Uma análise crítica do Acórdão do Tribunal Constitucional n.º 464/2019: o sistema de acesso a metadados ou a segurança *versus* liberdade[1]

Maria Clara Sottomayor

(Juíza do Supremo Tribunal de Justiça)

«Há uma arma de destruição massiva que está sendo usada todos os dias, em todo o mundo, sem que seja preciso o pretexto da guerra.
Essa arma chama-se fome.
Em pleno século XXI, um em cada seis seres humanos passa fome. O custo para superar a fome mundial seria uma fração muito pequena do que se gasta em armamento. A fome será, sem dúvida, a maior causa de insegurança do nosso tempo.
Mencionarei ainda uma outra silenciada violência: em todo o mundo, uma em cada três mulheres foi – ou será – vítima de violência física ou sexual durante o seu tempo de vida. É verdade que, sobre uma grande parte do nosso planeta, pesa uma condenação antecipada pelo fato simples de serem mulheres.
A nossa indignação, porém, é bem menor que o medo. Sem darmos conta, fomos convertidos em soldados de um exército sem nome e, como militares sem farda, deixamos de questionar.
(...)
Há quem tenha medo que o medo acabe».
Mia Couto, *Murar o medo*, Conferência do Estoril, 2011.

[1] Este artigo corresponde, com adaptações e desenvolvimentos, à posição que consta da declaração de voto que entreguei no Tribunal Constitucional para ser junta ao processo n.º 26/2018, após ter participado em todas as reuniões em que o Acórdão foi discutido.

Sumário: **1.** As normas impugnadas e o sentido da decisão do Tribunal Constitucional; **2.** A ligação entre as normas dos artigos 3.º e 4.º da Lei Orgânica n.º 4/2017 e a Lei 32/2008, de 17 de julho sobre a conservação de dados. **3.** O âmbito de proteção do artigo 34.º, n.º 4, da CRP. **4.** A declaração de inconstitucionalidade do artigo 4.º da Lei 4/2017 e a respetiva fundamentação. **4.1.** A divisão da norma em dois segmentos e a escolha do parâmetro constitucional. **4.2.** A violação do artigo 34.º, n.º 4, da CRP no acesso aos dados de comunicação intersubjetiva. **4.3.** A restrição dos direitos fundamentais à privacidade (artigo 26.º, n.º1) e à autodeterminação informativa (artigo 35.º, n.º 1 e 4) no acesso aos dados de tráfego que não envolvem comunicação intersubjetiva. **a)** A indeterminação do conceito de perigo. **b)** A exclusão de um dever de notificação aos visados. **c)** A complexidade e a incerteza do conceito (e do fenómeno) de terrorismo. **5.** A norma do artigo 3.º da Lei 4/2017 e o duplo juízo de constitucionalidade/inconstitucionalidade; **6.** A relação entre o direito constitucional e o direito da União Europeia. **6.1.** A tutela multinível dos direitos fundamentais.

1. As normas impugnadas e o sentido da decisão do Tribunal Constitucional

O Acórdão n.º 464/2019 incidiu sobre a apreciação da constitucionalidade, em processo de fiscalização abstrata sucessiva, das normas dos artigos 3.º º («Acesso a dados de base e de localização de equipamento») e 4.º («Acesso a dados de tráfego») da Lei Orgânica n.º 4/2017, de 25 de agosto, 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 Lei Orgânica 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 (…)» (artigo 1.º, n.º 1).

O teor das normas apreciadas pelo Tribunal Constitucional, no acórdão comentado, é o seguinte:

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.

Nos termos desta lei, por força das definições constantes dos artigos 2.º, 3.º e 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 o acesso a certas categorias de dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, assim legalmente definidas:

A – *Dados de telecomunicações* e *dados de Internet (*alíneas *a*) e *b*) do n.º 1 do artigo 2.º):

> *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.

B – No âmbito da categoria ampla de «dados de telecomunicações e *Internet*», a lei inclui uma classificação tripartida, distinguindo entre *dados de base*, *dados de localização de equipamento* e *dados de tráfego* (alíneas *a*) a *c*) do n.º 2 do artigo 2.º):

> *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 facturação da mesma».

O Tribunal Constitucional declarou a inconstitucionalidade, com força obrigatória geral de um segmento do artigo 3.º e de todo o artigo 4.º, ambos da Lei Orgânica n.º 4/2017, nos seguintes termos:

- A declaração de inconstitucionalidade da norma constante do artigo 3.º da Lei Orgânica n.º 4/2017, de 25 de agosto, limitou-se à parte em que o preceito

admite o acesso dos oficiais 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, da CRP; o Tribunal Constitucional considerou conforme à Constituição o segmento normativo contido na norma constante do artigo 3.º da Lei n.º 4/2017, 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.

- A norma constante do artigo 4.º da Lei n.º 4/2017 foi declarada inconstitucional, mas com fundamentação distinta consoante os dados de tráfego envolvam ou não comunicação intersubjetiva:

i) 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;

ii) 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 CRP, no que se refere ao acesso a dados de tráfego que não envolvem comunicação intersubjetiva.

Para se compreender a complexidade da fundamentação do acórdão, importa ter presente que o Tribunal procedeu à fragmentação do juízo de constitucionalidade sobre o artigo 3.º, tendo considerado um segmento da norma inconstitucional e outra parte do mesmo preceito conforme à Constituição. O que motivou este diferente juízo do Tribunal foi o diferente grau de determinabilidade ou de tipificação dos diferentes bens jurídicos que a norma visa proteger.

Relativamente ao artigo 4.º, o Tribunal declarou a inconstitucionalidade da totalidade da norma, mas também a dividiu, para o efeito de escolha da norma

constitucional paramétrica, entre dois segmentos, consoante os dados de tráfego envolvem, ou não, comunicação intersubjetiva.

2. A ligação entre as normas dos artigos 3.º e 4.º da Lei Orgânica n.º 4/2017 e a Lei 32/2008, de 17 de julho (sobre a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas)

A potencial invasão de dados pessoais, potenciada pelas normas sindicadas pelo Tribunal Constitucional neste Acórdão, agrava-se se considerarmos que, nos termos da Lei n.º 32/2008, de 17 de julho (que transpôs a diretiva 2006/24/EU, que veio a ser invalidada pelo Tribunal de Justiça da União Europeia, doravante TJUE, no acórdão *Digital Rights*), os dados pessoais dos cidadãos (telecomunicações e *internet*) são armazenados pelas empresas fornecedoras de serviços de comunicações eletrónicas e ficam disponíveis durante um ano (artigo 6.º, n.º 1, da Lei 32/2008), estando, durante esse período, disponíveis para serem acedidos pelos serviços de informação no seio de uma operação de prevenção criminal nos moldes definidos na Lei n.º 4/2017. Verifica--se, portanto, uma interação entre ambos os regimes jurídicos: a Lei n.º 32/2008, de 17 de julho (que não integrava o objeto do processo constitucional que deu origem ao acórdão dos metadados) reporta-se ao tratamento de dados (recolha, registo ou conservação), que serão, num momento posterior, *fornecidos* aos serviços de informação e segurança ou adquiridos por estes. Esta lei é questionável pelo âmbito da obrigação de conservação de dados pessoais que prevê – uma conservação generalizada e indiferenciada de todos os dados de tráfego e dos dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica – desrespeitando, quer direitos fundamentais dos cidadãos constitucionalmente protegidos, quer os critérios indicados pelo TJUE (cf. Acórdão *Tele2*, §§106 e ss). Na verdade, estas operações de recolha e de acesso a dados podem atingir, potencialmente, qualquer cidadão (muito para além dos suspeitos de criminalidade grave), sem que disso tenha consciência, bastando uma mera

conexão geográfica com a investigação ou uma conexão ocasional com uma pessoa que esteja a ser fiscalizada. Alguns Tribunais Constitucionais europeus declararam já, nas respetivas jurisdições, a inconstitucionalidade das leis ordinárias que procederam à transposição da Diretiva 2006/24/EU, relativa à conservação de dados (Decisão n.º 1258, de 8 de outubro de 2009, do Tribunal Constitucional romeno; Decisão n.º 256/08, de março de 2010, do Tribunal Constitucional alemão, Decisão de 22 março de 2011, do Tribunal Constitucional checo). Em Portugal, a declaração de inconstitucionalidade da Lei n.º 32/2008 foi já requerida pela Provedora de Justiça, num processo de fiscalização abstrata da constitucionalidade, por restrição desproporcionada dos direitos à reserva da vida privada e ao sigilo das comunicações.

