às situações potencialmente abrangidas, a regulamentação nacional «deve basear-se em elementos objetivos que permitam visar um público cujos dados sejam suscetíveis de revelar uma relação, pelo menos indireta, com atos de criminalidade grave ou de prevenir um risco grave para a segurança pública», nomeadamente através de um «critério geográfico quando as autoridades nacionais competentes considerem, com base em elementos objetivos, que existe um risco elevado de preparação ou de execução desses atos, numa ou em mais zonas geográficas» (cf. n.º 111).

Considerando a concreta legislação em causa no primeiro caso, a interpretação do arco normativo de Direito da União que inclui o artigo 15.º, n.º 1, da Diretiva 2002/58/CE, na parte que se refere à luta contra a *criminalidade grave* constante do enunciado da decisão (cf. 134, 1)) não pode deixar de ser entendida no específico contexto da transposição da Diretiva 2006/24/CE que, como se referiu, visava (cf. art. 1.º, n.º 1) harmonizar o direito dos Estados membros quanto às obrigações dos fornecedores de serviços de comunicações eletrónicas para garantir a disponibilidade de certos dados por eles gerados ou tratados, para garantir a sua disponibilidade (apenas) para efeitos de investigação, de deteção e de repressão de *crimes graves.* E, pese embora esse específico contexto (e fim, admitido pelo Direito da União como fundamento de medidas restritivas), a interpretação afasta (tão só) a conformidade com o Direito da União de medidas legislativas nacionais que prevejam uma *conservação generalizada e indiferenciada de todos os dados* (de tráfego

e de localização), *de todos os assinantes e utilizadores registados e, relação a todos os meios de comunicação eletrónica,* mas não resulta afastada à partida a *conservação seletiva* dos dados (de tráfego e de localização) em causa — a montante do respetivo acesso para os fins dos Estados membros elencados pelo Direito da União em derrogação (exceção) do princípio da confidencialidade das comunicações e dos correspondentes dados de tráfego (a regra).

Quanto à *segunda questão prejudicial* a que o TJUE deu resposta (em ambos os processos) — que este considerou independente do carácter generalizado ou circunscrito de uma conservação de dados i.e, independentemente do âmbito da obrigação de conservação de dados imposta aos prestadores de serviços de telecomunicações (cf. 113) — não pode deixar de sublinhar-se também o exato contexto da questão (legislação adotada na sequência da Diretiva 2006/24/CE) e teor das normas nacionais pertinentes quanto às condições de acesso aos dados, as exigências de segurança e o prazo de conservação — retomado no enunciado (conjunto) da segunda questão prejudicial apreciada pelo TJUE (*acesso* das autoridades aos dados conservados sem limitar esse acesso apenas para efeitos de luta contra a *criminalidade grave* [reitere-se, o fim único previsto na Diretiva 2006/24/CE — *de investigação, de deteção e de repressão de crimes graves*], acesso não submetido a um controlo prévio por um órgãos jurisdicional ou por uma autoridade administrativa independente e não exigência da conservação dos dados no território da União). Neste específico contexto, o TJUE também não afasta a possibilidade de *acesso* (não generalizado) a certos (não todos) dados conservados devendo a regulamentação nacional que o preveja basear-se em «critérios objetivos para definir as circunstâncias e as condições nas quais deve ser concedido às autoridades nacionais competentes o acesso aos dados dos assinantes ou dos utilizadores registados» em causa (cf. n.º 119). E determina de seguida que o acesso em relação ao (específico) fim em causa — objetivo da luta contra a criminalidade — «só poderá em princípio ser concedido aos dados de pessoas suspeitas de terem planeado, de estarem a cometer ou de terem cometido uma infração grave ou ainda de estarem envolvidas de uma maneira ou de outra numa infração deste tipo» (fazendo apelo, por analogia, ao acórdão proferido pelo TEDH no caso *Zakharov c. Rússia* [também citado no presente Acórdão em 6., *c*), ii., embora sem referenciar as diferenças do caso — e também do citado caso *Big Brother* — relativamente ao regime em que se inserem as normas ora sindicadas, estando ali em causa um regime de *bulk interception* e não de *targeted interception* (cf. caso *Big Brother,* 13/9/2018, par. 315]) mas admitindo também, «em situações específicas como aquelas em que os interesses vitais da segurança nacional, da defesa ou da segurança pública estejam ameaçados por atividades terroristas», o acesso aos «dados de outras pessoas quando existam elementos objetivos que permitam considerar que esses dados podem, num caso concreto, trazer uma contribuição efetiva para a luta contra essas atividades» (*idem,* n.º 119) — respondendo depois à segunda questão prejudicial no sentido de que o Direito da União Europeia se opõe a uma regulamentação nacional que regula o *acesso* aos dados conservados sem respeitar as três condições indicadas pelo TJUE (nos n.os 119, 120 e 122) e (as únicas) levadas à fórmula decisória do acórdão (cf. 134, 2)), entre as quais a limitação do acesso aos dados apenas para efeitos de criminalidade *grave* (condição que o TJUE, no caso *Ministerio Fiscal,* C-207/16, entendeu não ser exigível face ao afastamento da qualificação da ingerência em causa consubstanciada no pedido de acesso (a dados de identificação dos titulares do cartão SIM ativados num telemóvel roubado) como «grave» — cf. n.º 58 a 63).

Por último, e no que respeita à condição referida pelo TJUE no aresto em causa (cf. 121) — informação às pessoas visadas para que estas exerçam, nomeadamente, o direito ao recurso previsto no artigo 15.º, n.º 2, da Diretiva 2002/58/CE — e mencionada no presente Acórdão e neste considerada relevante para o juízo de proporcionalidade efetuado em relação ao artigo 4.º da LO n.º 4/2017 (cf. 11.2.4) — afiguram-se relevantes três notas: *i*) tal condição não foi levada à fórmula decisória (cf., 134, 2)); ii) a remissão para o Capítulo III da Diretiva 95/46/CE deve hoje ler-se como remissão para o Capítulo VIII (art. 77.º e ss.) do RGPD (art. 94.º, n.º 2, do RGPD que revogou aquela) — já em vigor, mais ainda não aplicável, à data da prolação do acórdão *Tele2/Watson* (cf. art. 99.º do RGPD); iii) mas tendo em conta a (já *supra* referida) limitação expressamente prevista na parte final da alínea *h*) do n.º 2 do artigo 23.º do RGPD, i.e., a expressa limitação ao direito dos titulares dos dados a serem informados da limitação «a menos que tal possa prejudicar o objectivo da limitação».

**B**) **A questão de constitucionalidade das normas sindicadas**

**B1**) **A norma do artigo 3.º da Lei Orgânica n.º 4/2017**

**5 —** Vencida parcialmente quanto à decisão e fundamentação na parte em que declara a inconstitucionalidade do segmento que prevê a segurança nacional.

Quanto à declaração de inconstitucionalidade da *norma constante do artigo 3.º da LO n.º 4/2017, na parte em que admite o acesso dos oficiais de informações do SIS e do SIED, relativamente a dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação, para efeitos de produção de informações necessárias à salvaguarda da defesa nacional e da segurança interna, por violação dos artigos 26.º, n.º 1, e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2.º da Constituição da República Portuguesa* (cf. II, 12.), a maioria que fez vencimento, após a análise do regime de acesso consagrado pela LO n.º 4/2017, nomeadamente as finalidades, os critérios, as formas, os limites e as garantias (que não podem deixar de ser completados pelas precisões de regime acima mencionadas), conclui pela não censura das medidas em causa no plano da adequação e da necessidade — conclusão que se acompanha. Todavia, na análise da proporcionalidade em sentido estrito da norma em causa, entendeu a maioria que o juízo de não desproporção não se estende ao segmento da norma que permite o acesso aos dados para efeitos de salvaguarda imediata da defesa nacional e da segurança interna (cf. II, 12.) «sem a mediação de critérios de determinabilidade destes conceitos através de "elementos tipificadores da ação"», já que, além do mais, os conceitos usados na norma questionada são demasiado vagos e estranhos ao universo da judicatura; a exigência de autorização judicial não dá no que a eles respeita, garantias suficientes de que a ingerência na privacidade dos cidadãos se cinge ao mínimo necessário e proporcional; e os conceitos de atribuições essenciais do SIRP remetem para uma prerrogativa de avaliação do SIS e do SIED que frustra o equilíbrio que apenas o escrutínio judicial rigoroso de cada pedido pode assegurar — concluindo que o legislador tem o ónus de concretização, de forma rigorosa e precisa, quais os critérios suscetíveis de justificar o acesso por parte dos oficiais de informações do SIS e do SIED aos dados — de base e de localização de equipamento (tal como definidos na LO n.º 4/2017) — dos cidadãos em causa.

Todavia, diversamente da maioria, entende-se que, quanto ao fim de «produção de informações necessárias à salvaguarda da (...) s*egurança interna*», a densificação do respetivo conceito, se entendido pela maioria como fim autónomo (a par dos demais depois indicados por referência a ilícitos criminais), pode ainda ser encontrada no quadro do sistema, ie, na conjugação do preceito em causa com as leis que regulam essa atividade do Estado (que, tal como a defesa nacional, constitui uma sua atribuição) e, ainda, as atribuições e competências do SIS (Lei n.º 30/84, de 5 de setembro, alterada em último lugar pela LO n.º 4/2014, de 13/8 — Lei Quadro do SIRP). Assim, no que respeita à atividade de produção de informações necessárias à salvaguarda da *segurança interna*, o respetivo conceito (de segurança interna) é ainda densificado no art. 1.º, n.º 1, da Lei n.º 53/2008, de 29/8 (alterada em último lugar pela Lei n.º 21/2019, de 25/2) [«*atividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática*»] — abrangendo esta atividade desenvolvida do Estado expressamente também fins de *prevenção* (e repressão) d*a criminalidade*, designadamente, o terrorismo, a criminalidade violenta ou altamente organizada, a sabotagem e a espionagem (que, nos termos do n.º 3 do mesmo art. 1.º constituem igualmente fins das medidas — de polícia — previstas na mesma Lei de Segurança Interna). E, nos termos da Lei n.º 30/84, as finalidades do SIRP «realizam-se *exclusivamente* mediante as atribuições e competências dos serviços» nela previstos, entre os quais o SIS — que, nos termos da alínea *e*) do n.º 2 do artigo 25.º da LSI, exerce funções de segurança interna — (e o SIED), competindo aos serviços de informação «a produção de informações necessárias à preservação da segurança interna, bem como à independência e interesses nacionais e à unidade do Estado» (art. 2.º, n.º 2). E em concreto ao SIS, enquanto serviço que integra a orgânica do SIRP (alínea *f*) do art. 7.º), compete, nos termos da mesma Lei, a «produção de informações que contribuam para a salvaguarda da segurança interna e a prevenção da sabotagem, do terrorismo, da espionagem e a prática de atos que, pela sua natureza, possam

