

Vossa referência:

Nossa Referência: Of.º n.º 10655 de 02/06/2017

Proc. n.º 115/2016 - L. 115

ASSUNTO: Envio de parecer sobre o Projeto de Lei nº 480/XIII/2ª - Proposta de Lei n.º 78/XIII

Ex.mo Senhor

Presidente da Comissão de Assuntos Constitucionais, Direitos e Liberdades e Garantias

Prof. Dr. Bacelar Vasconcelos

Por determinação superior, e tendo presente o teor do ofício nº 4566/2017, de 8 de março, do Senhor Secretário da Procuradoria-Geral da República, tenho a honra de remeter a Vossa Excelência os pareceres elaborados pelo Gabinete da Senhora Conselheira Procuradora-Geral da República sobre o Projeto de Lei nº 480/XIII/2ª - "Acesso a dados de tráfego, de localização ou outros dados conexos das comunicações por funcionários e agentes dos serviços de informações da República Portuguesa" – e sobre a Proposta de Lei n.º 79/XIII – "Acesso a dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas pelo Sistema de Informações da República", os quais mereceram a sua total concordância.

Com os melhores cumprimentos,

CACDLG

SHE STALLS

CACDLG

Helena Gonçalves

A Chefe de Gabinete

876944\_1 /sv



#### PARECER

### Projeto de Lei nº 480/XIII-2ª

Acesso a dados de tráfego, de localização ou outros dados conexos das comunicações por funcionários e agentes dos serviços de informações da República portuguesa

A Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República remeteu ao Conselho Superior do Ministério Público, com solicitação de parecer, o Projeto de Lei nº 480/XIII-2ª, pelo qual se pretende introduzir alterações à Lei 30/84, de 5/9 – Lei Quadro do Sistema de Informações da República Portuguesa –, e à Lei 62/2013, de 26/8 – Lei de Organização do Sistema Judiciário -, de forma a permitir, mediante autorização judicial prévia, o acesso a informações bancárias, informações fiscais e a dados de tráfego, de localização ou outros dados conexos das comunicações por funcionários e agentes dos serviços de informações da República portuguesa.

Em satisfação do solicitado procede-se a análise do identificado Projeto de Lei.

### I- Objeto

**1.** Com vista a estabelecer a competência e o procedimento de acesso por funcionários e agentes dos serviços de informações da República Portuguesa, mediante autorização judicial prévia a cargo de secção especial para autorização de acesso a informação e a dados do Supremo Tribunal de Justiça, a dados de tráfego, de localização ou outros dados conexos das comunicações, para cumprimento das atribuições legais desses serviços (art. 1º), o projeto de lei introduz as alterações aos seguintes preceitos legais:



- (i) Lei 30/84, de 5 de setembro (Lei Quadro do Sistema de Informações da República Portuguesa):
- Alteração ao nº 2 do Art. 2º Finalidades do SIRP¹, e ao art. 5º² Acesso a dados e informações pelos funcionários e agentes do SIRP;
- Aditamento dos arts. 5º A Competência para a concessão de autorização; 5º B
   Procedimento do pedido de autorização e 5º C Transmissão, tratamento, manutenção e destruição das informações e dados.

# (ii) Lei 62/2013, de 26 de agosto (Lei de Organização do Sistema Judiciário)

- Alterações aos nºs 2 e 3 do art. 47º³ (que, na atual redação, passarão a constituir os nºs 4 e 5) - Organização do STJ;
- Alterações ao nº 3 do art. 66º⁴ (que na atual redação passará a constituir o nº
   4), Quadro de Magistrados do Ministério Público no STJ.

<sup>&</sup>lt;sup>1</sup> Que dispõe atualmente que «2 - 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».

<sup>&</sup>lt;sup>2</sup> Que dispõe atualmente que «1 - Os funcionários e agentes, civis ou militares, que exercem funções policiais só poderão ter acesso a dados e informações na posse dos serviços de informações desde que autorizados por despacho do competente membro do Governo, sendo proibida a sua utilização com finalidades diferentes da tutela da legalidade democrática ou da prevenção e repressão da criminalidade. 2 - O funcionário ou agente, civil ou militar, que comunicar ou fizer uso de dados de informações com violação do disposto no número anterior será punido com prisão até 3 anos, se pena mais grave não lhe for aplicável, independentemente da medida disciplinar que ao caso couber».