3. O âmbito de proteção do artigo 34.º, n.º 4, da CRP

Após a 5.ª revisão constitucional, ficou claro que o âmbito de proteção do artigo 34.º, n.º 4, da CRP abrange não apenas o conteúdo das telecomunicações, mas também os dados de tráfego, por respeitarem aos elementos funcionais de 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, a data, o tempo e a frequência das ligações efetuadas.

A divisão dos dados de tráfego em dados que envolvem comunicação intersubjetiva e que se referem, não só ao conteúdo das comunicações, mas também às circunstâncias do processo de comunicação (dia, hora, local, duração da mensagem, identidade dos sujeitos), e em dados de tráfego que não envolvem comunicação intersubjetiva, porque relacionados com a relação entre uma pessoa e uma máquina, por exemplo, os sítios da internet que a pessoa consulta, é nova na jurisprudência do Tribunal Constitucional, contrariamente ao largo consenso da doutrina e da jurisprudência, no sentido de incluir todos os dados de tráfego no

conceito de comunicações constitucionalmente relevante para a proibição de ingerência.

Tinha sido já aflorada no Acórdão n.º 403/2015 uma distinção entre dados pessoais que envolvem comunicação e dados pessoais desligados de qualquer ato de comunicação, sujeitando apenas os primeiros à tutela do artigo 34.º, n.º 4, da CRP. Contudo, em vários pontos do acórdão utiliza-se, em contradição com a citada distinção, um conceito unitário de dados de tráfego tutelados pelo artigo 34.º, n.º 4, da CRP e a distinção, entre dados que envolvem comunicação intersubjetiva e dados que não a envolvem, não foi levada ao dispositivo do Acórdão, que declarou a inconstitucionalidade da totalidade da norma do artigo 78.º, n.º 2, sem qualquer subdivisão em segmentos normativos. Os dados pessoais, que inequivocamente a jurisprudência do Tribunal Constitucional entendia estarem fora do âmbito de tutela do artigo 34.º, n.º 4, da CRP, eram 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 (cf. Acórdãos n.ºs 486/2009 e 403/2015). Todavia, mesmo estes, normalmente aparecem associados a uma concreta comunicação e sendo assim merecem a tutela do artigo 34.º, n.º 4, da CRP. Como informa o parecer da Comissão Nacional da Proteção de Dados n.º 38/2017, esta categoria de dados que não estão ligados a um ato de comunicação é meramente residual, pois, nos dias de hoje, ocorrem comunicações mesmo quando o utilizador do equipamento de comunicação não o aciona direta e intencionalmente. É o caso das atualizações do correio eletrónico ou das mensagens que se recebem nos *chats*, o que significa que as comunicações são praticamente constantes, mesmo quando os cidadãos utilizadores dos equipamentos nada fazem.

Se na definição do conceito de comunicações constitucionalmente relevante o Acórdão n.º 464/2019 não deu o salto que se impunha dar, representando até um recuo em relação à jurisprudência anterior, que se reportava a um conceito amplo de dados de tráfego para o incluir na tutela à autodeterminação comunicativa

proporcionada pelo artigo 34.º, n.º 4, da CRP, importa frisar que o Tribunal Constitucional manteve e até reforçou a interpretação garantística do conceito de «matéria de processo penal» do artigo 34.º, n.º 4, da CRP, não cedendo a interpretações extensivas ou analógicas do citado conceito.

O Tribunal Constitucional desde o Acórdão n.º 403/2015, que incidiu sobre questão jurídico-constitucional semelhante à do Acórdão agora comentado, que adere a uma interpretação do artigo 34.º, n.º 4, da CRP, que limita as restrições do direito fundamental ao sigilo das comunicações ao caso expressamente previsto na lei – pendência de um processo penal – rejeitando a admissibilidade hermenêutica de qualquer extensão analógica do conceito de «processo penal» ou de «matéria de processo penal» suscetível de permitir obter fundamento constitucional para restrições ao direito verificadas a montante do processo penal. O Acórdão n.º 464/2019 teve o aspeto positivo de reforçar este alcance da norma constitucional, esclarecendo que «*a limitação das restrições 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*». A possibilidade de uma decisão constitucional «criativa» ou «construtiva» nesta matéria, que propusesse uma identidade valorativa entre o processo penal e a atividade dos serviços de informação no domínio da prevenção

criminal, estaria desde logo afastada pela ideia de Constituição como sistema de direitos fundamentais e pelo princípio *in dubio pro libertate*.

4. A declaração de inconstitucionalidade do artigo 4.º da Lei 4/2017 e a respetiva fundamentação

4.1. A divisão da norma em dois segmentos e a escolha da norma constitucional paramétrica

O Acórdão agora comentado declarou a inconstitucionalidade da norma do artigo 4.º da Lei n.º 4/2017, tendo dividido a mesma em dois segmentos:

i) – uma parte reportada aos dados de tráfego que resultam de atos de comunicação intersubjetiva, envolvendo um número finito de interlocutores e, em regra, determinado pelo emissor da comunicação, por via de *email* ou outro tipo de mensagem;

ii) – outra parte relativa a dados de tráfego que não envolvem comunicação intersubjetiva, mas *comunicações de massa*, dirigidas a um número potencialmente infinito de utilizadores (p.ex. a navegação em rede, visitando e lendo informações em *websites*).

O Acórdão n.º 464/2019 apreciou a constitucionalidade do primeiro segmento, em função do disposto no artigo 34.º, n.º 4, da CRP e a constitucionalidade do segundo, em função das normas dos artigos 35.º, n.º 1 e 26.º, n.º 1, em conjugação com o n.º 2 do artigo 18.º, n.º 2, da CRP.

Enquanto no n.º 4 do artigo 34.º da Constituição, o legislador constituinte apenas autorizou 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 rígidos, que conferem ao legislador uma maior margem de determinação. É que o legislador constituinte, nesta norma, 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, e atribui-lhe poderes de regulação sujeitos ao regime das leis restritivas de direitos, liberdades e garantias consagrado no artigo 18.º da CRP, designadamente, ao princípio da proporcionalidade.

No que concerne aos dados de tráfego no âmbito das comunicações intersubjetivas, é convocável a tutela especial da autodeterminação comunicativa consagrada no artigo 34.º, n.º 4, da CRP. Já os dados de tráfego de internet fora desse âmbito estão protegidos, segundo a conceção do Acórdão n.º 464/2019, apenas pelas normas gerais dos artigos 26.º, n.º1 e 35.º, n.º1 e 4, da CRP, que admitem restrições em domínios que extravasam o âmbito da investigação criminal.

Sendo assim, a apreciação da constitucionalidade deste segmento do artigo 4.º (relativo a dados de tráfego que não envolvem comunicação intersubjetiva), à luz do princípio da proporcionalidade e de juízos de ponderação de valores ou de concordância prática entre direitos em conflito, deixa potencialmente em aberto a margem de manobra ao legislador ordinário para permitir, em futura legislação, o acesso dos serviços de informação da República a estes dados de tráfego excluídos da tutela do artigo 34.º, n.º 4, da CRP.