alterar ou destruir o Estado de direito constitucionalmente estabelecido» (art. 21.º) — finalidades, pelo menos em parte, coincidentes com os fins da própria atividade de segurança interna (prevenção da criminalidade) e também com as finalidade de acesso a dados pelos oficiais do SIS e do SIED previstas no art. 3.º da LO n.º 4/2017 (prevenção de sabotagem, do terrorismo e da espionagem — crimes previstos hoje, respetivamente, no artigo 79.º, com a epígrafe «Dano em bens militares ou de interesse militar», do Código de Justiça Militar (CJM), aprovado pelo artigo 1.º da Lei n.º 100/2003, de 15/11, cujo artigo 2.º, n.º 3, revogou, além do mais, o artigo 315.º do Código Penal que previa então o correspondente crime de «Sabotagem contra a defesa nacional»; no artigo 4.º («Terrorismo») — e 5.º («Terrorismo internacional»), 2.º («Organizações terroristas») e 5.º-A («Financiamento do terrorismo») — da Lei n.º 52/2003, de 22/8, que transpôs para a ordem jurídica interna a Diretiva (UE) 2017/541, do Parlamento e do Conselho, de 15/3/2017, relativa à luta contra o terrorismo (sublinhando-se aliás que a definição de «terrorismo» para efeitos do Código de Processo Penal abrange, no termos da alínea *i*) do seu artigo 1.º, as condutas que integram os crimes de organizações terroristas, terrorismo, terrorismo internacional e financiamento do terrorismo); e, integrando o catálogo de crimes contra a independência e a integridades nacionais, no artigo 317.º do Código Penal («Espionagem») e no artigo 34.º («Espionagem») do mencionado CJM).

Tendo em conta uma leitura integrada e sistémica dos referidos preceitos, considera-se ser ainda possível, pelo menos em parte, reconduzir os fins de tal atividade (de segurança interna) a fins de *prevenção da criminalidade* — concretamente dos crimes referenciados na LSI e, coincidentemente, também no artigo 3.º da LO n.º 4/2017 — em termos que não padecem, pelo menos nessa medida, do apontado vício falta de mediação de critérios de determinabilidade do conceito de segurança interna. Diversamente, não se alcança idêntica conclusão quanto ao segmento do artigo 3.º que se refere à *defesa nacional* (cf. art. 1.º, n.º 1, da Lei n.º 31-A/2009, de 7 de Julho, que aprova a Lei de Defesa Nacional e arts. 7.º, alínea *e*) e 20.º da Lei-Quadro do SIRP), pelo que se acompanha, sem reservas, o juízo de inconstitucionalidade nessa parte. Acompanhando este juízo e com a ressalva acima explicitada, entende-se, pois, que os restantes segmentos da norma do artigo 3.º não violam os artigos 26.º, n.º 1, e 35.º, n.ºs 1 e 4, em conjugação com o artigo 18.º, n.º 2, da Constituição, acompanhando-se, deste modo, a alínea *b*) da Decisão (cf. III, alínea *b*).

**B2**) **A norma do artigo 4.º da Lei Orgânica n.º 4/2017**

**6 —** Vencida quanto à decisão e fundamentação, por considerar que, diversamente da maioria, a norma do artigo 4.º da LO n.º 4/2017 não configura uma violação do artigo 34.º, n.º 4, no que respeita aos dados de tráfego que envolvem comunicação intersubjetiva, e dos artigos 26.º, n.º 1, e 35.º, n.ºs 1 e 4, em conjugação com o artigo 18.º, n.º 2, da Constituição, no que se refere a dados de tráfego que não envolvem comunicação subjetiva.

Quanto à declaração de inconstitucionalidade da *norma constante do artigo 4.º da Lei Orgânica n.º 4/2017, de 25 de agosto, por violação do disposto no artigo 34.º, n.º 4, da Constituição, no que diz respeito ao acesso aos dados de tráfego que envolvem comunicação intersubjetiva, e por violação do disposto nos artigos 26.º, n.º 1 e 35.º, n.ºs 1 e 4, em conjugação com o artigo 18.º, n.º 2, todos da Constituição, no que se refere ao acesso a dados de tráfego que não envolvem comunicação intersubjetiva* (cf. II, 11.), a maioria que fez vencimento entendeu, no que respeita a dados de tráfego que envolvem comunicação intersubjetiva, em linha com o Acórdão n.º 403/2015, que o artigo 34.º, n.º 4, da Constituição limita a possibilidade de ingerência estadual nas comunicações ao âmbito circunscrito do processo criminal (assim afastando a adoção pelo legislador de qualquer solução distinta para a colisão entre os valores constitucionalmente protegidos e os direitos fundamentais em causa), entendendo ainda que as alterações introduzidas pela LO n.º 4/2017 no sistema de acesso não o aproximam de forma decisiva do processo penal em moldes de justificar uma mudança quanto ao juízo de constitucionalidade (cf. 9.2 e 11.1 e explicitação subsequente na fundamentação constante dos pontos 11.1.1 a 11.1.3.). Depois, e no que respeita aos dados de tráfego que *não* envolvem comunicações intersubjetivas, concluiu a maioria, aplicando intensidade de escrutínio equivalente à que considera resultar do parâmetro do artigo 34.º, n.º 4, que a ação de prevenção prevista na norma sindicada, tal como articulada com as condições de admissibilidade previstas no artigo 6.º da LO n.º 4/2017 e tendo em conta a insuficiência dos meios de reação dos

cidadãos contra intervenções ilícitas, «desequilibra desrazoavelmente a ponderação de meio-fim ínsita na vertente apontada do princípio da proporcionalidade», concluindo pela violação do direito à autodeterminação informativa, consagrado nos artigos 26.º, n.º 1, e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2, da Constituição (cf. 11.2 e fundamentação desenvolvida nos pontos 11.2.1 a 11.2.2).

Diversamente da maioria, entende-se que o artigo 4.º da LO n.º 4/2017 (como aliás o artigo 3.º da mesma Lei Orgânica) não viola o disposto no artigo 34.º, n.º 4, da Constituição; e, uma vez superada a violação deste parâmetro constitucional (no que respeita ao âmbito de proteção do mesmo quanto a dados de tráfego que envolvem comunicação intersubjetiva), entende-se igualmente que o artigo 4.º não viola (como aliás o artigo 3.º da mesma LO, no segmento não declarado inconstitucional, não viola) os artigos 26.º, n.º 1, e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2, da Constituição, por a medida de acesso aí consagrada, na sua modelação legal, não configurar uma restrição desproporcionada dos direitos ali consagrados (direito à reserva da intimidade da vida privada e direito à autodeterminação informativa). Isto, pelas razões que de seguida brevemente se explicitam.

**7** — No que respeita ao parâmetro do n.º 4 do artigo 34.º da Constituição, entende-se que os fins e interesses aí fixados passíveis de justificar uma restrição do direito fundamental à inviolabilidade das comunicações — casos previstos na lei *em matéria de processo criminal* (para a maioria, em exclusivo, ou, na expressão do Acórdão n.º 403/2015 pela mesma maioria retomada, uma «reserva absoluta de processo criminal», cf. II, 9.2) —, podem comportar uma leitura mais ampla, por apelo a uma interpretação sistemática (e atualista), quando — como sucede com as medidas de acesso aos metadados em causa nos presentes autos —, estando em causa a salvaguarda de valores e objetivos fundamentais do Estado, como a segurança e a preservação da ordem constitucional (cf. II, 9.2 do Acórdão), contra certos comportamentos especialmente graves suscetíveis de os pôr em perigo e recondutíveis a tipos de ilícitos criminais graves (e que podem configurar criminalidade violenta ou altamente violenta — cf. alíneas *j*) e *l*) do n.º 1 do Código de Processo Penal (CPP)), essa salvaguarda possa implicar restrições ao âmbito de proteção de direitos fundamentais dos cidadãos e, assim, também do direito fundamental à inviolabilidade das comunicações previsto no mesmo artigo 34.º

Por um lado, os valores e objetivos do Estado subjacentes à medida restritiva do direito fundamental em causa, constituem inequivocamente valores e objetivos essencialíssimos do Estado, que encontram respaldo no elenco das «Tarefas fundamentais do Estado» previstas, em especial, nas alíneas *a*) a *c*) do artigo 9.º da Constituição e reflexo no âmbito de proteção dos direitos fundamentais (cf. art. 27.º, n.º 1).

Depois, e em particular, a relevante tarefa estadual de garantia do valor constitucional da segurança (seja interna, seja face ao exterior, seja coletiva, seja individual) — agregando, como se afirma no Acórdão, a dimensão positiva de um conjunto muito vasto de direitos fundamentais e interesses coletivos (cf. II, 12.), não pode deixar de se entender hoje, no que concretamente ao fim de prevenção do «terrorismo» diz respeito, também à luz do disposto na Constituição em matéria de relações internacionais — concretamente na parte em que prevê que Portugal pode «convencionar o exercício, em comum, em cooperação ou pelas instituições da União, dos poderes necessários à construção da união europeia», em particular no que ao «espaço de liberdade, segurança e justiça» (cf. art. 7.º, n.º 6, da Constituição, na redação introduzida em pela revisão constitucional de 1992 e resultante, em último lugar, da revisão constitucional de 2001), domínio material de atribuições da União que constitui domínio de competência partilhada com os Estados membros (cf. art. 4.º n.º 2, alínea *j*) do TFUE) e cujos objetivos abrangem a garantia de um elevado nível de segurança [no território da União e dos seus Estados membros] a prosseguir, nomeadamente através de medidas de prevenção da criminalidade e, se necessário, através da aproximação das legislações penais (cf. art. 67.º, n.º 3, e art. 83.º, n.os 1 e 2, do TFUE) — consistindo o terrorismo um domínio de «criminalidade particularmente grave com dimensão transfronteiriça» (cf. art. 83.º, n.º 1, do TFUE), sendo por isso neste contexto que se integra a mencionada Diretiva (UE) 2017/541, relativa à luta contra o terrorismo.