<sup>&</sup>lt;sup>3</sup> Que dispõem atualmente «2 - No Supremo Tribunal de Justiça há ainda uma secção para julgamento dos recursos das deliberações do Conselho Superior da Magistratura. 3 - A secção referida no número anterior é constituída pelo mais antigo dos vice-presidentes do Supremo Tribunal de Justiça, que tem voto de qualidade, e por um juiz de cada secção, anual e sucessivamente designados, tendo em conta a respetiva antiguidade».



## 2. Fundamentos da proposta de alteração

De acordo com a Exposição de Motivos, o projeto de lei tem como fundamentos:

**a.** Ausência de iniciativas legislativas que retomem a iniciativa Legislativa do XIX Governo Constitucional, que visou aprovar um novo regime jurídico do SIRP, e que, no segmento normativo relativo ao acesso a dados conservados pelas operadoras de telecomunicações – metadados -, veio a ser considerada inconstitucional pelo Acórdão do Tribunal Constitucional nº 403/2015, de 27 de Agosto;

**b.** Não diminuição da necessidade de acesso por parte do SIRP aos referidos dados, no contexto da manutenção e da não diminuição das ameaças terroristas, ocorrências que importa prevenir;

**c.** Papel incontornável desse acesso no contexto da *Estratégia Nacional de Combate ao Terrorismo*, aprovada pela Resolução do Conselho de Ministros nº 7-A/2015, de 20 de fevereiro;

**d.** Necessidade de dotar o SIRP de capacidade de cooperação, em igualdade de circunstâncias com os serviços congéneres europeus e outros países "que respeitam as exigências do Estado de direito Democrático", na deteção e prevenção de ameaças terroristas;

**e.** Alteração do modo de atuação dos movimentos terroristas e da sua organização, o que dificulta o combate do fenómeno e torna mais exigente a sua prevenção.

<sup>4</sup> Que dispõe que «É aplicável, com as necessárias adaptações, o disposto nos n.os 2 e 3 do artigo 57.º e no artigo 58.º».



## 3. Antecedentes da proposta

A matéria relativa ao *acesso a dados e informação* por parte dos oficiais de informações do SIS e do SIED, foi objeto da Proposta de Lei nº 345/XII, que veio a dar lugar ao Decreto da Assembleia da República nº 426/XII<sup>5</sup>.

Para efeitos do exercício das atribuições de recolha, processamento, exploração e difusão de informações "adequadas a prevenir a sabotagem, a espionagem, o terrorismo, e a 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 (al. c) do nº 2 do art. 4º), o art. 78º daquele Decreto previa, mediante prévia e obrigatória autorização da Comissão de Controlo Prévio<sup>6</sup>, o acesso dos serviços de informação a:

- Informações bancárias;
- Informações Fiscais;
- 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, data hora, duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização.

O referido Decreto da Assembleia da República foi objeto de pedido de fiscalização preventiva da constitucionalidade formulado pelo Presidente da República, no segmento normativo do nº 2 do art. 78º relativo ao acesso aos dados referentes às

<sup>&</sup>lt;sup>5</sup> Pelo qual se aprovou o Regime Jurídico do Sistema de Informações da República Portuguesa, revogando a lei 30/84, de 5/9, 9/2007, de 19/2 e os DL 225/85, de 4/7 e 254/95, de 30/9.

<sup>&</sup>lt;sup>6</sup> Órgão independente de fiscalização do SIRP inovatoriamente criado pelo mesmo Decreto, composta por juízes Conselheiros do STJ, designados pelo CSM.



comunicações, visando a apreciação da sua conformidade constitucional com o disposto no nº 4 do artigo 34º da Constituição da República.

Tendo apreciado as duas questões expressamente colocadas a propósito - (i) deve o acesso aos metadados considerar-se uma ingerência nas telecomunicações para os efeitos previstos na norma constitucional? (ii) pode considerar-se que a autorização prévia e obrigatória da Comissão de Controlo Prévio equivale ao controlo existente no processo criminal? -, o Tribunal Constitucional pronunciou-se no sentido da inconstitucionalidade da norma constante do nº 2 do art. 78º do Decreto da AR, no referido segmento, por violação do nº 4 do art. 34º da CRP, entendendo, em síntese, que:

- Os dados relativos às telecomunicações a que se refere o nº 2 do art. 78º do Decreto da AR consubstanciam dados de tráfego, e, como tal, estão a coberto da proteção da norma constitucional do nº 4 do art. 34º da CRP;
- A restrição dos direitos fundamentais objeto da proteção constitucional do nº 4 do art. 34º da CRP apenas é admitida em sede de processo penal;
- As atribuições do SIRP para efeitos de acesso àqueles dados recolha, processamento, exploração e difusão de informações -, porque preventivas, não se inserem no âmbito da investigação criminal, constituindo-se as suas ações de prevenção como procedimentos administrativos que, devendo respeitar os direitos, liberdades e garantias, não obedecem aos princípios jurídico-constitucionais conformadores do processo penal, proclamados no art. 32º da CRP;
- A ingerência nos dados de comunicação não tem, no presente contexto, lugar num procedimento que dê garantias e faculdades de proteção de alcance assimilável àquelas que conformam constitucionalmente o processo criminal;



• A Comissão de Controlo Prévio prevista no Decreto da Assembleia da República é um órgão administrativo que não tem poderes equivalentes a uma intervenção em processo criminal.<sup>7</sup>

## 4. Concreto conteúdo da proposta - Apreciação

## 4.1. Art. 2°, n° 2

**4.1.1.** Como referido, o projeto de lei introduz alterações ao nº 2 do art. 2º 8 da Lei 30/84, de 5/9, que atualmente rege sobre as *Finalidades* do SIRP 9.

Já a Declaração de voto de vencido do Conselheiro José António Teles Pereira, (que adiante se referirá mais atentamente) vai no sentido da conformidade constitucional do nº 2 do art. 78º do Decreto da AR, por entender, que, constituindo o acesso aos dados de tráfego, pelo SIRP, uma ingerência nas telecomunicações, a mesma é permitida pelo nº 4 do art. 34º da CRP, interpretado, através de uma redução teleológica, por forma a incluir a atividade dos Serviços de Informações ao lado da atividade de investigação criminal, na exceção à proibição consagrada naquele normativo constitucional. Por outro lado, considerou que a intervenção da Comissão de Controlo Prévio representa um mecanismo de controlo concreto da necessidade, adequação e proporcionalidade da interceção de dados, que a Constituição impõe, e assume, no particular contexto da atuação do SIRP, um papel equivalente, por proximidade axiológica, ao do juiz no processo penal, o qual, nos concretos termos constantes do Decreto da Ar, considerou não contrariar as exigências da Constituição.

<sup>&</sup>lt;sup>7</sup> O Acórdão teve uma Declaração de Voto e uma Declaração de Voto de vencido. A Conselheira Maria Lúcia Amaral votou a decisão mas deixou exarada a sua posição no sentido de que o juízo de inconstitucionalidade se deveria ter fundado apenas nas razões referentes à inexistência de um sistema interno de fiscalização e controlo do cumprimento dos limites legais do acesso, que fosse, ele, também protetor da ameaça da liberdade que esse acesso sempre representa, conforme exigido pelo disposto no nº 2 do art. 18º da CRP, e cuja inexistência não seria ultrapassada pela autorização prévia e obrigatória da Comissão de Controlo Prévio. Deixa, porém, anotada posição favorável a uma leitura aberta do nº 4 do art. 34º, no sentido de a sua interpretação dever ser feita numa perspetiva global das normas constitucionais, e não apenas literal, interpretação que admitiria, caso preenchidas as referidas exigências do nº 2 do art. 18º da CRP, o acesso aos dados de tráfego pelo SIRP.

<sup>&</sup>lt;sup>8</sup> As alterações em causa estão em linha com a redação dada ao nº 2 do art. 4º do Decreto 426/XII da Assembleia da República a que supra se fez referência. Procurando eventualmente responder a algumas das "críticas" feitas no Acórdão do Tribunal Constitucional, designadamente pela sua excessiva indefinição e,



A alteração proposta, mantendo a epígrafe do preceito e o seu nº 1 intocados, introduz no nº 2 o elenco das finalidades a que se destinam as concretas atividades daqueles Serviços:

- «2- Aos serviços de informações incumbe desenvolver, no respeito da Constituição e da lei, atividades de recolha, processamento, exploração e difusão de informações:
- a) Necessárias à salvaguarda da independência nacional, dos interesses nacionais e da segurança interna e externa do Estado Português;
- b) Que contribuam para garantir as condições de segurança dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de Direito e adequadas a prevenir a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido.
- c) Adequadas a prevenir a sabotagem, a espionagem, o terrorismo e sua proliferação, nos termos da lei de combate ao terrorismo, e a criminalidade altamente organizada de natureza transnacional.

consequente dificuldade de controlo da atuação do SIRP nesse domínio, a referência à recolha, processamento, exploração e difusão de informações adequadas a prevenir a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido deixou de ser feita na al. c), referente à prevenção dos fenómenos criminais ali elencados – atividade a que se reporta o acesso aos dados de telecomunicações.