A principal incoerência da fundamentação do Acórdão n.º 464/2019 diz respeito, desde logo, à escolha de um parâmetro constitucional diferente para aferir da constitucionalidade do segmento do artigo 4.º, que permite o acesso dos serviços de informação aos dados de tráfego que não envolvem comunicação intersubjetiva. É que, admitindo o Acórdão que estes dados pessoais podem ser tão ou mais reveladores da personalidade do utilizador do que os dados de tráfego que envolvem comunicação intersubjetiva, referindo-se a uma «equivalente danosidade» destes dados, não faz sentido que aprecie a constitucionalidade desta norma à luz de uma norma paramétrica distinta, e menos protetora, da que utilizou para aferir a constitucionalidade do segmento do artigo 4.º, que se reporta a dados pessoais provenientes de atos de comunicação entre dois ou mais sujeitos. Esta

dualidade paramétrica, que permite um regime diferenciado de intromissão do Estado nos dados de internet, parece ser mais o fruto de um pragmatismo na luta contra o terrorismo – que precisa de aceder aos dados de navegação dos indivíduos suspeitos – do que uma questão conceitual.

Na verdade, o conceito de comunicações tem vindo constantemente a evoluir por força das novas tecnologias e das mais variadas formas como pode ser utilizada a internet, devendo, a este propósito, fazer-se uma interpretação atualista e dinâmica da Constituição, que abranja não só a interação interpessoal e bidirecional, mas também a comunicação em massa e unidirecional.

Tendo o Acórdão n.º 464/2014 aberto a restrição a estes direitos fundamentais à aplicação do princípio da proporcionalidade, devia tê-lo feito à luz de um critério de proporcionalidade «forte» na apreciação da constitucionalidade. Contudo, limitou-se a prometer «intensidade de escrutínio», «similar ou equivalente» ao grau de intensidade da proteção conferida pelo artigo 34.º, n.º 4, da CRP ou a referir vagamente um «critério de apreciação da constitucionalidade rigoroso», sem retirar daí as implicações protetivas para os direitos dos cidadãos cujos dados de internet poderão estar sujeitos a um acesso pelos serviços de informação, não controlável pelo sujeito visado.

Sabe-se que os dados de tráfego, que resultam da utilização da internet desligados de uma comunicação intersubjetiva, podem traduzir uma comunicação ainda mais íntima e secreta do que aquela que ocorre entre dois sujeitos, consistindo numa forma de comunicação da pessoa consigo mesma, com as suas questões existenciais, pensamentos, dúvidas, sonhos, medos ou angústias, revelando informações sobre os seus hábitos de vida, valores, crenças, gostos, saúde ou a forma como passa os tempos livres, dos quais se podem deduzir características pessoais do utilizador e traços fundamentais da sua personalidade que até nunca são reveladas na comunicação intersubjetiva. O acesso pelos SIRP a dados desta natureza retira aos cidadãos afetados o monopólio do controlo sobre as suas informações – o seu direito a viver só e a controlar o que os outros sabem a

seu respeito – violando o seu direito à autodeterminação informativa e constituindo uma invasão da privacidade e do direito ao livre desenvolvimento da personalidade dos visados. Estes dados, ficando retidos pelas empresas de telecomunicações, durante um ano, e sendo o acesso dos serviços de informação permitido fora de um processo penal, ou de qualquer processo judicial, potenciam o risco de todos os cidadãos serem controlados pelo Estado e reduzidos a perfis ou *identidades digitalmente criadas* e *heteroconstruídas* com a consequente desumanização dos indivíduos e a sua estandardização por ideologias, valores e crenças, podendo alguns perfis ser etiquetados como "perigosos" para a segurança do Estado com base em preconceitos ou juízos subjetivos e altamente falíveis. Não pode deixar de se equacionar, neste debate – sem desvalorizar a gravidade do fenómeno do terrorismo e a necessidade de o combater – que a luta contra o terrorismo comporta riscos elevados de excesso, correndo-se o risco de sob o pretexto do combate ao terrorismo, alguns cidadãos considerados incómodos serem devassados e reduzidos a um conjunto de informações «catalogadas» em ficheiros dos serviços secretos do Estado.

A este propósito, portanto, a primeira afirmação a fazer é que, por razões de coerência valorativa, colocando-se um segmento do artigo 4.º da lei dos metadados fora do âmbito de proteção do artigo 34.º, n.º 4, da CRP, o critério de proporcionalidade para aferir da constitucionalidade desta norma, ou de outra que no futuro venha a ser aprovada sobre esta matéria, deve ser mais exigente do que aquele que foi aplicado na fundamentação do Acórdão n.º 464/2019, pois estão em causa, não só ofensas à privacidade, à liberdade e à igualdade de tratamento entre todos os cidadãos, na medida em que sempre haverá uns mais fiscalizados do que outros em virtude de pertencerem a categorias suspeitas (p. ex migrantes ou refugiados, ou pessoas politicamente incómodas), como também a **preservação da democracia**. É importante reiterar que o poder dos serviços de informação do Estado no acesso a dados pessoais não se insere dentro de um processo penal ou de qualquer outro processo judicial, que podem nunca vir a ser instaurados, não

dispondo os indivíduos suspeitos, nessa medida, de direitos processuais de defesa contra estas ações de prevenção ou de fiscalização, nem sequer de direitos de informação da existência das mesmas. Para se precaverem contra esta ingerência dos serviços secretos de informação, os indivíduos tenderão a limitar a sua liberdade de movimentos e de expressão com danos para a liberdade de todos e para a própria democracia.

É inevitável antever que dos critérios de apreciação da constitucionalidade deste segmento da norma do artigo 4.º resultam indicações ao legislador sobre o mínimo de garantias que um novo regime jurídico atinente a este tema terá que respeitar para ser considerado conforme à Constituição. Note-se que esta lei já é a segunda, cujas normas relativas ao acesso aos metadados não passam o teste da constitucionalidade. A primeira lei dos metadados, com uma norma sobre o acesso a dados pessoais pelos serviços de informação, foi o Decreto 426/XII da Assembleia da República, que aprovou o regime jurídico do Sistema de Informações da República Portuguesa, objeto de um processo de fiscalização preventiva no Tribunal Constitucional que culminou com a declaração de inconstitucionalidade do n.º 2 do artigo 78.º do citado diploma, por violação do artigo 34.º, n.º 4, da CRP, pelo Acórdão n.º 403/2015.

O afastamento da aplicação da norma paramétrica do artigo 34.º, n.º 4, da CRP para a apreciação do segmento do artigo 4.º, que admite o acesso pelo SIS aos dados de internet que não envolvem comunicação intersubjetiva, representa, no contexto descrito, uma abertura ao legislador, sem que seja necessário um pesado processo de revisão constitucional, para aprovar outra lei que permita o acesso pelo SIS a estes dados de internet, observando os critérios de constitucionalidade apontados no Acórdão n.º 464/2019 e que não incluem, como veremos, um aspeto fundamental para a proteção dos direitos fundamentais: o cumprimento pelos serviços secretos de um **dever de informação ou de notificação**, *a posteriori,* aos cidadãos visados pela ingerência. A coerência valorativa, imposta pela semelhança da devassa que o Tribunal Constitucional reconheceu existir entre o acesso a todos

os dados de tráfego e de internet regulados no artigo 4.º da Lei 4/2017 (independentemente de existir ou não comunicação intersubjetiva), assim o implicaria.

4.2. A violação do artigo 34.º, n.º 4, da CRP no acesso aos dados de comunicação intersubjetiva

O Acórdão do Tribunal Constitucional declarou a inconstitucionalidade do artigo 4.º da Lei Orgânica, por violação do artigo 34.º, n.º 4, mas restringiu a tutela fornecida por esta norma constitucional à comunicação intersubjetiva (mensagens de correio eletrónico, chamadas de telemóvel, conversas por *Voip,* designadamente, *Skype* ou *Whatsapp*) e às suas circunstâncias ou elementos funcionais.

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).