Depois, sendo os fins do procedimento de acesso aos dados de tráfego (sempre na específica aceção da LO n.º 4/2017) pelos oficiais de informações do SIS e do SIED previsto no artigo 4.º da LO

n.º 4/2017 — produção de informações necessárias à *prevenção de espionagem e do terrorismo* —, identificados por referência a (dois, com a ressalva supra indicada quanto à previsão de punição dos atos e organizações terroristas resultante da transposição da referida Diretiva (UE) 2017/541) tipos de ilícito criminal graves, os mesmos fins — ainda que situados em momento temporal necessariamente prévio às fases preliminares do processo penal, incluindo a fase do inquérito (cf. art. 13.º da LO n.º 4/2017, entendendo-se a prevista intervenção do Procurador-Geral da República no procedimento de molde assegurar, sendo caso disso, o exercício das competências próprias do Ministério Público, em especial o exercício da ação penal e a defesa da legalidade — cf. arts. 219.º, n.º 1, e 220.º, n.º 2, da Constituição) — se afiguram ainda valorativamente próximos, senão equivalentes, aos fins («matéria de processo criminal») legitimadores da intervenção restritiva pelo legislador previstos expressamente na parte final daquele n.º 4 do artigo 34.º da Constituição (sem que exista neste caso uma 'simples' devolução ao legislador da tarefa de fixação dos casos em que tal restrição possa ocorrer, ie, uma autorização explícita do legislador constituinte ao legislador ordinário para legislar sobre os casos de restrição dos direitos fundamentais em causa, sem fixação por aquele do critério a observar pela intervenção deste último, como sucede, v.g., no artigo 35.º, n.º 4, da Constituição, quanto ao direito à autodeterminação informativa e à proteção de dados pessoais, também tido como parâmetro constitucional relevante para a análise da conformidade constitucional das normas sindicadas) — i.e, aos fins que legitimam a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação.

Em suma, mesmo sem admitir à partida uma leitura da Lei Fundamental que permita, em cada momento temporal, 'novas' ponderações pelo legislador ordinário de eventuais colisões entre valores essenciais da comunidade estadual constitucionalmente protegidos (a prosseguir em cada momento face a novos fenómenos ou situações suscetíveis de os pôr em perigo) e direitos fundamentais — e sempre na condição ou no pressuposto de ainda se tratar da proteção de valores nucleares do Estado (como a independência, a soberania nacional, a defesa da ordem constitucional e a segurança, interna e externa) e da qual depende, necessariamente, a proteção de outros tantos valores essenciais do Estado (*maxime* a proteção de direitos, liberdades e garantias) — não pode deixar de se admitir, pelo menos, que a concreta ponderação efetuada pelo legislador constituinte ao fixar como critério de atuação do legislador ordinário a *matéria de processo criminal* admite uma leitura mais abrangente de molde a acomodar nesse critério (que delimita o âmbito das restrições à garantia da inviolabilidade das comunicações) medidas, como a prevista na norma sindicada nos autos, que ainda apresentem identidade valorativa ou axiológica por referência ao mesmo processo criminal, incluindo as suas fases preliminares, que de igual modo se destinem a proteger os referidos valores nucleares da comunidade estadual. A axiologia subjacente à Lei Fundamental e as tarefas por esta cometida ao Estado não podem deixar de convocar uma leitura mais ampla do n.º 4 do artigo 34.º da Constituição admitindo que fiquem ainda abrangidas na sua letra as medidas de acesso previstas na norma sindicada.

Note-se, aliás que a ordem jurídico-constitucional não afasta a hipótese de adoção, mediante autorização judicial, de medidas de acesso a conversações ou comunicações telefónicas ou por qualquer meio técnico diferente do telefone (similares às medidas de acesso em causa mas porventura mais gravosas na medida em que possam incidir sobre o conteúdo das comunicações, o que a LO n.º 4/2017 não contempla), lesivas de certos direitos fundamentais durante a fase preliminar do inquérito, mesmo sem que ocorra a constituição de arguido (cf. art. 187.º, n.º 1 e 189.º , e 58.º, ambos do CPP) [registe-se também a similitude de formulação entre a redação do art. 6.º, n.º 2, alínea *b*) e, quanto aos limites temporais das medidas de acesso, da alínea *d*) do n.º 2 do art. 9.º e a redação dos n.os 1 e 6 do art. 187.º do CPP]), pelo que a aludida projeção da reserva de processo criminal acolhida pela maioria sobre a esfera jurídica da pessoa, em particular quando constituída arguida (cf. II, 9.1), não é sequer certa, já que tal ocorrência pode não se verificar. E note-se também que a ordem jurídico-constitucional não afasta a hipótese de obtenção de dados sobre a localização celular pelas autoridades judiciárias e de polícia criminal, mesmo quando não se referirem a nenhum processo em curso, nos termos previstos no artigo 252.º-A, n.os 1 e 3, do CPP, mas cuja obtenção deve ser comunicada a um juiz. Ora, em qualquer caso, é exatamente a configuração do procedimento de autorização previsto na LO n.º 47/2017 — por órgão integrado na organização judiciária (e no seu nível superior) — e a natureza e estatuto dos seus membros

(magistrados judiciais independentes), aliados aos contornos do procedimento autorizativo e ao controlo (judicial) do mesmo, prévio e durante o tratamento dos dados, que permitem ainda assegurar, de forma não desproporcionada, os direitos dos visados numa fase em que, por força das especificidades próprias do domínio em causa (produção de informações com vista à prevenção de atos que constituem tipos de ilícito criminal graves e criminalidade organizada) a participação dos mesmos é necessariamente, sob pena da frustração de tal fim, ainda excluída.

**8** — Concluindo-se, diversamente da maioria, que o artigo 4.º da LO n.º 4/2017 não viola o n.º 4 do artigo 34.º da Constituição, também no que respeita aos demais parâmetros constitucionais convocados (artigo 35.º, n.os 1 e 4, e artigo 26.º da Constituição) alcançamos conclusão diversa da maioria. Entende-se que a medida de acesso a dados de tráfego (com o específico sentido fixado pela mesma Lei na alínea *c*) do n.º 2 do artigo 2.º) prevista na norma do artigo 4.º, restritiva de direitos fundamentais, tal como articulada, não apenas com as condições de admissibilidade previstas no artigo 6.º da LO n.º 4/2017 (como considerado pela maioria, mas sem levar em conta os demais preceitos que se reportam igualmente ao procedimento de autorização do pedido de acesso — seja à apreciação da necessidade, adequação e proporcionalidade da medida (art. 10.º, n.os 1 e 3), seja à própria noção de «medida pontual de acesso» a autorizar (art. 9.º, n.º 3), cuja proporcionalidade é apreciada pela formação especial de juízes criada pelo legislador e integrada organicamente no STJ), mas articulada necessariamente *também* com os demais traços do regime legal das medidas de acesso aos dados de tráfego, não violam o princípio da proporcionalidade, em especial na sua dimensão de proibição do excesso.

Tal como considera o presente Acórdão quanto às medidas de acesso previstas no artigo 3.º (cf. II, 12., p. 68), também se afigura possível identificar, com suficiente clareza, as razões justificativas das medidas — restritivas de direitos — consagradas no artigo 4.º da LO n.º 4/2017: a proteção de valores constitucionalmente consagrados. Tratando-se de acesso a metadados, concretamente dados de tráfego na aceção própria da LO n.º 4/2017, para efeitos de produção, pelos serviços de informação em causa, de informações necessárias à *prevenção de atos de espionagem e do terrorismo*, está em causa a prevenção de atos e condutas que, na sua essência, visam prejudicar valores essenciais do Estado com consagração constitucional: desde logo, no primeiro caso, interesses militares do Estado português relativos à independência nacional, à unidade e à integridade do Estado ou à sua segurança interna e externa (cf. art. 33.º, n.º 1, por remissão do art. 34.º, n.º 1, alíneas *a*) e *d*) do CJM); e, no segundo caso, a integridade e independência nacionais, funcionamento das instituições constitucionalmente previstas ou intimidação de pessoas, grupos de pessoas ou a população em geral, mediante a prática de certos atos que constituam crimes, em especial contra a vida, a integridade física ou a liberdade das pessoas (cf. art. 2.º, n.º 1, da Lei n.º 52/2003, de 22 de agosto, por remissão do art. 4.º da mesma Lei). Ora, tais valores e interesses inerentes à ordem constitucional do Estado têm inequívoca consagração constitucional (cf., em especial, arts. 1.º, 2.º e 3.º, 9.º, alíneas *a*), *b*) e *c*) e 11.º, n.º 1) e de cuja salvaguarda depende igualmente a salvaguarda dos direitos, liberdades e garantias consagrados na Lei Fundamental.

O acesso aos dados de tráfego previsto no artigo 4.º e com os objetivos aí fixados não merece — tal como não merece o acesso aos dados previsto no artigo 3.º (que, pese embora os conceitos aí utilizados [dados de base e dados de localização de equipamento «quando não deem suporte a uma concreta comunicação»], também abrange, em rigor, dados de tráfego) — censura no que respeita à sua adequação e necessidade: não só a medida de acesso aos dados de tráfego ínsita no artigo 4.º da LO n.º 4/2017 configura um meio idóneo para alcançar o fim de produção de informações necessárias à prevenção de atos de espionagem e do terrorismo, como não se afigura evidente a existência de meios *menos* lesivos (i.e, menos restritivos dos direitos fundamentais em causa) suscetíveis de, com igual eficácia, alcançar os objetivos traçados pelo regime de acesso.

Assim, a eventual desproporção da medida de acesso em causa só poderia resultar da aferição da sua proporcionalidade em sentido estrito, com recurso a uma metodologia de ponderação de bens, ou seja, da aferição da sua justa medida face à prevalecente valia dos fins de interesse público e valores do Estado em causa, também pressuposto e condição da salvaguarda de outros valores igualmente com relevância constitucional. Entende-se, porém, que não há violação do princípio da proporcionalidade na vertente de proibição do excesso, inexistindo violação da proporcionalidade em sentido estrito. Para a formulação de tal juízo de não violação da proporcionalidade em sentido

estrito, ou seja, para a conclusão de que o sacrifício imposto aos direitos fundamentais dos visados pela medida de acesso aos dados de tráfego (e, por maioria de razão aos dados de base e de localização de equipamento na aceção da LO n.º 4/2017) não excede a justa medida, no confronto com os fins visados, afiguram-se essenciais os traços do regime de acesso aos dados contido na LO n.º 4/2017- em que se insere a norma do artigo 4.º sindicada — supra enunciados em A1*, i*) a *iv*), quanto à *iniciativa*, na vertente da *fundamentação do pedido e seu objeto,* ao *controlo judicial e autorização prévia*, à *apreciação judicial* e ao regime de garantias instituído, os quais não foram cabalmente considerados pela fundamentação subscrita pela maioria.