2 - 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.»

<sup>&</sup>lt;sup>9</sup> Preceito que dispõe que «1 - As finalidades do Sistema de Informações da República Portuguesa realizam-se exclusivamente mediante as atribuições e competências dos serviços previstos na presente lei.



**4.1.1.1.** Na alteração a este preceito destaca-se, dada a sua relevância para as restantes alterações propostas, o conteúdo normativo da al. c), o qual, relativamente ao que era já a redação da correspondente alínea do nº 2 do art. 4º do Decreto nº 426/XII, da AR, adita o segmento *nos termos da lei de combate ao terrorismo*.

Segmento explicativo que pretenderá reforçar a relação entre as atividades de *recolha*, *processamento*, *exploração e difusão* de informações, que constituem a matriz funcional do SIRP, à prevenção criminal, e que se configura como uma tentativa de ultrapassar eventuais incompatibilidades constitucionais da previsão da al. c), designadamente com o nº 4 do art. 34º da CRP.

Pretensão que poderá contribuir, ainda que com alterações de que adiante se dará nota, para a eventual compatibilização constitucional do acesso aos dados de tráfego pelos serviços de informação.

**4.1.1.2**. Suscita-se a eventual ponderação da previsão relativa à *criminalidade altamente organizada* para efeitos de acesso a dados de comunicação pelo SIRP no âmbito da sua atividade de prevenção nesse âmbito.

Com efeito, o conceito processual penal de *criminalidade altamente organizada* previsto na al. m) do art. 1º do Código de Processo Penal<sup>10</sup>, abarca um alargado e diferenciado leque de crimes, nos quais se incluem ilícitos criminais que integram o habitualmente designado fenómeno de criminalidade económico-financeira, como é o caso dos crimes de *corrupção*, *tráfico de influência*, *participação económica em negócio ou branqueamento*.

"as condutas que integrarem crimes de associação criminosa, tráfico de pessoas, tráfico de armas, tráfico de estupefacientes ou de substâncias psicotrópicas, corrupção, tráfico de influência, participação económica em negócio ou branqueamento».

8



Tipologias e/ou fenómenos criminais que se afigura não justificarem, do ponto de vista das atribuições do SIRP, das finalidades que se pretendem alcançar com a proposta de lei, que estes serviços possam aceder a dados de telecomunicações e Internet relacionados com tal tipo de atos.

Poder-se-ão colocar dúvidas relacionadas com a verificação dos requisitos constitucionais de *necessidade*, *adequação e proporcionalidade* que devem presidir ao acesso, não apenas em concreto mas também à previsão legal dessa possibilidade.

Assim, estamos em crer que a solução da Proposta de Lei, neste particular, deverá ser ponderada no sentido de excluir tais fenómenos criminais/tipologias de crime - corrupção, tráfico de influência, participação económica em negócio ou branqueamento -, que, nos termos legais integram o conceito de criminalidade altamente organizada, da possibilidade de acesso aos dados de telecomunicações e Internet pelo SIRP.

## 4.2. Art. 5° - Acesso a dados e informações

**4.2.1.** O projeto de lei propõe a alteração do nº 1 do art. 5º da Lei 30/84 nos seguintes termos:

«1 - Os funcionários e agentes, civis ou militares, têm acesso, mediante autorização judicial a conceder nos termos da presente lei, a informação e registos relevantes para a prossecução das suas competências, contidos em ficheiros de entidades públicas, nos termos de protocolo, ouvida a Comissão Nacional de Proteção de Dados no quadro das suas competências próprias».



(i) Por contraponto ao atual nº 1 da Lei 30/84, o projeto de lei parece alterar aquele que é o atual objeto da norma<sup>11</sup> - o acesso, por parte dos *funcionários e agentes, civis e militares, que exercem funções policiais*, a informação que esteja na posse do SIRP.

A redação ora proposta, que se afigura algo imprecisa quanto ao seu concreto objeto, é construída, ao que se pode apreender, a partir do nº 1 do art. 78º e do referido nº 5 do art. 14º do Decreto 426/XII da AR, bem como dos nºs 2 e 3 do art. 9º da Lei 9/2007, de 19 de Fevereiro.