Este segmento da declaração de inconstitucionalidade significa que o legislador ordinário não poderá, fora do âmbito do processo penal e das garantias e meios de defesa de que os arguidos dispõem, permitir aos serviços de informação o acesso a estes dados para o efeito de prevenção criminal. Assegura-se, assim, que a comunicação à distância entre privados se processe como se o 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 e que o Estado não a invada.

O Tribunal Constitucional reiterou assim a orientação do Acórdão n.º 403/2015, sobre o direito à autodeterminação comunicativa e a sua dupla dimensão negativa e positiva: que afirmava o seguinte:

«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».

(...)

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».

(...)

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.»

4.3. A restrição dos direitos fundamentais à privacidade (artigo 26.º, n.º 1) e à autodeterminação informativa (artigo 35.º, n.º 1 e 4) no acesso aos dados de tráfego que não envolvem comunicação

A parte mais problemática da fundamentação da declaração da inconstitucionalidade diz respeito aos dados de tráfego, que não envolvem comunicação intersubjetiva, na medida em que, aqui, o Tribunal Constitucional, apesar de ter declarado a inconstitucionalidade deste segmento da norma, 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, todos da CRP, na sua fundamentação acaba por potenciar uma futura intervenção legislativa suscetível de permitir ingerências excessivas nestes dados, os quais, como vimos, podem ser mais reveladores da personalidade e do mundo privado e existencial de cada pessoa do que as comunicações intersubjetivas.

a) A indeterminação do conceito de perigo

O Tribunal Constitucional, para fundamentar a inconstitucionalidade do segmento do artigo 4.º que se reporta ao acesso a dados de tráfego que não envolvem um ato de comunicação intersubjetiva, refere-se ao carácter indeterminado dos pressupostos da intervenção dos serviços de informação, e propõe, como critério aferidor do fundamento da ingerência, à semelhança das medidas policiais restritivas de direitos fundamentais (artigo 272.º, n.º 2, da CRP), a necessidade, a exigibilidade e a proporcionalidade da medida, nada mais afirmando afinal do que o próprio regime jurídico em que se situa o artigo 4.º já afirmava no artigo 6.º, n.º 1, da Lei Orgânica n.º 4/2017. Adita apenas, como critério limitador, a noção de "perigo concreto" para determinados bens jurídicos, noção que também se reveste de natureza vaga e indeterminada. Continua, assim, a ser

desrespeitado, na minha opinião, o princípio da determinabilidade das restrições a direitos fundamentais.

Entendo, diferentemente, que a aplicação do princípio da proporcionalidade aos poderes do SIS e do SIED de acesso a dados de tráfego, no domínio da prevenção criminal, deve obedecer – precisamente porque estes serviços de informações não são órgãos policiais – a requisitos mais estritos do que os plasmados no artigo 272.º, n.º 2, da CRP.

Nesta sede, entendo que o Tribunal Constitucional, para aferir da constitucionalidade à luz 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, todos da CRP, devia ter aplicado um critério de proporcionalidade que passasse não só por reservar o acesso a estes dados para situações de perigo, comprovado em termos fácticos e normativos, para bens jurídicos essenciais à sobrevivência do Estado de Direito, como propôs o presente Acórdão, como também exigir que esse perigo esteja próximo ou iminente, e que exista uma relação de causalidade entre os factos indiciadores das suspeitas de terrorismo ou espionagem e um dano altamente provável para esses bens jurídicos.

Por mais importante que seja a luta contra o terrorismo, ela não se justifica a si mesma, não devendo a lei bastar-se com um conceito simples e amplo de perigo para a legitimar – o conceito de perigo, mesmo factualmente fundamentado, será sempre um conceito vago e impregnado de subjetividade, que, em virtude da força apelativa da própria palavra, será suscetível de permitir justificar qualquer intervenção – devendo a lei exigir um perigo qualificado para bens jurídicos fundamentais, reportados à dignidade da pessoa humana, como a vida, a integridade física e a liberdade, e não um perigo para bens jurídicos coletivos, impossíveis de definir com precisão, como a segurança interna ou externa, o segredo ou a autoridade do Estado ou o interesse público. Estes bens jurídicos têm um conteúdo elástico e altamente manipulável, como ilustra a jurisprudência dos tribunais comuns num caso em que, para justificar o acesso aos metadados do telemóvel de um jornalista pelo então diretor e outros funcionários do SIS,

devassando designadamente as suas fontes, estes invocaram a defesa do segredo de Estado e da segurança interna e externa, tendo vindo a ser condenados por crime de acesso ilegítimo agravado, p. e p. pelo artigo 6.º, n.ºs 1 e 4, al. a), da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime)[2].

A ligação ou a semelhança de objetivos entre atividade de informações, atividade policial e investigação criminal não isenta a primeira de um controlo mais rigoroso (e de pressupostos legais mais determinados), desde logo porque o trabalho de recolha e tratamento de informações pessoais não é transparente, nem controlável pelos cidadãos, enquanto a atividade policial é, em regra, visível e mais facilmente controlável pelos destinatários e pela sociedade.

Recorde-se que, como afirma a lei, a atividade dos serviços de informação reduz-se ao seu estrito âmbito, não podendo confundir-se com a atividade própria de outros organismos, como a atividade dos tribunais ou a atividade policial. É de salientar também a importância da proteção dos direitos, liberdades e garantias dos cidadãos, como limite à atividade dos serviços de informação, especialmente frente à utilização de dados informatizados.

Particularmente problemática, em sede da aplicação do princípio da proporcionalidade, nos termos em que a ela procedeu o Acórdão agora comentado, é a parte dos fundamentos em que reporta a intervenção de acesso a dados pessoais do SIS e do SIED «a uma "fase prévia" à própria prevenção criminal», ou a uma prevenção criminal «positiva» ou «pró-ativa», conceitos que abrem ainda mais a porta ao risco de violação dos direitos dos cidadãos do que a própria lei em apreciação, que se reporta à prevenção criminal. Este conceito, interpretado de acordo com a Constituição, não pode deixar de assumir um sentido técnico-jurídico determinado e restrito e não o sentido amplo que lhe é atribuído pelo Acórdão, que pode vir, assim, a permitir, no futuro, uma jurisprudência legitimadora da constitucionalidade de intervenções reportadas a essa fase

[2] Cf. acórdão do Tribunal da Relação de Lisboa, de 07-03-2018, proc. n.º 5481/11.4TDLSB.L1-3.

«prévia», que necessariamente alarga, como aliás reconhece o Tribunal Constitucional, os riscos de erro de prognose.

b) A exclusão de um dever de notificação aos visados

Dada a insuficiência do conceito de perigo, ainda que com a «identificação normativa da situação fáctica» que está na sua origem, como defende o Tribunal Constitucional, a única forma de evitar (ou de reduzir substancialmente) os riscos de excesso de intervenção é **a exigência legal de notificação** aos visados, para que estes possam ter conhecimento de que os seus dados foram recolhidos pelos serviços secretos e solicitar a sua destruição, bem como pedir indemnização por perdas e danos, em caso de intervenções ilícitas. Na verdade, seria essencial que o Tribunal Constitucional, para substituir o parâmetro do artigo 34.º, n.º 4, pelo do artigo 35.º, n.ºs 1 e 4, fizesse esta exigência ao legislador como requisito de constitucionalidade de qualquer regime jurídico que a este propósito venha a ser aprovado no futuro. A jurisprudência do TEDH, que deve ser usada como critério interpretativo das normas constitucionais, assim o tem entendido. No caso *Roman Zakharov v. Russia* (decisão de 04, de dezembro de 2015, queixa n.º 47143/06), o TEDH exigiu, pela primeira vez, como medida de salvaguarda contra o risco de arbitrariedade, a previsão, pela legislação nacional, de providências para *a supervisão das medidas secretas de vigilância, mecanismos de notificação das pessoas visadas e vias de recurso.* No mesmo sentido, se orientou o TJUE no Acórdão *Tele2* (n.º 121), «*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. Com efeito, essa informação é, de facto, necessária para permitir que essas pessoas exerçam, nomeadamente, o direito ao recurso, explicitamente previsto no artigo 15.º, n.º 2, da Diretiva 2002/58, lido em conjugação com o artigo 22.º da Diretiva 95/46, em caso de violação dos seus direitos*».