Na apreciação em causa relevam em particular, os elementos do regime atrás indicados que apontam para a contenção — ao estritamente necessário — da medida de acesso aos dados (justa medida), desde logo — e em termos que se consideram determinantes — tratar-se de uma medida de acesso a dados *direcionada* ou *selectiva* (arts. 6.º, n.º 1, alínea *a*), e 9.º, n.º 2), com base numa *suspeita concreta e individualizada* (art. 9.º, n.º 3) e que, além da sua duração temporal limitada, não só não se estende à totalidade dos dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas (independentemente da questão da base jurídica em que se funda, a montante do acesso, tal armazenamento), como não admite a informação em larga escala, por transferência integral dos registos existentes, nem a ligação em tempo real às redes de comunicações eletrónicas (arts. 9.º, n.º, 3 e 6.º, n.º 2). Em especial, a aferição dos pressupostos (alternativos) da autorização do pedido (previstos nas alíneas *a*) e *b*) do n.º 1 do art. 6.º), se não dispensa a observância (pelo requerente) dos elementos que constituem a fundamentação do pedido de acesso, inclusive os factos que o suportam, as finalidades e as razões das medidas pontuais de acesso requeridas e a identificação da pessoa ou pessoas, caso sejam conhecidas, envolvidas nos factos (cf. alíneas *b*) e *c*) do n.º 2 do art. 9.º) — o «juízo de prognose ou da avaliação» feito pelos serviços a que alude a maioria — igualmente não dispensará a sua verificação e ponderação («ponderação da relevância dos fundamentos do pedido», conforme previsto no artigo 5.º, n.º 1) pela entidade que autoriza, em moldes que não se concebem meramente 'automáticos' ou, como parece indicar a maioria, levando a cabo uma apreciação só em função do que os serviços 'formalmente' enunciarem no pedido, assim referenciando qualquer cidadão como «alvo» ou qualquer situação como «urgente» (alíneas *a*) e *b*) do n.º 1 do art. 6.º).

Ora, relevam igualmente para tal apreciação e ponderação os traços de regime (atrás apontados) relativos à autorização prévia, seja quanto à natureza do ente competente, seja quanto aos pressupostos de que depende a decisão autorizativa, seja, ainda, quanto aos critérios que presidem à apreciação e decisão. Neste âmbito entende-se, ao invés da maioria, relevar também de modo determinante para o juízo de proporcionalidade em sentido estrito a natureza do ente competente para a autorização prévia (e controlo) — formação específica das secções criminais do STJ, composta apenas por magistrados (mais antigos) que integram aquelas secções. Ora, ainda que, como sustenta a maioria se estivesse tão só «perante uma atuação de natureza administrativa e não judicial» (cf. II, 11. A questão da constitucionalidade do artigo 4.º da Lei Orgânica n.º 4/2017), a natureza da formação em causa (formação organicamente emanada das secções criminais do STJ) e a qualidade de magistrado judicial dos membros que a integram, com os atributos próprios dessa função, em especial a independência, se apresentam como especiais elementos garantísticos, quer da verificação do preenchimento dos pressupostos de que depende a autorização (em particular os mencionados nos arts. 6.º, n.$^{os}$ 1, alíneas *a*) e *b*)) e da adequada fundamentação «de modo detalhado e circunstanciado» do pedido de acesso (arts. 9.º, n.º 2 e 3, em particular a *suspeita concreta e individualizada* e art. 10.º, n.º 3, quanto às «informações claras e completas» a levar em conta na fundamentação da decisão quanto ao pedido), quer da aferição, necessariamente casuística e com base naqueles fundamentos, da necessidade, adequação e proporcionalidade do pedido de acesso e da sua justa medida face aos fins previstos na lei de molde a salvaguardar os direitos, liberdades e garantias constitucionalmente previstos.

Assim, as medidas de acesso aos dados em causa, porque determinadas no quadro de um procedimento de autorização particularmente exigente, segundo pressupostos e critérios que se afiguram densificados de modo suficiente, orientado pela sua 'estrita necessidade', não configuram um sacrifício dos direitos envolvidos que exceda a justa medida face aos prevalentes *fins* últimos ínsitos na norma sindicada — produção, pelos serviços em causa, de informações necessárias à *prevenção*

*de atos de espionagem e do terrorismo*, i.e, prevenção de atos e condutas que, constituindo tipos de ilícito criminal, visam na sua essência prejudicar ou pôr em perigo valores essenciais do Estado com previsão constitucional e condição da salvaguarda de outros valores igualmente com relevo constitucional, como a proteção de direitos fundamentais. Deste modo a proteção dos relevantes valores do Estado cuja prossecução se visa alcançar através das medidas sindicadas afigura-se sempre de particular grandeza e relevância em moldes que ainda permite justificar, em ponderação, o sacrifício de direitos fundamentais resultante do carácter restritivo das medidas — sublinhe-se, medidas pontuais de acesso, seletivas, casuísticas, orientadas pelo princípio da necessidade de conhecer e limitadas no tempo — de acesso aos dados de tráfego (na aceção da alínea *c*) do n.º 2 do art. 2.º da LO n.º 4/2017), sem que as mesmas se afigurem excessivas para alcançar os fins do Estado em causa, não tendo por isso o legislador ordinário excedido a sua justa medida.

**9** — Três notas se afiguram ainda pertinentes, em particular, quanto à argumentação da maioria no que respeita à desconformidade do artigo 4.º da LO n.º 4/2017 com a Constituição.

Em primeiro lugar, entende-se não proceder a argumentação da maioria quando ancora o juízo de proporcionalidade e a sua violação na falta de previsão na lei de comunicação ao visado das medidas restritivas adotadas ou seja, insuficiência dos meios de reação dos cidadãos contra o acesso aos seus dados — que, por um lado, se encontra expressamente excecionada pelo Direito da União no caso de o direito à informação sobre a limitação poder prejudicar o objetivo da limitação (art. 23.º, n.º 2, alínea *h*), parte final, do RGPD *supra* referido) — o que se entende suceder no acesso aos dados em causa; e, por outro, não integra o enunciado da fórmula decisória adotada pelo TJUE no acórdão proferido, em sede de questão prejudicial de interpretação, no caso *Tele2/Watson* (citada em II, 6., *b*) do Acórdão).

Em segundo lugar, a aplicação, pela maioria que fez vencimento, de uma exigência similar ou equivalente à aplicada no domínio do artigo 34.º, n.º 4, da Constituição, fora da esfera de proteção desta norma, resulta afinal, num idêntica proibição de atuação por parte do legislador ordinário — que parece redundar na limitação da autorização que constitucionalmente lhe é conferida para restringir o conteúdo dos direitos fundamentais tutelados por outras disposições constitucionais também em causa, para além da sujeição ao regime de restrição dos direitos, liberdades e garantias consagrado no artigo 18.º, em especial, n.º 2, da Constituição. Ora, na leitura 'equivalente' da maioria quanto à exigência do controlo de conformidade constitucional aplicada aos artigos 26.º e 35.º da Constituição, parece resultar, inclusive, mesmo em caso de (futura e eventual) diversa ponderação do legislador de revisão constitucional no que ao direito à inviolabilidade das comunicações diz respeito e à matéria que possa justificar a sua eventual restrição, a impossibilidade ou a extrema dificuldade de o legislador exercer a sua margem de apreciação na concretização do mandato constitucional em matéria de restrições de modo a abranger restrições aos direitos em causa justificadas, em ponderação, pelos fins previstos nas normas da LO n.º 4/207 ora sindicadas. Isto já que apenas as parece admitir nos (muito) restritos termos e condições previstos no Acórdão, nomeadamente afirmando que o princípio da proporcionalidade «impõe que o Estado invoque uma situação de *perigo previsível, concreta e de verificação altamente provável* justificando os juízos de prognose através da *identificação normativa da situação fáctica* que está na origem do perigo, a possibilidade de ocorrência de eventos lesivos num prazo próximo e a relação da situação de perigo com pessoas determinadas» (cf. II, 11, 11.2.4, em especial p. 65-66) e a previsão de atos e procedimentos que permitam o conhecimento e a cognoscibilidade da intromissão pelos interessados e a reação contra as medidas restritivas (cf. II, 11, 11.2.4, em especial pp. 65-66).

Em terceiro e último lugar, a fundamentação do acórdão assenta em grande parte num cotejo entre a atividade do SIRP (e do SIS e SIED) e o domínio do processo e da investigação criminal (e da atividade de polícia) — para concluir que o sistema de acesso a dados consagrado pela LO n.º 4/2017 não o aproxima ou equipara, de todo, formal e materialmente, do processo penal (cf. II, 11., 11.1.3) assim não justificando uma mudança quanto ao juízo de inconstitucionalidade formulado no Acórdão n.º 403/2015. Todavia, tal cotejo afigura-se em parte menos adequado já que, pese embora eventuais pontos de contacto, nomeadamente quanto à participação de ambos na prossecução do objetivo de garantir a segurança interna no quadro do Estado e no exercício de funções de segurança interna (cf. art. 25.º, n.º 1 e 2, da já citada LSI), é incontornável a diferenciação das funções próprias cometidas ao SIRP e, no seu quadro, especificamente ao SIS e ao SIED

(já acima mencionadas, cf. arts. 20.º e 21.º da Lei-Quadro do SIRP) e aos órgãos de polícia com competência do domínio criminal (cf. em especial arts. 1.º, 3.º, 6.º e 7.º da Lei n.º 49/2008, de 27/8; art. 3.º da Lei n.º 53/2007, de 31/8; e arts. 2.º e 5.º da Lei n.º 37/2008, de 6/8). Ora, daquele cotejo parece resultar da fundamentação do acórdão uma aplicação do princípio da proibição do excesso segundo um figurino (próprio do contexto de investigação, perseguição e punição de crimes) pelo menos em parte estranho à especificidade própria do domínio de atribuições e competência dos serviços de informação previstos na lei do SIRP — o SIS e o SIED (cf. arts. 21.º e 20, respetivamente, da Lei-Quadro do SIRP).

**10** — Por fim, acresce referir que, submetendo a medida de acesso contida na norma do artigo 4.º da LO n.º 4/2017, na medida em que a mesma configure ainda a concretização de uma das exceções contidas no artigo 15.º, n.º 1, da Diretiva n.º 2002/58/CE, ao crivo dos pressupostos estipulados pela jurisprudência do TJUE no caso *Tele 2/Watson* — na formulação da resposta à segunda questão prejudicial (conjunta) supra enunciada, assim aclarando o sentido interpretativo de um arco normativo que integra a norma do referido n.º 1 do artigo 15.º daquela Diretiva —, a medida de acesso prevista no artigo 4.º da LO n.º 4/2017 sempre respeitaria, inequivocamente, tais pressupostos.