Assim, no confronto da norma proposta com a norma vigente, constata-se que:

- Mantém-se a referência a funcionários e agentes, civis e militares, eliminando-se a menção às funções policiais;
- Altera-se a entidade detentora da informação a que os destinatários da norma podem aceder, passando a prever-se a o acesso *a informações e registos contidos em ficheiros de entidades públicas*, enquanto na lei atual a informação passível de acesso é a informação detida pelos serviços de informações;
- Altera-se a entidade/órgão com competência para autorizar o acesso à informação e registos passa-se a exigir *autorização judicial* para o acesso à informação e registos ali mencionados, enquanto na atual lei o acesso à informação objeto desta norma depende *de despacho do competente membro do Governo*.
- Exige-se, expressamente, que a informação e registos a aceder sejam relevantes para a prossecução das competências dos destinatários da norma atualmente a lei reporta-se

<sup>11</sup> Que dispõe que «1 - Os funcionários e agentes, civis ou militares, que exercem funções policiais só poderão ter acesso a dados e informações na posse dos serviços de informações desde que autorizados por despacho do competente membro do Governo, sendo proibida a sua utilização com finalidades diferentes da tutela da

legalidade democrática ou da prevenção e repressão da criminalidade».



à proibição da sua utilização com finalidades diferentes da tutela da legalidade democrática ou da prevenção e repressão da criminalidade.

• O acesso à informação passa a efetuar-se, para além da autorização exigida, nos termos de protocolo, ouvida a Comissão Nacional de Proteção de Dados no quadro das suas competências próprias – remissão naturalmente inexistente na atual norma uma vez que nesta está em causa informação detida pelos serviços de informação e não por outras entidades públicas.

# 4.2.1.1. Apreciação

Com a introdução da nova redação ao nº 1 do art. 5º da Lei 30/84, o projeto de lei parece ter pretendido criar uma regra geral de acesso, por parte dos funcionários ali elencados, a informações detidas por outras entidades públicas, certamente com o intuito de constituir o amparo normativo do regime de acesso previsto no nº 2.

No entanto, e salvo o devido respeito, a criação de uma tal regra geral é feita sem que se pressinta a preocupação de conjugar a alteração proposta com outras alterações também propostas pelo projeto de lei e com outros normativos legais que integram o regime jurídico do SIRP, quer da própria Lei 30/84 quer da Lei 9/2007, de 19 de fevereiro.

### Assim:

a. Salvo melhor opinião, a norma do nº 1 do art. 5º ora proposta deixa sem regulamentação legal a matéria relativa ao acesso, por parte dos funcionários, agentes, civis e militares, com funções policiais, às informações detidas pelos serviços de informação. Acesso, que, na atual lei, apenas é possível mediante autorização do membro do governo competente.

Não existindo qualquer outra norma relativa a tal matéria, suscitam-se dúvidas sobre qual a informação detida pelos serviços de informação a que aqueles funcionários



e agentes poderão aceder, em que condições e sob autorização de que órgão esse acesso poderá ter lugar.

Lacuna<sup>12</sup> que se afigura ser precaver, atenta a natureza e sensibilidade dos dados constantes das informações recolhidas e tratadas pelo SIRP. Caraterísticas que demandam que o acesso às informações detidas por aqueles serviços seja objeto de regulamentação mínima, designadamente quanto à autorização para esse efeito e às suas finalidades.

Por outro lado, afigura-se que **fica igualmente sem previsão legal o sancionamento da utilização indevida dessa informação**, uma vez que o nº 5 do art. 5º do projeto apenas se reporta ao uso de informações e dados em violação do nº 2 desse mesmo preceito – objeto normativo que apenas se reporta a três categorias especificas de informação, não abarcando, desse modo, toda a informação que é acedida/detida pelos funcionários e agentes a que o preceito se reporta, designadamente à informação que é detida pelos serviços de informação.

Sendo certo que o sancionamento do uso indevido, por aquela categoria de funcionários e agentes, da informação na posse dos serviços de informação (que ora é objeto do nº 1 do art. 5º) se encontra sancionado no atual nº 2 do art. 5º. 13

**b.** Como referido, tendo em conta toda a estrutura e conteúdo normativo do art. 5°, a atual redação da norma do nº 1 parece pretender constituir a base do sistema de acesso do SIRP não apenas às informações objeto do nº 2 – *informação bancária*, *fiscal*,

<sup>12</sup> E sem prejuízo de poder ter sido intenção do projeto de lei excluir esse acesso, opção para a qual se não encontra justificação.