Para que os meios de impugnação contra o acesso a dados sejam efetivos, afirmam o TEDH e o TJUE que a lei tem de prever meios de notificação das medidas de vigilância aos visados, pelo menos num momento posterior à cessação da intervenção, de forma a possibilitar que estes possam usar os recursos previstos para questionar a legalidade das medidas, ou, em alternativa, que qualquer pessoa que suspeite ter sido monitorizada possa recorrer às entidades competentes e aos tribunais para saber se os seus dados foram apreendidos e solicitar a sua destruição (TEDH, Acórdão *Big Brother Watch*, n.º 310). Tendo em conta que o fenómeno da prevenção criminal se basta com uma suspeita, que pode ser vaga e baseada numa convicção subjetiva, tem de se reconhecer que os poderes que a lei confere ao Estado no domínio da prevenção do terrorismo e da espionagem podem atingir 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.

O presente Acórdão, apesar de reconhecer este risco, criado pela falta de densificação do regime jurídico em apreciação, detetando o problema, acaba por se conformar com ele. Isto é, preocupa-se, sobretudo, com as exigências de *determinabilidade* quanto à definição dos pressupostos das medidas de prevenção ou de ingerência, mas pouco com as exigências de *impugnabilidade* pelo indivíduo visado e de *responsabilização do Estado* pelos erros. Com efeito, a necessidade de estipulação legislativa, como requisito de conformidade à Constituição, de um *dever de notificação aos indivíduos, cujos dados são objeto de acesso*, constitui um elemento essencial, a meu ver, para analisar se o regime jurídico agora questionado, ou qualquer outro que venha a ser previsto numa eventual lei destinada a substituir as normas agora declaradas inconstitucionais, respeita, ou não, o princípio da proporcionalidade (artigo 18.º, n.º 2, da CRP).

Com efeito, de nada adianta a previsão legal de meios de reação ou recursos, se os cidadãos não tiverem conhecimento de que os serviços de informação tiveram acesso aos seus dados pessoais. Para que a norma que prevê o acesso a dados de

tráfego, que não envolvem comunicação intersubjetiva, pudesse passar no teste da proporcionalidade, seria, então, necessária a consagração legislativa de um dever de informação das pessoas visadas pela operação, a fim de que os cidadãos possam acionar meios de impugnação e requerer a destruição dos seus dados, quando eles sejam inúteis para a investigação em causa, à semelhança do afirmado pelo TJUE no caso *Tele 2* (cf. n.º 121) e no Acórdão *Schrems*, C-362/14, EU:C:2015:650, n.º 95. Para o efeito, devem, assim, ser criados pela lei meios específicos de reação e de responsabilização do Estado em caso de acesso ilícito a dados de tráfego, distintos dos meios gerais de impugnação, e caraterizados por uma maior simplicidade, celeridade e acessibilidade ao cidadão comum, bem como meios de notificação aos visados, pelo menos nos casos em que a operação de acesso aos dados conservados abranja pessoas que não participaram nos atos ou planos de terrorismo, ou nos casos em que afinal se verificou que a suspeita de planeamento de terrorismo ou de espionagem não tinha fundamento.

c) A complexidade e a incerteza em torno do conceito (e do fenómeno) do terrorismo

As consequências, para os direitos dos cidadãos, da indeterminação dos pressupostos da intervenção e da difícil (ou quase impossível) impugnabilidade das intervenções ilícitas agravam-se pela margem de erro normalmente apresentada pelas reações ao terrorismo e pela incerteza quanto à extensão do fenómeno na comunidade internacional, que se reveste de flexibilidade e generalidade. Apesar de a lei em apreciação remeter para o conceito de terrorismo, tal como tipificado em legislação penal extravagante (Lei n.º 52/2003, de 22 agosto, com as subsequentes alterações, designada por Lei de combate ao terrorismo), as normas criminalizadoras abrangem uma ampla gama de comportamentos, verificando-se, também, uma incerteza na definição dos elementos típicos (objetivos e subjetivos) do conceito, tal como ilustrado pela própria jurisprudência penal dos tribunais

comuns[3]. Para além deste risco quanto à extensão do conceito, existe também um risco de discriminação inerente à identificação de quem são os sujeitos suspeitos e abrangidos por uma operação de prevenção criminal.

O direito penal e processual penal antiterrorista, se bem que satisfazendo uma legítima necessidade coletiva de segurança dos Povos, não se deve transformar num "direito penal do inimigo", que conduz à estigmatização de determinados indivíduos e à perda de privacidade e de liberdade dos cidadãos em geral. O papel dos Tribunais Constitucionais europeus é decisivo, para evitar "derivas securitárias" e manter um juízo crítico permanente na procura do justo equilíbrio entre segurança e direitos fundamentais ou, numa outra perspetiva, entre sistema democrático e luta antiterrorista.

Os juízos de ponderação, ao abrigo do princípio da proporcionalidade, não devem limitar-se a ponderar valores ou direitos em conflito, mas antes devem fazê-lo num quadro mais amplo, presidido pela preocupação, como tem sido orientação do TEDH, de que as intervenções dos serviços de informações, no acesso a dados pessoais, não assumam um caráter de tal modo geral e excessivo, que venha a gerar, nos cidadãos comuns, uma auto-restrição à sua liberdade de movimentos e de expressão, que, enquanto fenómeno coletivo, acabe por constituir uma realidade mais limitadora da democracia do que o perigo representado pelo terrorismo, que pode ser mais alimentado pelo medo do que pela realidade.

5. A norma do artigo 3.º e a sua divisão em dois segmentos para o efeito de um juízo duplo de constitucionalidade/inconstitucionalidade

O Tribunal Constitucional procedeu também a uma divisão desta norma em dois segmentos, para o efeito de proferir um juízo de inconstitucionalidade (parcial) apenas em relação a um deles, que se reporta ao acesso dos oficiais de informações do SIS e do SIED a dados de base e de localização de equipamento

[3] Cf. acórdãos do Supremo Tribunal de Justiça, de 25-03-2010, proc. n.º 76/10.2YRLSB.S1 e do Tribunal da Relação de Lisboa, de 26-09-2018 e de 10-10-2018, ambos do proc. n.º 257/18.0GCMTJ-F.L1-3; e de 27-11-2018, proc. n.º 78/15.2JBLSB.L1-5.

para efeitos de produção de informações necessárias à salvaguarda da *defesa nacional* e da *segurança interna*. Mas entendeu o Tribunal que o segmento da norma que permite o acesso a estes dados para a prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada já será, pelo contrário, conforme à Constituição. Esta posição valorizou a circunstância destes últimos conceitos serem, na perspetiva da maioria que votou pela constitucionalidade deste segmento da norma, conceitos tipificados na lei ou determináveis, diferentemente dos restantes bens jurídicos – defesa nacional e segurança interna – que seriam conceitos indeterminados, ou conceitos *«sem a mediação de critérios de determinabilidade (...) através de "elementos tipificadores limitadores da ação", na expressão do Tribunal Constitucional alemão (cf. BVerfG, 110, pp. 33, 57 e 60)».*