Desde logo, a medida de acesso das autoridades nacionais (SIS e SIED), a dados previamente armazenados, prevista no artigo 4.º, é limitada neste caso, com evidência, à criminalidade grave — por apenas respeitar à produção de informações necessárias à prevenção de atos de *espionagem* e do *terrorismo*. Depois, a medida de acesso em causa é submetida a um controlo prévio de um órgão jurisdicional ou de uma autoridade administrativa, como decorre daquela jurisprudência — condição que, mesmo na perspetiva da maioria (que desqualifica a intervenção, para efeitos de autorização prévia, de uma específica formação das secções criminais do STJ, neste organicamente integrada, composta por juízes dessas secções do STJ), se verifica com evidência.

E, por último, quanto ao requisito da exigência da conservação dos dados em causa em território da União Europeia, admitindo-se não resultar tal exigência de modo expresso do regime geral aplicável à transmissão diferida e conservação em arquivo nos centros de dados do SIS e do SIED (mas que também o não permite expressamente) e acesso aos mesmos (cf. em especial art. 11.º da LO n.º 4/2017 e Portaria n.º 237-A/2018, em especial art. 2.º, n.os 1 e 2), a mesma exigência sempre resultaria necessariamente ou de uma interpretação do direito nacional em conformidade com o Direito da União aplicável na matéria (artigo 15.º, n.º 1, da Diretiva, tal como interpretado pelo TJUE no acórdão *Tele2/Watson*) ou, admitindo-se que as medidas em causa ainda possam ficar, em parte, abrangidas pelo âmbito de aplicação do RGPD, nos termos do regime neste contido — sublinhe-se, com aplicabilidade direta na ordem jurídica interna — quanto à transferência de dados pessoais para países terceiros (e organizações internacionais) contido no seu Capítulo V (artigos 44.º a 50.º).

**11** — Em suma, pelas razões apontadas, considera-se que a medida de acesso a dados de tráfego em causa prevista no artigo 4.º da LO n.º 4/2017, inserida no regime de acesso configurado pelo legislador contido naquele diploma, não viola o princípio da proporcionalidade, por referência ao âmbito de proteção consagrado nos artigos 26.º, n.º 1, e 35.º, n.os 1 e 4, da Constituição, respeitando a mesma norma também, em qualquer caso, os pressupostos decorrentes da jurisprudência pertinente do TJUE. — *Maria José Rangel de Mesquita*

**Declaração de voto**

**1** — Votei vencido na alínea *b*) do dispositivo, que não declara inconstitucional a norma constante do artigo 3.º da Lei Orgânica n.º 4/2017, de 25 de agosto, na parte em que admite o acesso dos oficiais de informações do SIS e do SIED a dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação, para efeitos de produção de informações necessárias à prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada. Por estar convencido de que a norma em causa atenta de forma direta contra a Constituição.

Descontado este aspeto parcelar e localizado, subscrevo em toda a linha o entendimento maioritário e, concretamente, as declarações de inconstitucionalidade constantes das alíneas *a*) e *c*) do dispositivo. Uma concordância nas decisões que vale, igual e irrestritamente, para as fundamentações que, respetivamente, as suportam. Só que é minha convicção que as mesmas razões que sustentam a declaração de inconstitucionalidade da norma constante do artigo 4.º da mesma Lei Orgânica, e atinente ao acesso a dados de tráfego que não envolvem comunicação intersubjetiva — por violação do disposto nos artigos 26.º, n.º 1 e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2, todos da Constituição da República —, impõem a mesma conclusão (de inconstitucionalidade) relativamente à norma constante do artigo 3.º da Lei Orgânica n.º 4/17, aqui em exame.

**2** — Resumidamente e por um lado, sobra unívoco que também a intromissão nos dados de base e de localização que não acompanham comunicações intersubjetivas comportam uma específica e inarredável danosidade. Já como atentado à autodeterminação informacional, já como perigo de devassa da esfera de reserva e privacidade das pessoas concretamente atingidas.

Não se desconhece que a expressividade destes dados, do ponto de vista do desvelamento da vida privada e familiar, e, por vias disso, o potencial de danosidade da intromissão não consentida — quer como dano quer como perigo — se revelam, por natureza e em princípio, menos drásticos quando comparados com a intromissão nos dados a que se reporta o artigo 4.º da Lei Orgânica em exame. A saber: por um lado, os dados de tráfego correspondentes a comunicações intersubjetivas e, como tais, pertinentes à categoria, ao estatuto e ao regime dos dados de telecomunicação; e, por outro lado, os dados de tráfego de *internet,* a sinalizar *inter alia* os *sites* visitados, os documentos consultados e a informação procurada. O que permite aos serviços obter conhecimentos sobre estes dados de tráfego, sua frequência, relacionamento entre si, conteúdos, circunstâncias de lugar, tempo e conexões conjunturais, etc. Tudo dados cujo conhecimento e tratamento podem, consoante os casos, revelar-se particularmente significativos relativamente aos gostos, preocupações, planos, compromissos políticos, ideológicos, filosóficos, correntes de pensamento, condução da vida, tendências, afetos, problemas de saúde, etc. Como podem mesmo, no extremo, permitir traçar perfis psicológicos e reconduzir as pessoas atingidas a tipologias de agentes relevantes para as decisões legislativas ou os movimentos de acompanhamento e vigilância. Não sendo por isso de excluir que a recolha destes dados de tráfego possa, eventualmente, revelar-se mais invasiva e lesiva do que a própria intromissão nos dados de *telecomunicação*, *sc*. dos dados de tráfego correspondentes a circunstâncias externas da comunicação intersubjetiva. De todo o modo e como ficou antecipado, sempre a intromissão não consentida nestes dados de tráfego arrastará consigo um potencial de devassa e de ameaça em princípio mais drástico e gravoso do que a recolha e tratamento dos dados de base e de localização que não suportem atos de comunicação intersubjetiva. Isto é, dos dados de que aqui expressamente curamos.

**3** — Assim, estando aqui em causa atos menos lesivos de intromissão, tal circunstância — ou seja, a menor lesividade — não poderá deixar de ser levada em conta na hora de definir os regimes legais de recolha e tratamento (não consentidos) levados a cabo em nome da salvaguarda dos bens jurídicos individuais e coletivos, atingidos ou ameaçados pelas manifestações de criminalidade a prevenir. Tudo apontando, por isso, para um regime mais permissivo e um quadro mais alargado das autorizações legais, a legitimar as ações de intromissão (nestes dados de base e de localização), com vista à prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e de criminalidade altamente organizada.

Ações que, importa não esquecê-lo, embora menos invasivas — quando comparadas com a intromissão nos dados de tráfego (de telecomunicação ou de internet) a que se reporta o artigo 4.º — comportam sempre um irredutível coeficiente de lesividade do direito à autodeterminação informacional e de perigo para a reserva da vida privada e familiar.

**4** — Tudo, em definitivo, está no desenho e tipificação das constelações fácticas erigidas em pressupostos das autorizações legais que justificam o sacrifício destes bens jurídicos pessoais, nos termos e à luz das exigências do princípio de proporcionalidade (artigo 18.º, n.º 2, da Constituição da República), na plenitude das implicações normativas em que ele se desdobra.

A começar pela satisfação integral das exigências de *legalidade* e de *reserva de lei,* a reclamarem, desde logo, autorizações legais vertidas em leis *claras* e *determinadas.* Isto é, leis que,

à partida, permitam aos seus destinatários identificar com segurança os pressupostos das autorizações: desde o "catálogo" de crimes pertinentes; à densificação material das situações face às quais é objetivamente razoável um juízo de prognose e de antecipação do perigo; à densificação do limiar de suspeita de envolvimento (das pessoas atingidas pela intromissão) nas situações de ameaça ou perigo de uma qualquer daquelas manifestações de criminalidade, etc.

Resumidamente e como de forma clara e vincada refere o presente acórdão a propósito da intromissão nos "dados de tráfego que não envolvem comunicação intersubjetiva", trata-se de levar tão longe quanto possível um exercício de tipificação da *fattispecie* correspondente à autorização legal de intromissão. A reclamar, designadamente e no plano da *law in books*, previsões normativas "face às quais seja possível um juízo materialmente fundado de prognose de ocorrência do perigo para um número circunscrito de bens jurídicos de importância extrema para a comunidade, como a vida, o corpo e a liberdade das pessoas ou a segurança do Estado de direito". E, por vias disso e reflexamente, previsões normativas que no plano da *law in action* não franqueiem a porta à "liberdade de escolha (por parte dos oficiais dos serviços de informações) dos pressupostos que justificam a necessidade da intervenção". Isto porquanto uma "lei vaga, imprecisa e demasiado abrangente converteria as medidas restritivas em arbítrio, por ausência de critérios objetivos quanto à razão de ser da sua utilização".

**5** — Foi por considerar que não satisfaziam estas exigências que — fundada e pertinentemente — o entendimento maioritário declarou a inconstitucionalidade da norma que autoriza a intromissão nos dados de tráfego que não suportam comunicações intersubjetivas contida no artigo 4.º da Lei Orgânica n.º 4/2017. Nomeadamente pelo recurso a conceitos de grande abertura e plasticidade, "semanticamente maleáveis e insuficientemente determinados, no âmbito dos quais a incerteza sobre os pressupostos de acesso aos dados de tráfego é bastante grande, atendendo à singularidade de cada caso concreto". A que acresce a ausência da previsão normativa de mecanismos de reação — a começar pela consagração de formas de notificação ou informação *a posteriori* — das pessoas concretamente atingidas. Que, apanhadas nas malhas deste paradigmático meio oculto de investigação, não tem qualquer forma de reagir contra atos arbitrários e ilegais de intromissão e devassa de que não têm conhecimento. Bem podendo, deste modo, multiplicar-se as "situações em que o indivíduo perde o controlo sobre a circulação dos seus dados pessoais e em que claramente pode ser violado o seu direito à autodeterminação informativa, sendo transformado em 'objeto de informações'".

**6** — São estas, em breve síntese, algumas das razões que sustentam a declaração de inconstitucionalidade da norma constante do artigo 4.º e atinente à intromissão nos dados de tráfego (da internet) não correspondentes a atos de comunicação pessoal à distância. Tudo razões que se ajustam como luva à hipótese normativa aqui em exame e atinente aos dados de base e localização, constante do artigo 3.º da mesma Lei. Precisamente porque se reportam a vícios, insuficiências ou lacunas que resultam no inadimplemento das exigências do princípio da legalidade/determinabilidade, e que inquinam em igual medida ambos os regimes — respetivamente, dos dados de tráfego (artigo 4.º) e dos dados de base e de localização (artigo 3.º) —, nesta parte inteiramente coincidentes. Trata-se, noutros termos, de vícios que atingem os momentos de comunicabilidade e "mesmidade" dos dois regimes e não interferem com aspetos específicos suscetíveis de apontar para soluções normativas diferenciadas. Por vias disso e na medida em que suportam a declaração de inconstitucionalidade da norma do artigo 4.º (relativa aos dados de tráfego que não suportam comunicações intersubjetivas), só podem, por identidade de razões, desencadear em igual medida, a inconstitucionalidade da norma aqui *sub judice* e constante do artigo 3.º da Lei Orgânica n.º 4/2017, de 25 de agosto.