<sup>&</sup>lt;sup>13</sup> Que dispõe que «O funcionário ou agente, civil ou militar, que comunicar ou fizer uso de dados de informações com violação do disposto no número anterior será punido com prisão até 3 anos, se pena mais grave não lhe for aplicável, independentemente da medida disciplinar que ao caso couber».



dados de tráfego e de localização e outros dados conexos das comunicações -, mas também a outras informações e dados que se encontrem na posse de entidades públicas. Fazendo depender esse acesso, em todos os casos, de autorização judicial e dos termos de protocolo.

Salvo melhor opinião, a proposta não parece adequar-se à realidade que pretende regular, suscitando, ainda, dúvidas quanto ao procedimento de autorização judicial quando não estejam em causa os dados e as informações a que se refere o nº 2.

### Assim:

(i) No que respeita ao acesso aos dados das comunicações dever-se-á ter em consideração que esses dados não estão contidos em ficheiros de entidades públicas mas sim de operadoras de telecomunicações, as quais não assumem aquela natureza jurídica.

O conteúdo normativo do nº 1 do art. 5º poderá, quanto a este aspeto, revelar-se redutor e suscetível de criar divergências interpretativas que, atenta a sensibilidade da matéria, deverão ser evitadas.

Pelo que se justificará a reponderação da redação do nº 1 do art. 5º no segmento relativo à definição da natureza das entidades que detém a informação a que se pretende possibilitar o acesso pelo SIRP.

(ii) Uma vez que o acesso às informações a que se refere o nº 2 se encontra previsto e regulado na lei, na ausência de qualquer concreta referência legal ao que possa ser objeto do protocolo previsto no nº 1 não se vislumbra a sua exata abrangência nem a sua necessidade, salvo no que possa respeitar, vg., a questões técnicas de acesso, à definição de procedimentos de articulação, à definição da categoria de funcionários que poderão aceder, à forma de atribuição das necessárias credenciações.



Tanto assim que o projeto prevê as formas de acesso e de transmissão das informações e dos dados a aceder nos limites e termos da autorização judicial de que o concreto acesso depende (art. 5° -C).

Ao que acresce que, atenta a informação em causa, os termos do acesso, designadamente quanto ao tipo de informação e quanto ao modo como se deve processar, deverão ficar expressamente previstos na lei e não depender de atos de natureza protocolar entre as entidades envolvidas.

Admite-se, como referido, a necessidade de protocolo para efeitos da concretização das mencionadas questões técnicas e procedimentais para o acesso eletrónico a que alude o art. 5° C do projeto.

Em todo o caso, exigir-se-á, face à natureza da matéria em causa, e sem prejuízo da exigência de intervenção da CNPD, que fique expressa na lei a finalidade e os limites do protocolo a que se refere a norma, pelo menos quando estiverem em causa as informações e dados previstos no nº 2.

(iii) Cremos que será também importante referir que o nº 1 do art. 5º ora proposto parece não atender ao que se dispõe nos nºs 2 e 3 do art. 9º da Lei 9/2007, de 19 de Fevereiro. Afigura-se que o atual objeto do nº 1 do art. 5º permitirá suscitar dúvidas quanto à manutenção em vigor do citado art. 9º, ainda que este se destine a categorias funcionais específicas, pois poderá traduzir-se na manutenção de um regime menos exigente, designadamente no que respeita à necessidade de autorização judicial.

Com efeito, atento o que ora parece pretender-se regular no nº 1 do art. 5º, **poderá questionar-se a sua compatibilização com os nºs 2 e 3 do citado art. 9º**, que tem um universo subjetivo mais restrito, uma vez que limita o acesso à informação detida por entidades públicas aos *diretores, diretores-adjuntos e diretores de departamento do SIED e do SIS*.



Colocando-se, assim, a questão de saber se existe coincidência, ou não, entre o conteúdo normativo objetivo dos dois preceitos, ou seja, se está em causa o mesmo tipo de informações e registos. E, sendo esse o caso, qual a razão que justifica que o acesso, a coberto do atual art. 9°, não seja objeto de alterações e adequação ao regime que ora se pretende criar, designadamente quanto à sujeição do acesso a autorização judicial.

Não sendo esse o caso, sempre se exigiria que o referido artigo 9º fosse objeto de atualização, de modo a que do mesmo conste expressamente excluída do seu regime menos exigente a informação a que se refere o nº 2 do art. 5º.