Considero, contudo, que a fundamentação relevante para a declaração de inconstitucionalidade do artigo 4.º da Lei Orgânica n.º 4/2017, no segmento que se refere aos dados de tráfego que não envolvem comunicação intersubjetiva, é extensível à fundamentação da inconstitucionalidade de todo o artigo 3.º, independentemente do grau de determinação/indeterminação dos bens jurídicos que justificam o acesso a estes dados. Na verdade, a maior ou menor tipificação dos bens jurídicos torna-se irrelevante num contexto legislativo que, como demonstram os fundamentos para a inconstitucionalidade do artigo 4.º, padece de escassa densificação da moldura legislativa e de vaguidade da definição do alvo da intervenção (cf. artigo 6.º, n.º 1, da Lei Orgânica n.º 4/2017), bem como dificulta aos cidadãos a reação contra intervenções ilícitas ou riscos de abuso. É difícil de compreender, em termos substanciais e lógicos, como pode, em simultâneo, o caráter indeterminado dos pressupostos da intervenção fundamentar a inconstitucionalidade do artigo 4.º à luz dos artigos e 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 CRP, e não constituir um obstáculo à constitucionalidade do artigo 3.º, sobretudo em relação aos dados de localização, cujo acesso pelos serviços de informação pode também revelar-se altamente

intrusivo na privacidade e da liberdade individual. Tal disparidade na avaliação dos critérios de proporcionalidade explica-se, contudo, pela diferente composição de maiorias de geometria variável, em relação a cada uma das normas, o que dificulta a unidade lógica do texto do acórdão.

A distinção entre dados de base e de localização, que não dão suporte a uma comunicação, por um lado, e dados de tráfego, que não envolvem comunicação intersubjetiva, por outro, para o efeito da defesa feita pelo acórdão de um diferente grau de intrusão na liberdade e na privacidade destas duas categorias de dados, não se afigura suficientemente inequívoca e relevante para fixar uma linha entre a constitucionalidade e a inconstitucionalidade, como entendeu a posição que fez vencimento no Acórdão. É que também as informações sobre a localização de um indivíduo, mesmo desligadas de um ato de comunicação, são suscetíveis de revelar aspetos da sua liberdade – liberdade religiosa, por exemplo – e da sua privacidade, tão pessoais e secretas, como as reveladas pelos dados de tráfego que não envolvam comunicação interpessoal, como o caso já referido da navegação na internet.

Defendo, portanto, a inconstitucionalidade de toda a norma do artigo 3.º, por violação dos direitos à privacidade e à autodeterminação informativa (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 CRP, pelos motivos invocados para fundamentar a inconstitucionalidade do artigo 4.º, na parte relativa ao acesso a dados de tráfego que não envolvem comunicação intersubjetiva, conforme expostos no ponto 4. deste texto.

6. A relação entre o direito constitucional e o direito da União Europeia

A inclusão, no corpo do acórdão, de um ponto sobre a relação entre o direito nacional e o direito comunitário, revela-se desnecessária, de um ponto de vista jurídico-constitucional e prático-judiciário, e discutível de um ponto de vista teórico e dogmático.

Ao Tribunal Constitucional compete apenas aplicar os parâmetros específicos de constitucionalidade constantes das normas do artigo 34.º, n.º4 (inviolabilidade das telecomunicações e demais meios de comunicação), 35.º, n.º 1 (direito à autodeterminação informativa) e artigo 26.º, n.º 1 (reserva da intimidade da vida privada e familiar), da Constituição da República Portuguesa. No presente caso, a questão suscitada reporta-se à constitucionalidade de normas, por referência ao direito constitucional nacional, que contém um parâmetro específico e mais protetor dos direitos fundamentais dos cidadãos do que o do direito europeu e comunitário, pois exige, para fundamentar a restrição da privacidade das comunicações, que estejamos em matéria de processo penal (artigo 34.º, n.º 4, da CRP), ou seja, as restrições ao segredo das telecomunicações não podem ser mero instrumento de investigação extraprocessual e a pendência de processo-crime é uma exigência constitucional para a sua validade.

A aplicação de outro parâmetro pelo Tribunal Constitucional, *in casu,* as normas constitucionais que tutelam o direito à autodeterminação informativa (artigo 35.º, n.ºs 1 e 4 da CRP) e a privacidade (artigo 26.º, n.º 1, da CRP), em conjugação com o princípio da proporcionalidade (artigo 18.º, n.º 2, da CRP), potencia a consideração, pelo juiz constitucional, da jurisprudência do TJUE e do TEDH, não como o resultado da observância do princípio do primado do Direito Comunitário ou como normas paramétricas, mas na forma de um diálogo interjurisdicional, ao abrigo da cláusula aberta consagrada no artigo 16.º, n.º 1, e do artigo 8.º, ambos da CRP, na medida em que aquela jurisprudência densifique ou enriqueça o conteúdo e o alcance dos direitos fundamentais consagrados na Constituição ou reconheça novos direitos ou novas dimensões de direitos já consagrados. Nestes termos, os juízos de ponderação, de acordo com o princípio da proporcionalidade, à luz do artigo 18.º, n.º 2, da CRP, fazem-se em moldes metodológicos semelhantes aos previstos na jurisprudência do TJUE (artigo 52.º, n.º 1, da CDFUE), e do TEDH (artigo 8.º da CEDH). Contudo, tendo o Tribunal Constitucional admitido o contributo desta jurisprudência, não retirou dela, como

vimos, um dos critérios mais importantes para a defesa dos cidadãos: o dever de notificação aos cidadãos visados pelas medidas de ingerência nos seus dados pessoais.

Mas, é importante clarificar, que este contributo do direito europeu para a jurisprudência constitucional, nada tem a ver com qualquer primado do direito da União Europeia, como parece pretender o Tribunal Constitucional nalguns excertos da sua fundamentação.

A resposta à questão da relação entre o direito nacional e o direito comunitário (cf. *ponto 6, alínea b) dos fundamentos do acórdão*) não é necessária, nem sequer relevante para a apreciação da constitucionalidade das normas impugnadas, consistindo antes num mero excurso teórico, que apesar de ser apresentado no Acórdão como uma posição única e consensual, não o é. Esta questão é analisada de diferentes formas e conhece diversas correntes doutrinais[4]. Nesta sequência, discordo, quer da sistematização do acórdão, que descreve nos seus fundamentos as normas de direito da União Europeia em primeiro lugar, em relação às normas constitucionais paramétricas, quer da invocação do princípio do primado do direito comunitário quando está em causa matéria de direitos, liberdades e garantias. Por respeito à tradição constitucional dos Estados membros, as normas constitucionais que consagram direitos fundamentais devem prevalecer sobre o Direito da União quando consagram uma tutela mais ampla.

6.1. A tutela multinível dos direitos fundamentais

Nos termos do artigo 4.º, n.º 2, do TUE, a União Europeia respeita a identidade nacional e as funções essenciais do Estados, nomeadamente as que se destinam a garantir a integridade territorial, a manter a ordem pública e a salvaguardar a segurança nacional. A segurança nacional é matéria da exclusiva responsabilidade de cada Estado-Membro, assim afastando esta função essencial

[4] Cf. JORGE MIRANDA, "Anotação ao artigo 8.º da Constituição", in *Constituição Portuguesa Anotada*, Volume I, Universidade Católica Editora, anotação XXI, pp. 172-177.

do Estado das atribuições partilhadas da União Europeia, subtraindo-a do âmbito de aplicação do direito derivado da União.

Contudo, as medidas adotadas pelos Estados para proteger a segurança nacional, caso impliquem restrições a direitos fundamentais, devem obedecer a parâmetros mínimos de salvaguarda destes direitos, nomeadamente à privacidade e ao segredo das comunicações, não podendo os Estados descer o nível de proteção garantido pelo direito comunitário. Daí a necessidade de se ter em conta o nível de proteção da jurisprudência do TJUE, não como observância do princípio do primado do direito da União Europeia, mas numa perspetiva de diálogo interjurisdicional ou de cooperação, desprovido de qualquer relação hierarquizada entre tribunais. Está em causa a União como «União de direitos» e a determinação de qual é a "melhor tutela europeia", processo em que o direito constitucional nacional tem um papel decisivo, pois fornece, no artigo 34.º, n.º 4, da CRP, uma tutela mais ampla ao segredo das comunicações do que a generalidade das Constituições europeias e do que a Carta dos Direitos Fundamentais da União Europeia. O Preâmbulo da Carta dos Direitos Fundamentais da União Europeia, atribuindo peso às tradições constitucionais comuns dos Estados-membros e à tutela multinível dos direitos fundamentais, reafirma «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».