É por isso que (apenas) nesta precisa e localizada dimensão, não acompanho o entendimento que tem por si o sufrágio maioritário do Tribunal. — *Manuel da Costa Andrade*

[1] "[...]

c) *Declarar a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4.º, da Lei Orgânica n.º 4/2017, de 25 de agosto, por violação do disposto no artigo 34.º, n.º 4, da Constituição, no que diz respeito ao acesso aos dados de tráfego que envolvam comunicação intersubjetiva, e por violação do disposto nos artigos 26.º, n.º 1 e 35.º, n.os 1 e 4, este em conjugação com o artigo 18.º, n.º 2, todos da Constituição, no que se refere ao acesso a dados de tráfego que não envolvam comunicação intersubjetiva.*

[...]".

[2] "[...] *a*) *declarar a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 3.º, da Lei Orgânica n.º 4/2017, de 25 de agosto, na parte em que admite o acesso dos oficiais de informações do Serviço de Informações de Segurança (SIS*) e *do Serviço de Informações Estratégicas e de Defesa (SIED), relativamente a dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação, para efeitos de produção de informações necessárias à salvaguarda da defesa nacional e da segurança interna, por violação dos artigos 26.º, n.º 1, e 35.º, n.os 1 e 4, em conjugação com o artigo 18.º, n.º 2, da Constituição da República Portuguesa;*

[...]".

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

[...]".

[4] Esta disposição — que integrava um diploma contendo uma alteração global do Regime Jurídico do Sistema de Informações da República Portuguesa, substituindo as Leis n.os 30/84, de 5 de setembro, e 9/2007, de 19 de fevereiro — tinha o seguinte conteúdo:

*Artigo 78.º*

***Acesso a dados e informação***

*1 —*

*2 — Os oficiais de informações do SIS e do SIED podem, para efeitos do disposto na alínea c*) do *n.º 2 do artigo 4.º, e no seu exclusivo âmbito, aceder a informação bancária, a informação fiscal, a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização, sempre que sejam necessários, adequados e proporcionais, numa sociedade democrática, para o cumprimento das atribuições legais dos serviços de informações, mediante a autorização prévia e obrigatória da Comissão de Controlo Prévio, na sequência de pedido devidamente fundamentado.*

[5] Aí se referiu:

"[...]

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

[...]".

Esta específica questão foi por mim abordada, nesse contexto processual, no item 9.2. do voto de vencido que juntei ao Acórdão n.º 403/2015, também por referência ao valor persuasivo que atribuí — e continuo a atribuir — ao Acórdão n.º 486/2009 (cf. o ponto 2.2. deste).

[6] Referi-me a esse *espaço de proximidade* — creio ser um termo apropriado — no ponto 10.1. do voto de vencido no Acórdão n.º 403/2015.

[7] Frederic F. Manget, "Intelligence And Law Enforcement", *in The Oxford Handbook of National Security Intelligence*, (ed. Loch K. Johnson), Oxford University Press, Oxford, 2009, p. 189.

[8] A ideia de um *ciclo* (que etimologicamente corresponde a um círculo) *de produção de informações* conceptualiza a dinâmica da função de produção de informações, através da qual, "[...] *sequenciando atividades portadoras de uma funcionalidade específica, se cria uma narrativa, ligando os diversos passos envolvidos na criação de um produto final, designado 'informação'* [*intelligence*], começando pela recolha de informações de base ou de notícias [*collection of raw material*] [...], conduzindo, após processamento (validação, cotejo, análise e avaliação), a um relato sistematizado dirigido a um destinatário [*to some form of intelligence reporting to an end user*], *seja este um decisor politico, um comandante militar ou uma autoridade encarregue da perseguição criminal* [...]. *É a ideia de que a informação assim tratada acrescenta valor ao processo decisório relativo às políticas públicas* [situadas nos diversos níveis funcionais dos destinatários] *e induz uma resposta do destinatário que conduz esta narrativa a uma espécie de retorno sobre si própria, gerando como que um efeito de feedback que realimenta o processo já num plano superior, expressando a sua descrição, antes linearmente apresentada, como um ciclo*" [David Omand, "Is it time to move beyond the intelligence Cycle?", *Understanding the Intelligence Cycle*, (MarK Phythian, ed), Routledge, Londres, Nova York, 2014, p. 134].

[9] "[*A*] *característica comum e principal desta atividade reside no seu caráter sensível, por questões de propriedade e de legalidade, mas principalmente por razões de vulnerabilidade das suas fontes e métodos à adoção de contramedidas* [...]. *Daqui decorre o caráter secreto da atividade de informações: o secretismo constitui a imagem de marca das informações, a base da sua relação com o governo (com o destinatário da informação) e a sua autoimagem*" (Michael Herman, *Intelligence Services in The Information Age*, Frank Cass Publishers, Londres, 2002, pp. 3/4).

[10] Peter Gill, "«Knowing the self, knowing the other». The comparative analysis of security intelligence", *Handbook of Intelligence Studies* (ed. Loch K. Johnson), Routledge, Londres, Nova York, 2007, p. 89, nota 1.

[11] Peter Gill, "Theories of Intelligence", *The Oxford Handbook of National Security Intelligence*, cit., p. 45.

[12] *Ibidem*.

[13] O risco vale para a produção de informações como fenómeno social referenciável a determinados âmbitos temáticos, em termos bem distintos daqueles que correspondem à tutela penal plasmada nos tipos de perigo concreto ou abstrato. Esta tutela, de cariz antecipatório, assenta na construção de tipos específicos com essa motivação, por contraposição à lesão efetiva do bem jurídico, que define os crimes de dano (cf. Jorge de Figueiredo Dias, *Direito Penal, Parte Geral*, tomo I, 2.ª ed., Coimbra, 2007, pp. 308/310). Relativamente a esses *tipos* (crimes de perigo), estamos, quer no plano da incidência temática, quer no plano da manifestação de situações com esse possível referencial, fora do domínio da produção de informações.

[14] Aos quais é particularmente propensa: "[...] *nos esquemas gerais de perceção do mundo social pelos seus atores e pelo público* [...] *o espaço imaginário do «espião» é incomensuravelmente maior que o seu espaço real* [...]", como certeiramente observou Alain Dewerpe (*Espion. Une anthropologie historique du secret d'État contemporain*, Éditions Gallimard, Paris, 1994, pp. 9/10).

[15] Richard A. Posner, "The 9/11 Report: A Dissent", *The New York Times Book Review*, 29/08/2004, acessível em: https://www.nytimes.com/2004/08/29/books/the-9-11-report-a-dissent.html. Corresponde o texto a uma recensão crítica ao Relatório da Comissão Nacional de Inquérito aos ataques de 11 de setembro (*The National Commission on Terrorist Attacks Upon the United States*), apresentado em julho de 2004: *The 9/11 Commission Report. Final Report of The National Commission on Terrorist Attcks upon the United States. Authorized Edition*, W. W. Norton & Company, Ltd., New York, London, 2004, 568 pp. Tal crítica foi depois desenvolvida no livro de Richard A. Posner, *Preventing Surprise Attacks. Intelligence Reform In The Wake of 9/11*, Rowman & Llittlefield Publishers, New York, Oxford, 2005, pp. 180/185. Note-se que a proposta da criação nos EUA de um serviço de informações doméstico — referida no *Relatório* como equacionar "[...] *a proposal for an 'American MI5"* — foi expressamente rejeitada pela Comissão de Inquérito (cf. pp. 423/425).

[16] "Direito de Polícia", *Tratado de Direito Administrativo Especial*, (coords. Paulo Otero, Pedro Gonçalves) vol. I, Coimbra, 2009, pp. 320/321.

[17] A expressão é associada a um texto publicado em 1989 por Americo R. Cinquegrana ["The Walls (and wires) Have Ears: The Background and First Ten Years of The Foreign Intelligence Surveillance Act of 1978", *in University of Pennsylvania Law Review*, vol. 137, 1989, pp. 793/827] descrevendo essa separação, no quadro dos procedimentos restritivos estabelecidos pelo *Foreign Intelligence Surveillance Act* de 1978, interpretados — nos termos em que então o eram — pela estrutura de controlo judicial estabelecida nesse Diploma, o designado *FISA Court* ou *FISC*.

[18] *The 9/11 Commission Report*…, cit. Neste Relatório consta, no capítulo 3 (*Counterterrorism Evolves* — pp. 71/107, cf., em especial o subcapítulo *Legal Constraints on the FBI and «the Wall»*, pp. 78/80), uma dura crítica do modelo organizacional identificado como "the Wall". A razão histórica dessa separação exacerbada, assentou numa interpretação discutível da prática do *Fisa Court*, na sequência do caso Aldrich Ames (um caso de espionagem, no início dos anos 90 do século passado, que começou num quadro de *intelligence* e terminou como processo crime), visou colocar a perseguição criminal ao abrigo de uma possível "contaminação de provas" originadas na vertente de *intelligence* do FBI. Note-se que a *9/11 Comission* considerou muito positivamente "[*t*]*he removal of 'the wall' that existed before 9/11 between intelligence and law enforcement* [...]".

Trata-se de uma conclusão discutível, dificilmente sustentável na generalidade dos sistemas constitucionais europeus, e cujo suposto caráter benéfico, em termos de eficiência na luta contra o terrorismo internacional, permanece fundamentalmente por demonstrar. Certo é que, no presente (em 2019) dispomos de suficiente conhecimento retrospetivo para sustentar uma avaliação crítica das opções que, então (em 2001/2003) a "quente", na sequência do profundo efeito traumático dos ataques do 11 de setembro, foram tomadas. Sabemos, por exemplo, que a destruição de barreiras à compartimentação de informação (os tão criticados "muros", e a filtragem do conhecimento com base no "princípio da necessidade de saber") conduziu, desde logo, a massivas fugas de informação (casos Chelsea Manning, Edward Snowden, WikiLeaks), e conduziu — e esse é o aspeto aqui verdadeiramente relevante — a um abaixamento significativo dos mecanismos de defesa dos direitos individuais, decorrentes das exigências de controlo do acesso à informação por parte do *Fisa Court*, passando este a emitir, na sequência de alterações legislativas introduzidas em 2008 no *FISA Act*, mandados genéricos (por oposição a permissões de acesso individualizadas, como até então sucedia) de transferência em massa dos dados (de todos os dados) das operadoras de comunicações para os requerentes, concretamente para a NSA, transformando o *Fisa Court*, numa espécie de "*agência administrativa*", com dificuldade em fugir ao duro qualificativo de *"rubber stamp court*" (cf. David Rudenstine, *The Age of Deference. The Supreme Court, National Security, and the Constitutional Order*, Oxford University Press, Oxford, New York, 2016, pp. 145/149, e David E. Sanger, *The Perfect Weapon*. *War, Sabotage, and Fear in the Cyber Age*, Scribe Publications, Londres e Victoria, Austrália, 2018, pp. 65/67).