(iv) A exigência de autorização judicial prevista genericamente no nº 1 do art. 5º parece referir-se, tal como redigida a norma, ao acesso a todas as informações e registos que estejam contidos em ficheiros de entidades públicas e que sejam relevantes para a prossecução das competências dos serviços de informação,

No entanto, o nº 3 do preceito, pese embora remeta para a autorização a que se refere o nº 1, parece reduzir as exigências/pressupostos dessa autorização às finalidades previstas na al. c) do nº 2 do art. 2º, deixando, assim, sem regulação, quanto a tais exigências/pressupostos, as finalidades da atividade dos serviços de informação prevista nas al. a) e b) deste preceito.

Por outro lado, o art. 5° B, que o projeto pretende aditar à Lei 30/84, referente ao procedimento do pedido de autorização, apenas contempla o pedido de acesso às informações e aos dados a que alude o nº 2 do artigo 5º, nada prevendo, em termos de procedimento, quanto às demais informações e dados na posse de entidades públicas a que o SIRP pode aceder, ainda que a redação do nº 1 do art. 5º não faça qualquer distinção quanto à exigência de autorização judicial.



O que poderá suscitar dúvidas sobre o concreto âmbito e objeto do nº 1 do art. 5º, e da autorização no mesmo prescrita, afigurando-se que o legislador do projeto parece ter dito mais do que o efetivamente pretendido.

Assim, permitimo-nos sugerir a reponderação do nº 1 do art. 5º na redação do projeto, de modo a que se clarifiquem as questões assinaladas, em particular:

- A ausência de regulação do acesso dos funcionários e agentes, civis ou militares, às informações detidas pelos serviços de informação;
  - A natureza das entidades detentoras da informação a aceder;
- A finalidade e os limites do protocolo a que se refere o preceito, pelo menos quando estiverem em causa as informações e os dados previstos no nº 2.
- A compatibilização do nº 1 do art. 5º com os nºs 2 e 3 do art. 9º da Lei 9/2007, de 19 de Fevereiro;
- O concreto âmbito e objeto da autorização judicial no mesmo prevista, tendo em conta a limitação das exigências/pressupostos dessa autorização às finalidades previstas na al.c) do nº 2 do art. 2º e a limitação do procedimento do pedido de autorização previsto no art. 5º B às informações e dados a que se refere o nº 2 do art. 5º.

### 4.2.2. - N° 2, 3 e 4 do art. 5°

O projeto de lei retoma a questão do acesso às *informações bancárias e fiscais e aos dados de tráfego, localização ou outros dados conexos das comunicações* pelos serviços de informação, possibilidade que foi originariamente introduzida pelo Decreto da Assembleia da República nº 426/XII, e que veio a ser objeto de declaração de não conformidade constitucional (apenas na parte respeitante ao acesso de dados das telecomunicações, única que foi colocada à apreciação do Tribunal Constitucional).



Prevê-se, assim, quanto a tal matéria que:

- 2 Os funcionários e agentes dos serviços de informações do SIS e do SIED podem, para efeitos do disposto na alínea c) do n.º 2 do artigo 2.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.
- 3 A autorização referida no número 1 é concedida quando não exista outro meio que permita a salvaguarda eficaz e atempada dos bens jurídicos a proteger e houver razões para crer que o acesso aos dados solicitados é indispensável, adequada e proporcional para prevenir a prática dos crimes previstos na alínea c) do n.º 2 do artigo 5.º.
- 4 Para cada pedido deve ser emitida uma única autorização, que pode combinar várias medidas no âmbito da mesma ação.

### 4.2.2.1. - Apreciação

### a. Acesso a informação bancária e a informação fiscal

O art. 78º do Decreto 426/XII da Assembleia da República previa o acesso do SIRP a informação bancária e a informação fiscal, matéria que não foi objeto de dúvidas de constitucionalidade em sede de fiscalização preventiva.

Aquando da análise da Proposta de Lei do Governo, que veio a dar lugar ao identificado Decreto da AR, a Procuradoria-Geral da República tomou posição nos seguintes termos:

No que se refere ao acesso a informações bancárias não temos qualquer objeção à proposta tendo em conta as finalidades prosseguidas pelo SIRP. Desde logo porque o acesso depende da prévia autorização da Comissão de Controlo Prévio.