No espaço europeu, coexistem diversas formas de tutela dos direitos fundamentais, que lhes conferem uma proteção plural e multinível: o nível de proteção de direitos fundamentais da UE, o nível de proteção do direito internacional e das convenções ratificadas, que inclui a CEDH, tal como

interpretada pelo TEDH, e o nível de proteção das constituições nacionais dos Estados-Membros.

No contexto de conflitos entre o alcance ou a formulação dos direitos fundamentais consagrados nas diferentes ordens jurídicas, as relações entre tribunais não podem ser analisadas através de um qualquer conceito de hierarquia. A relação entre o Direito comunitário e os direitos nacionais constrói-se com base nos princípios da atribuição de competências e da colaboração ou complementaridade de ordenamentos autónomos e distintos. Em particular, a relação entre a ordem constitucional europeia e a ordem constitucional nacional consiste numa relação "interativa", mas não hierarquizada, em que o problema do eventual conflito de normas se reconduz a uma questão de concordância prática.

A problemática do tratamento de dados relativos às comunicações é matéria objeto de regulação por parte do Direito da União Europeia e do TEDH. No caso vertente, tendo em conta a convergência axiológica entre as disposições da Carta e as normas constitucionais, em princípio, não sucederá, no que diz respeito ao direito à reserva da vida privada, ao direito à proteção de dados pessoais e à liberdade de expressão, qualquer incompatibilidade ou conflito. Faz sentido, portanto, tomar-se em consideração a proteção que o direito à privacidade e os dados pessoais tem conhecido na jurisprudência do TJUE e na jurisprudência do TEDH (considerada um *standard* mínimo de proteção pelo Direito da União), numa perspetiva de diálogo interconstitucional, sem prejuízo de o Tribunal Constitucional confrontar as normas questionadas apenas com o seu específico parâmetro constante da Constituição. É que a Constituição da República Portuguesa, pela amplitude do seu catálogo de direitos, e por ter, em matéria de segredo das comunicações, a posição mais amiga dos direitos fundamentais, representa uma referência neste diálogo recíproco, o que, desde logo, torna questionável a opção sistemática do Acórdão, na arrumação das matérias, e que confere um lugar de primazia ao Direito da União Europeia, em detrimento do lugar que concede às normas constitucionais paramétricas como normas

fundamentais e supremas da ordem jurídica nacional. Tanto mais que o princípio do primado do Direito Comunitário sobre o direito interno dos Estados-membros não tem um valor absoluto, estando concebido fundamentalmente como uma norma de salvaguarda de competências. Por isso, tem entendido a doutrina constitucionalista que o primado não constitui um princípio constitucional ou uma ordem de valores superior às constituições dos Estados-membros[5]. Para além disto, o primado do direito da UE está condicionado pela *reserva constitucional de respeito pelos princípios fundamentais do Estado de direito democrático* (artigo 8.º, n.º 4, *in fine,* da CRP), também designada por «reserva de ordem pública constitucional» ou «núcleo essencial» da Constituição, em que se inclui o princípio do respeito, garantia e efetivação dos direitos e liberdades fundamentais.

Note-se que é a própria União Europeia que reconhece expressamente aos Estados membros autonomia para aplicarem um nível de proteção mais elevado do direito à privacidade quando em conflito com a proteção da segurança pública e a prevenção, investigação, deteção ou repressão de infrações penais (cf. artigo 1.º, n.º 3 da Diretiva (EU)2016/680 do Parlamento Europeu e do Conselho, segundo o qual «*A presente diretiva não obsta a que os Estados-Membros prevejam garantias mais elevadas do que as nela estabelecidas para a proteção dos direitos e liberdades do titular dos dados no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes*»).

A questão do primado do direito da União Europeia, referida no presente Acórdão, não é, pois, pertinente no presente contexto, mas meramente semântica, virtual ou teórica, dado que os princípios gerais de direito da UE e o catálogo de direitos da Carta de Direitos Fundamentais da UE correspondem às tradições constitucionais comuns dos Estados-membros, e que a estes princípios, direitos e tradições está submetido o próprio direito originário da UE (artigo 6.º, n.º 3, do TUE). Neste sentido, nos casos de interconstitucionalidade ou de

[5] Cf. GOMES CANOTILHO/VÍTAL MOREIRA, *Constituição da República Portuguesa Anotada*, Vol. I, anotação XVI ao artigo 8.º, p. 266.

constitucionalismo de vários níveis, cabe ao Tribunal Constitucional assumir o papel de guardião dos princípios do Estado de direito democrático e dos direitos fundamentais dos cidadãos.

Os conceitos de "cooperação multinível" e de "aprendizagem mútua" continuam, assim, em matéria de direitos, liberdades e garantias, a ser os mais adequados para, numa lógica baseada na horizontalidade, levar a cabo a importante missão de tutela de direitos e liberdades fundamentais[6]. Neste âmbito, a cooperação entre o Tribunal de Justiça e os Tribunais Constitucionais dos países da UE não opera apenas em sentido único, mas nos «dois sentidos», exprimindo-se numa «real influência recíproca»[7].

No domínio de aplicação do princípio da proporcionalidade para avaliar a adequação e a necessidade das restrições aos direitos fundamentais, o TJUE, ao efetuar juízos de ponderação reconhece também a escala de valores do Estado-membro para proteger direitos ou interesses relevantes. Reciprocamente, os Tribunais Constitucionais têm também em conta a jurisprudência comunitária e do TEDH, quando procedem aos juízos de ponderação para avaliar da constitucionalidade de leis nacionais restritivas de direitos fundamentais.

O princípio do primado do direito da União parece, assim, ceder, a favor da aplicação dos direitos de outros ordenamentos jurídicos, inclusivamente das ordens jurídico-constitucionais nacionais, sempre que estas se mostrem mais protetoras da pessoa humana e dos seus direitos fundamentais. A proteção dos direitos fundamentais tem operado de baixo para cima, ou seja, dos Estados-Membros para a União, pelo que a Carta dos Direitos Fundamentais da União Europeia não conseguirá inverter esta situação, continuando as tradições

[6] Cf. CATARINA SANTOS BOTELHO, «O Tribunal de Estrasburgo, o Tribunal de Justiça da União Europeia e os Tribunais Constitucionais nacionais: perigo de um "Triângulo das Bermudas"? – A Complexa Interacção Multinível entre as Instâncias Jurisdicionais de Protecção dos Direitos Fundamentais», in *Estudos em homenagem ao Prof. Doutor Alberto Xavier,* Almedina, 2013, p. 424

[7] Cf. CARDOSO DA COSTA, «O Tribunal Constitucional português e o Tribunal de Justiça das Comunidades Europeias», in *Ab Uno Ad Omnes,* Coimbra Editora, p. 1380.

constitucionais nacionais, marcadas por contextos sociopolíticos particulares, a desempenhar um papel preponderante [8].

O princípio do primado do direito da União, estabelecido pelo TJUE, é incindível de uma ideia de "contrapartida" exigida pelos tribunais nacionais, que «(...) consiste na garantia da efetiva sujeição das normas da União destinadas a prevalecer nas ordens jurídicas dos Estados-Membros a parâmetros de validade essencialmente coincidentes com os que integram o "núcleo duro" das constituições nacionais, a começar pelos direitos fundamentais»[9].