Podemos atribuir a alguma pressão dos Estados Unidos sobre os aliados europeus certo "contágio" destes por esta prática de facilitação do *acesso em massa* a metadados (não de um acesso individualizado a determinados dados, decorrente de uma suspeita concreta, como inequivocamente sucede com a LM portuguesa) que conduziu à *Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março*, invalidada em 2014 pelo Tribunal de Justiça da União Europeia.

[19] Trata-se de uma asserção muito discutível, tributária de um "determinismo" construído *a posteriori*, já depois de conhecido o resultado, em que os factos-base "perdem" o caráter obscuro e ambíguo que antes (quando a previsão era útil) necessariamente apresentavam. Este viés cognitivo — amplamente desmontado no livro de Richard A. Posner, referido na nota 15 *supra* — é usualmente identificado em psicologia social como "*determinismo insidioso*" (*creeping determinism*), particularmente presente na análise deste tipo de fenómenos (cf. Malcolm Gladwell "Connecting The Dots. The paradoxes of intelligence reform", *The New Yorker*, março 2, 2003, pp. 83 e ss., disponível através da seguinte ligação: https://www.newyorker.com/magazine/2003/03/10/connecting-the-dots: "[...] *'creeping determinism' — the sense that grows on us, in retrospect, that what has happened was actually inevitable — and the chief effect of creeping determinism* [...] *is that it*

*turns unexpected events into expected events.* [...] *'The occurrence of an event increases its reconstructed probability and makes it less surprising than it would have been had the original probability been remembered.'* [...]").

[20] Contabilizando apenas os atentados (efetivamente realizados) posteriores ao 11 de setembro de 2001, isolando nestes os ocorridos em países da União Europeia, com direta ligação ao que se convencionou chamar motivação *jihadista* (expressa na ligação direta à *Al-Qaeda* e ao chamado *Estado Islâmico* ou, simplesmente, numa assumida inspiração por estas estruturas), partindo dos atentados de 11 de março de 2004, em Madrid (ataques à bomba em comboios que provocaram, diretamente, 192 mortos), temos, seguindo o registo constante da *Wikipedia* (na entrada "List of Islamist Terrorist Attacks", https://en.wikipedia.org/wiki/List_of_Islamist_terrorist_attacks, consultada na segunda quinzena de agosto de 2019), 32 ações registadas até maio de 2019, totalizando 444 mortos.

[21] Os serviços de informações apresentam na Alemanha uma estrutura semelhante aos serviços portugueses, assente num serviço interno, o *Departamento Federal de Proteção da Constituição* (*Bundesamt für Verfassungsschutz* — BfV), e um serviço de informações externo, o Serviço Federal de Informações (*Bundesnachrichtendienst* — BND).

[22] V. os artigos 41.º e 43.º da Lei Quadro do SIRP (Lei n.º 30/84, de 5 de setembro, com última alteração pela Lei Orgânica n.º 4/2014, de 13 de agosto); cf. o "Regulamento do Centro de Dados do Serviço de Informações Estratégicas e de Defesa e do Centro de Dados do Serviço de Informações de Segurança", aprovado pela Resolução do Conselho de Ministros n.º 188/2017, publicado no *Diário da República,* 1.ª série — n.º 233 — 5 de dezembro de 2017.

[23] Ponto 1 da decisão: "[*a*] *base de dados de contraterrorismo, como base de dados conjunta de diversos serviços de segurança, visando o combate ao terrorismo internacional, limitada na sua função a facilitar o acesso a informação e que só permite o uso de tal informação para desempenho de funções operacionais em situações excecionais de urgência, é* [tal base] *compatível com a Constituição*".

[24] Refere-se esta decisão de 2016 à alteração dos poderes de investigação do departamento Federal de Polícia Criminal, no quadro da luta contra o terrorismo internacional, ampliando os respetivos poderes de recolha de informação nesse âmbito. A referenciação dos serviços de informações, numa passagem desta decisão, decorreu da permissão, nesse contexto legal (no §20v, sec 5 da *Bundeskriminalamtgesetz*), de troca de informações assim recolhidas com estes, "[...] *existindo indicações factuais da necessidade desses dados à recolha e análise de informação referida a âmbitos situados na competência do BfV* [serviço de informações interno] *e dos serviços militares de contrainformação* [...]"; neste quadro colocou o Tribunal a questão da "mudança do propósito", como elemento de densificação necessário da possibilidade de transferência de dados (cf. o ponto 320 da Sentença de 20/04/2016).

[25] Este acesso individualizado faz toda a diferença, neste domínio, em termos de segurança da informação detida pela operadora e de redução da potencialidade agressiva da recolha de dados. Com efeito, em termos "[...] *de enquadramento jurídico, podemos distinguir dois tipos de recolha de dados relacionados com a produção de informações: (1)* r*elativa a comunicações individualizadas* [*targeted surveillance of individual communications*]*, referidas a alvos concretos, baseada num determinado grau de suspeita relativamente a uma pessoa concreta, organização* [*ou referenciada pelo uso de um determinado equipamento nesse particular contexto*]*; e (2)* v*igilância e recolha de informação não referida a alvos concretos e individualizados e não assente em suspeitas concretas, frequentemente associada a expressões-conceito* [*catchwords*] *do tipo 'vigilância em massa' ou 'recolha em massa'* [*mass surveillance or bulk collection*] *de informação. A Comissão de Veneza do Conselho da Europa utiliza a noção de recolha de informação estratégica relativamente a este último tipo, precisamente para acentuar que o processo de filtragem ou de seleção da informação relevante se refere a uma massa de dados que foi recolhida sem base numa suspeita específica*" [Christian Schaller, "Strategic Surveillance and Extraterritorial Basic Rights Protectin. German Intelligence Law After Snowden", *German Law Journal*, vol. 19, n.º 4 (2018), p. 945].

[26] O sentido desta limitação temática — "[...] *para efeitos de luta contra a criminalidade grave* [...]" — aparece-nos, na jurisprudência posterior do TJUE, como que formulado pela negativa, no Acórdão de 02/10/2018 (processo n.º C-207/19; *Ministerio Fiscal*): "[*o*] *artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que o acesso das autoridades públicas aos dados com vista à identificação dos titulares dos cartões SIM ativados num telemóvel roubado, tais como o apelido, o nome próprio e, sendo caso disso, o endereço desses titulares, constitui uma ingerência nos direitos fundamentais destes últimos, consagrados nesses artigos da Carta, que não apresenta uma gravidade tal que esse acesso deva ser limitado, em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, à luta contra a criminalidade grave*".

[27] Remeto aqui para o que escrevi no voto de vencido no Acórdão n.º 403/2015

"[...]

*É* [...] *relevante sublinhar o contexto da aquisição deste tipo de informação (dos ditos metadados). Pode tratar-se (i)* d*e uma aquisição de informação em larga escala, por transferência integral, para alguma autoridade pública, dos registos existentes num operador, ou pode tratar-se (ii) duma transferência individualizada, realizada (autorizada e controlada) caso a caso, com base numa suspeita concreta e individualizada. É relevante a distinção porque colocam as duas situações problemas muito distintos.*

[...]

[*A*] *segunda situação — a obtenção de dados de tráfego caso a caso —, desde logo pela sua escala, dimensão individualizada e especificamente motivada por factos concretos, controlados exteriormente ao interessado na aquisição da informação, não contém o perigo da verdadeira 'pesca de arrastão' à escala global, que conduziu o Tribunal de Justiça da União Europeia, no Caso Digital Rights Ireland, Ltd. (C-293/12), Acórdão de 8 de abril de 2014, a considerar inválida a 'Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE'.*

*Estava em causa nesta situação, com efeito, a conservação pelos operadores, obrigatoriamente, de dados de tráfego por um período mínimo de seis meses e máximo de dois anos, a qual, incidindo sobre todas as comunicações, indiferenciadamente à escala global europeia, comportava uma ingerência, não substanciada em indícios concretos e atendíveis, 'nos direitos fundamentais de quase toda a população europeia' (v. os pontos 56 e 58 do Acórdão). Ora, este fator de perigo desaparece (no específico sentido em que o Tribunal de Justiça o enunciou) quando o que ocorre é, tão-somente, a prestação de uma informação pelo operador de telecomunicações, em suporte de papel, quanto às chamadas realizadas por um determinado número e à localização espacial dessas chamadas (do equipamento com o qual foram realizadas) por referência a uma antena que distribuiu o sinal. Mais ainda, quando essa informação só é obtida em situações individualizadas, baseadas na existência de indícios consistentes, necessariamente referidos a pressupostos específicos exigentes, controlados caso a caso por uma entidade independente, cuja atuação visa, precisamente, limitar o acesso aos dados e a sua utilização ao estritamente necessário para se alcançar o objetivo prosseguido num espaço de legitimidade legal e constitucional.*

[...]" (sublinhado no original).

[28] Todavia, admitindo que a distinção introduzida pelo Tribunal se refere a alguma ambiguidade significativa presente no elemento dinâmico dos dados de internet (cf. pontos 11.2 e 11.2.1. do Acórdão), parece-me evidente — abordando o exemplo intuitivamente em causa relativamente à internet — que uma listagem dos *sites* visitados por alguém, é tão desafiante, relativamente à ideia de autodeterminação informacional e de proteção da privacidade, como o conhecimento dos números de telemóvel para os quais alguém ligou ou dos quais recebeu comunicações. Considero, pois, que qualquer permissão de acesso a listagens de *sites* visitados — mesmo que assente num relacionamento comunicacional unilateral — traduz-se, como claramente decorre da LM, na obtenção de *dados de tráfego* e, em função do seu especial potencial disruptor da privacidade, deve ser objeto de um rigoroso controlo de pertinência ao enquadramento temático motivador da pretensão de acesso. Ora, é evidente — é mesmo ostensivo — que a LM faz incidir sobre as pretensões de acesso a dados por parte dos serviços de informações mecanismos adjetivos e critérios substanciais de controlo (pela formação judicial autorizante) suficientemente densos, exigentes e, considerando globalmente os diplomas do SIRP, suficientemente diversificados, através da atuação de várias estruturas independentes de fiscalização, para podermos afirmar que existe, em tal contexto, uma exigentíssima filtragem do acesso.