Costuma ser apontado como um afastamento do princípio do nível de proteção mais elevado, consagrado no artigo 53.º da Carta dos Direitos Fundamentais da União Europeia, a orientação definida no Acórdão do TJUE, designado como Acórdão *Melloni* (26/02/2013, proc. C-399/11), que fez prevalecer sobre o nível de proteção do Estado espanhol o padrão de proteção da União Europeia, que não era o mais elevado, no que diz respeito à faculdade de recusar a execução de um mandado de detenção europeu em caso de condenação na ausência do arguido.

O TJUE aplicou o padrão de proteção da União, por entender ser o mais adequado, nas circunstâncias do caso concreto, a prosseguir o objetivo da cooperação judiciária em matéria penal e o princípio do reconhecimento mútuo das decisões proferidas na ausência do arguido, mas não procedeu a um afastamento, definitivo e válido para todos os casos, do princípio do nível de proteção mais elevado. O TJUE continua a aceitar a subsistência e a coexistência de diversas formas de tutela dos direitos fundamentais, e a admitir que as autoridades e os órgãos jurisdicionais nacionais apliquem os padrões nacionais de proteção dos direitos fundamentais, desde que essa aplicação não comprometa o

[8] Cf. PEDRO MIGUEL ALVES RIBEIRO CORREIA e INÊS OLIVEIRA ANDRADE DE JESUS, «O princípio do nível de proteção mais elevado: Análise do artigo 53 da carta dos direitos fundamentais da união europeia à luz do acórdão Melloni», *Estudios Constitucionales*, Ano 12, n.º 2, 2014, p. 278.

[9] Cf. DIOGO FREITAS DO AMARAL/NUNO PIÇARRA, «O Tratado de Lisboa e o princípio do primado do direito da União Europeia: uma "evolução na continuidade"», *Revista de Direito Público,* Ano I, N.º 1, 2009, p. 13.

nível de proteção previsto na Carta, conforme interpretado pelo TJUE, nem o primado, a unidade e a efetividade do direito da União (§60 do Acórdão *Melloni*), remetendo os tribunais nacionais para a determinação do nível mais adequado de proteção, que não pode deixar de ser, na generalidade dos casos, o nível mais elevado ou mais intenso de proteção.

De resto, não se pode considerar existir qualquer incompatibilidade entre este princípio da tutela mais favorável e o princípio do primado, pois, numa interpretação sistemática coerente, deverá apenas considerar-se que é o próprio direito da União Europeia que admite uma exceção à sua aplicação preferencial, com fundamento nos objetivos da União, que incluem o reforço dos direitos dos cidadãos[10]. Desde logo, a Constituição portuguesa impõe limites à aplicabilidade interna do Direito da União: os princípios do Estado de Direito democrático, em que se inclui o sistema constitucional de proteção de direitos fundamentais. Neste quadro, conferir à norma comunitária um valor supraconstitucional seria contraditório, de forma insuperável, com a própria ideia de Constituição. O princípio do primado do direito comunitário tem uma origem jurisprudencial, e, sendo elaborado por juízes sem legitimidade democrática, não espelha, por isso, na sua versão de supremacia absoluta sobre as ordens jurídicas nacionais, nomeadamente, sobre as normas constitucionais, a vontade comum dos Parlamentos nacionais.

7. Conclusões

No Acórdão n.º 464/2019, o Tribunal Constitucional adotou uma técnica de divisão, em segmentos, das normas constitucionais apreciadas, que torna mais complexa e carente de coerência e de unidade a sua fundamentação.

O artigo 3.º, sobre o acesso do SIS e do SIED aos dados de base e de localização, quando não deem suporte a uma comunicação, foi dividido em dois

[10] Cf. MARIANA CANOTILHO, *O princípio do nível mais elevado de proteção em matéria de direitos fundamentais*, Coimbra, 2008, p. 177.

segmentos consoante os objetivos ou finalidades que a norma visa prosseguir, tendo o Tribunal Constitucional proferido uma declaração de inconstitucionalidade incidente apenas sobre a parte da norma que indica como finalidades da ingerência a proteção dos bens jurídicos da segurança interna e da defesa nacional, por ter considerado que o grau de indeterminação destes conceitos não é compatível com as exigências constitucionais das leis restritivas de direitos fundamentais, nos termos do artigo 18.º, n.º 2, da CRP.

Entendo, contudo, que a maior ou menor tipificação dos bens jurídicos torna-se irrelevante num contexto legislativo que padece de escassa densificação da moldura legislativa, de vaguidade na definição do alvo da intervenção (cf. artigo 6.º, n.º 1, da Lei Orgânica n.º 4/2017), e que dificulta aos cidadãos a reação contra intervenções ilícitas ou riscos de abuso, pelo facto de estes não serem notificados *a posteriori* do acesso dos serviços de informação a esses dados. Pelo que, considero toda a norma inconstitucional, por violação dos artigos 26.º, n.º 1, 35.º, n.ºs 1 e 4, em conjugação, com o artigo 18.º, n.º 2, da CRP.

O artigo 4.º da Lei n.º 4/2017, apesar de ter sido declarado inconstitucional na sua totalidade, foi segmentado em duas partes, consoante os dados de tráfego envolvam ou não comunicação intersubjetiva, excluindo o Acórdão os últimos do conceito de comunicação constitucionalmente relevante para o efeito da proteção mais ampla do artigo 34.º, n.º 4, da CRP.

Na verdade, esta opção do Tribunal Constitucional é questionável. Sabe-se que os dados de tráfego, que resultam da utilização da internet desligados de uma comunicação intersubjetiva, podem traduzir uma comunicação ainda mais íntima e secreta do que aquela que ocorre entre dois sujeitos, consistindo numa forma de comunicação da pessoa consigo mesma, com as suas questões existenciais, pensamentos, dúvidas, sonhos, medos ou angústias, revelando informações sobre os seus hábitos de vida, valores, crenças, gostos, saúde, dos quais se podem deduzir características pessoais do utilizador e traços fundamentais da sua personalidade que até nunca são reveladas na comunicação intersubjetiva.

Deixando o parâmetro de apreciação da constitucionalidade de ser o artigo 34.º, n.º 4, da CRP, o Tribunal, entendendo que estão em causa os direitos à reserva da vida privada (artigo 26.º, n.º 1, da CRP) e à autodeterminação informativa (artigos 35.º, n.ºs 1 e 4, da CRP), recorreu ao princípio da proporcionalidade para apreciar a constitucionalidade deste segmento da norma do artigo 4.º da Lei n.º 4/2017. Esta diferenciação de regimes assume importantes efeitos práticos. Com efeito, estando os dados que envolvem apenas comunicação em massa, ou dados de navegação na internet, excluídos do conceito de comunicação constitucionalmente relevante para o efeito da proteção mais intensa do artigo 34.º, n.º 4, da CRP, podem ser invadidos pelos serviços de informação, sem estar pendente um processo crime contra os indivíduos abrangidos pela intromissão. Nesta matéria, os fundamentos invocados pelo Acórdão n.º 464/2019, para justificar a inconstitucionalidade, assumem o significado de orientações do Tribunal Constitucional ao legislador para que uma futura lei sobre o acesso a metadados seja conforme à Constituição. Ora, é minha firme convicção que estas orientações ou critérios de conformidade constitucional, fixados pelo Tribunal Constitucional, são insuficientes para defender os direitos fundamentais dos cidadãos em face da ingerência dos serviços de informação nos seus dados de tráfego, e, portanto, na sua privacidade, liberdade e autodeterminação informativa, por três motivos: a indeterminação do conceito de perigo; a não exigência de um dever de notificação *a posteriori* aos cidadãos visados pela ingerência; a incerteza em relação à extensão do conceito de terrorismo.

A luta contra o terrorismo, se bem que satisfazendo uma legítima necessidade coletiva de segurança dos Povos, não se deve transformar num "direito penal do inimigo", que conduz à estigmatização de determinados indivíduos e à perda de privacidade e de liberdade dos cidadãos em geral.