[29] Tal como foi explicitado na discussão travada nesse processo de revisão (estávamos em junho de 1997), pelo Deputado do Partido Socialista José Magalhães (o proponente dessa intercalação):

"[trata-se de] *explicitar dimensões já hoje contidas no artigo 34.º, n.º 4, no sentido de acompanhar a inovação tecnológica, que é um pouco frenética nesta área, em que estão a aparecer criaturas híbridas já sem nada a ver com a correspondência, no sentido clássico nem com as telecomunicações tais quais as conhecíamos nos anos da graça de 1966, 1982 ou 1989 — aliás, ninguém chega a saber qual será bem o conspecto mundial quando for feita a próxima revisão constitucional.*

*Esta cláusula é abrangente e tendente a criar uma espécie de atualização automática do alcance da norma, abrangendo aquilo que a tecnologia for permitindo e estendendo a esses novos espaços tecnológicos o espaço de liberdade que é próprio do artigo 34.º*

[...]" (*Diário da Assembleia da República,* 2.ª série-RC — número 78, p. 2286).

[30] Nas seguintes passagens:

"[...]

*As* [...] *diferenças não esgotam a sua relevância na distinção entre os dados de base e os demais dados decorrentes do serviço de telecomunicações. Elas estendem-se à distinção entre os dados de tráfego e os dados de conteúdo. Sendo verdade que* [...] *a Constituição aproxima estes no sentido de ambos encontrarem acolhimento no artigo 34.º da CRP, mas tal não significa que lhes imponha, necessariamente, um tratamento rigorosamente idêntico. Tal nota distintiva não passou despercebida — e constitui um elemento importante a reter — ao Tribunal Constitucional no Acórdão n.º 486/2009, embora ali não tenha sido desenvolvida, por não interferir com a decisão. Com efeito, observou-se neste aresto:*

*'*[...]

*Aqui chegados, importa, portanto, concluir que os dados da faturação detalhada e os dados da localização celular que fornecem a posição geográfica do equipamento móvel com base em atos de comunicação, na medida em que são tratados para permitir a transmissão das comunicações, são dados de tráfego respeitantes às telecomunicações e, portanto, encontram-se abrangidos pela proteção constitucional conferida ao sigilo das telecomunicações. Outra coisa será o diferente grau de ofensa que o acesso a estes dados reveste para os direitos e liberdades protegidos pelo sigilo das telecomunicações, relativamente às 'escutas telefónicas', quer pela menor informação que revelam, quer pelo facto de não se tratar de um método oculto de obtenção de prova, o que tem suscitado a interrogação sobre se esse acesso deve estar sujeito aos mesmíssimos pressupostos (vide, Mouraz Lopes, em 'Escutas telefónicas: seis teses e uma conclusão', na Revista do Ministério Público, Ano 26.º, n.º 104, p. 143).*

[...]' *(ênfase acrescentado).*

[...]".

E, mais adiante:

"[...]

*A principal razão pela qual terá de ser diferente o tratamento final a conceder aos dados de tráfego, face aos dados de conteúdo, é fácil de compreender: sabendo que as restrições legais permitidas pelo artigo 34.º da CRP estão sempre*

*sujeitas ao princípio da proporcionalidade (neste sentido, cf. Jorge Miranda e Rui Medeiros, Constituição da República Portuguesa Anotada, cit., Tomo I, pág. 774), é por demais evidente que qualquer ponderação de proporcionalidade tem, necessariamente, de considerar, em um dos pratos da balança, a intensidade da lesão, e que, consequentemente, quanto menor a lesão, maior é o leque de atividades que podem ser consideradas legitimadas pela aferição de proporcionalidade.*

*Esta diferença é importante, designadamente, para compreender que* [...] *as posições deste Tribunal sobre a proporcionalidade das restrições de direitos a propósito das escutas telefónicas (dos dados de conteúdo), designadamente nos Acórdãos n.º 426/05 e n.º 4/06, não são imediata e automaticamente transponíveis, por ser relevante a falta de uma total identidade de razão, para a recolha individualizada, caso a caso — e é o que aqui está em causa —, de dados de tráfego.*

[...]".

[31] Como se refere na declaração de voto da Conselheira Maria Lúcia Amaral em 2015.

[32] Como na nota anterior.

[33] É com este sentido que Ahron Barak, fala em "*uniqueness of a Constitution*", como objeto interpretativo (*Purposive Interpretation in Law*, Princeton Univessity Press, Princeton, Oxford, 2005, p. 370).

[34] *Ibidem*, na mesma página.

[35] Dieter Grimm, "Dignity in a Legal Context: Dignity as an Absolut Right", *in*, *Understanding Human Dignity* (ed. Christopher McCrudden), Oxford University Press, Oxford, 2013, p. 384.

[36] O método em geral de elaboração do texto, que originou esse artigo 21.º, e, mais tarde, na versão final, o artigo 34.º, é explicitado por J. J. Gomes Canotilho, Vital Moreira (*Constituição da República Portuguesa Anotada,* Coimbra, 1978, pp. 4/5, nota 11).

[37] Cfr. *Diário da Assembleia Constituinte*, n.º 38, de 28 de agosto de 1975, p. 1058.

[38] Cuja extinção foi, sintomaticamente, logo determinada pelo Decreto-Lei n.º 171/74, de 25 de abril, da Junta de Salvação Nacional.

[39] A transição portuguesa, subsequente ao 25 de Abril, no que respeita à estruturação de uma arquitetura constitucional democrática, traduziu-se num processo gradual, conturbado, que assentou em modelos iniciais ambíguos, referidos a uma designada "democracia popular", que procurava emular experiências históricas conhecidas. A estabilização democrática em Portugal só ocorreu, verdadeiramente, com a Revisão Constitucional de 1982, com a extinção do Conselho da Revolução, sem esquecer a criação do Tribunal Constitucional.

[40] Pelo meio, em 10 de abril de 1983, incluiu este ciclo o assassinato, durante o Congresso da Internacional Socialista, do dirigente palestiniano moderado Issam Sartawi.

[41] Sublinha-se a circunstância de a deriva terrorista de um grupo político em Portugal ter ocorrido em paralelo à consolidação do processo democrático subsequente à Revolução do 25 de Abril. Foi o que sucedeu com o chamado caso FUP/FP25 (cf. o Acórdão do Tribunal Constitucional n.º 231/2004, que decretou a extinção do partido político Força de Unidade Popular, considerando-o, expressamente, um *alter ego* da organização terrorista FP/25).

[42] Este aspeto, na valoração do sentido dos Acórdãos do TJUE *Digital Rights* e *Tele 2*, por Paul F. Scott, *The National Security Constitution*, Hart Studies in Security and Justice, Hart Publishing, Oxford, 2018, pp. 89/92.

[43] Ilustrando com um exemplo referido, exatamente, àquilo que o legislador português não fez, esconjurando o correspondente perigo (já aflorado na nota 18, *supra*), lembramos o conhecimento, no quadro das chamadas *revelações Snowden*, do documento designado *Verizon Order*, referida a uma decisão do *FISA Court*, determinando à operadora em causa a transferência em massa para a *National Security Agency* dos *metadados* referidos a todas as chamadas efetuadas a partir dos EUA, e vice versa (David E. Sanger, *The Perfect Weapon*, cit., p. 66), opção justamente qualificada como decorrente de uma demissão do *FISA Court* do papel de controlo individualizado próprio de uma instância judicial. Exemplifica esta situação como o efeito traumático dos atentados de 11 de setembro "[...] *distorceu a capacidade racional de julgamento* [...]" dos destinatários dessa informação, ao ponto de os lançar num processo de acumulação, desprovido de sentido, de massas completamente ingeríveis de informação, "[...] *simplesmente porque algum dia poderia revelar-se útil*" (*ibidem*).

Esta perversão é justamente designada, no jargão dos analistas, como a *ilusão dos dados*, correspondente a uma patologia de caráter insidioso, indutora de ineficiência na análise, que se oculta num ilusório sentimento de eficácia decorrente de uma disponibilidade estratosférica de massas de informação, todavia impossíveis de explorar com utilidade e, consequentemente, de processar, não obstante parecerem situadas, ali mesmo, como que "*à mão de semear*". Trata-se de uma ilusão pura e simples: "[*d*]*iversas patologias próprias dos sistemas de informações estão relacionadas com esta ilusão*. *O 'sintoma' corresponde à 'procura compulsiva de dados', um comportamento reflexo de instituições cuja razão de ser é a recolha de informações. Os problemas induzem uma procura de cada vez 'mais dados', em lugar de 'melhores dados' ou melhor análise dos dados. Este fenómeno conduz a uma 'sobrecarga de informação', em que a capacidade de análise é socavada pela necessidade de gerir o peso da informação recolhida e, por isso, aparentemente disponível. Agrava-se, deste modo, o problema do 'ruído': uma vez que a probabilidade de os analistas que tratam a informação 'em bruto' se depararem com um fragmento contendo informação de 'alta qualidade' é menor do que a probabilidade de encontrarem algo relativamente de 'menor qualidade', o sistema pode mesmo sucumbir por esmagamento. O 'ruído', num sistema de informações, pode tornar ainda mais difícil 'unir os pontos'* [no original *connect the dots*, referenciando os passatempos de jornal destinados a descobri um desenho coerente num conjunto de pontos; podíamos expressar a mesma ideia com a expressão, alcançar um *desenho coerente*]" (James Sheptycky, "To go beyond the intelligence cycle of intelligence-led policing", *Understanding the Intelligence Cycle*, ed. Mark Phythian, Routledge, Londres, Nova York, 2014, p. 107).

[44] Em domínios objeto de harmonização pelo Direito da União quanto ao nível de proteção — e é este o sentido da chamada jurisprudência *Melloni* — "[...] *de um direito fundamental — i.e., os direitos de defesa, o direito de propriedade, o direito à privacidade — os Estados-Membros carecem de poder de impor quer o nível mais elevado, quer um nível mais*

*baixo de proteção* [...]" (Koen Lenaerts, José A. Gutiérrez-Fons, "A Constitutional Perspetive, *Oxford Principles of European Union Law*, vol. I, eds. Robert Schütz, Takis Tridimas, Oxford University Press, Oxford, 2018, p. 110).

[45] Como se indica no ponto 4.I) do voto de vencido da Conselheira Maria José Rangel de Mesquita.

[46] *O Princípio da Proibição do Excesso na Conformação e no Controlo de Atos Legislativos*, Coimbra, 2017, pp. 257, 606 e 673.

[47] *Ibidem*, pp. 857/858.

[48] Gonçalo de Almeida Ribeiro, *The Decline of Private Law. A Philosophical History of Liberal Legalism*, Hart Publishing, Oxford, 2019, p. 267.

112637542