Por outro lado, o n.º 2 do artigo 79.º do DL n.º 298/92, de 31 de dezembro (Regime geral das instituições de crédito e sociedades financeiras) prevê que " (...) os factos e elementos cobertos pelo dever de segredo só podem ser revelados:

- a) Ao Banco de Portugal, no âmbito das suas atribuições;
- b) À Comissão do Mercado de Valores Mobiliários, no âmbito das suas atribuições;
- c) Ao Fundo de Garantia de Depósitos, ao Sistema de Indemnização aos Investidores e ao Fundo de Resolução, no âmbito das respetivas atribuições;
- d) Às autoridades judiciárias, no âmbito de um processo penal;
- e) À administração tributária, no âmbito das suas atribuições;
- f) Quando exista outra disposição legal que expressamente limite o dever de segredo.

A norma agora prevista passará a ser um dos casos abrangidos pela alínea f) do n.º 2 do artigo 78.º do RGICSF.

Quanto ao acesso a informação fiscal, determina o n.º 2 do artigo 64.º da Lei Geral Tributária que "O dever de sigilo cessa em caso de: (...) Cooperação legal da administração tributária com outras entidades públicas, na medida dos seus poderes.»

Assim sendo, e mais uma vez por depender da autorização da Comissão de Controlo Prévio, não temos objeção a este acesso a informações fiscais, tendo em conta as finalidades prosseguidas pelo SIRP.

Cremos ser de manter a posição então assumida, agora reforçada pelo facto de se exigir prévia autorização judicial nos termos constantes do art. 5°-A, 5°-B e 5°.C do projeto de lei.

Não se olvida que, como se refere no Acórdão do Tribunal Constitucional nº 442/2007, de 14 de agosto de 2007 «o bem protegido pelo sigilo bancário cabe no âmbito de protecção do direito à reserva da vida privada consagrado no artigo 26.º, n.º 1, da Constituição da República».



No entanto, como também se refere naquele aresto do Tribunal Constitucional, « [Mas] uma coisa é o âmbito de protecção, prima facie, de uma previsão de um direito fundamental, outra é o seu âmbito de garantia efectiva (cfr. GOMES CANOTILHO, "Dogmática de direitos fundamentais e direito privado", in INGO SARLET (org.), Constituição, direitos fundamentais e direito privado, 2.º ed., Porto Alegre, 2006, 341 s., esp. 346 s.). Este só se recorta, neste caso, em resultado de um balanceamento entre os interesses e valores ligados à tutela da privacidade e os interesses, também constitucionalmente protegidos, com eles conflituantes. Nessa ponderação, e na lição de CANARIS (a propósito dos imperativos constitucionais de protecção, mas com considerações transponíveis, ao que julgamos, para uma metodologia geral da ponderação), há que levar em conta, não só a relação hierárquica abstracta entre os bens em conflito, mas também "o peso concreto dos bens e interesses envolvidos" - cfr. Direitos fundamentais e direito privado, trad. port. de Ingo Sarlet e P. Mota Pinto, Coimbra, 2003, 112 s. E, nesta ponderação contextualizada de interesses, não pode deixar de se dar relevo decisivo ao "nível do direito fundamental afectado" e ao grau da sua lesão. Ora, o segredo bancário localiza-se no âmbito da vida de relação, à partida fora da esfera mais estrita da vida pessoal, a que requer maior intensidade de tutela. Ainda que compreendido no âmbito de protecção, ocupa uma zona de periferia, mais complacente com restrições advindas da necessidade de acolhimento de princípios e valores contrastantes. Posição esta defendida no recente Acórdão n.º 42/2007 deste Tribunal, onde expressamente se afirma: "O segredo bancário não é abrangido pela tutela constitucional de reserva da vida privada nos mesmos termos de outras áreas da vida pessoal". A susceptibilidade de "restrições [ao segredo bancário] impostas pela necessidade de salvaguardar outros direitos ou interesses constitucionalmente protegidos" foi, também, amplamente admitida pelo Acórdão n.º 278/95 deste Tribunal, logo após se ter considerado o sigilo bancário integrado no âmbito de protecção do direito à reserva da intimidade da vida privada.»



Nessa medida, na perspetiva da compatibilização entre os interesses e valores protegidos pelo sigilo bancário e os interesses que se visam prosseguir com o acesso à informação bancária por parte dos serviços de informação, cremos que se poderá concluir pela admissibilidade constitucional da restrição ao direito fundamental protegido pelo sigilo bancário que resulta do acesso que ora se pretende conceder.<sup>14</sup>

Com efeito, de acordo com o projeto de lei, o acesso à informação bancária pelos serviços de informação tem em vista o desenvolvimento das atividades de recolha, processamento, exploração e difusão de informações adequadas a prevenir a sabotagem, a espionagem, o terrorismo e a sua proliferação e a criminalidade altamente organizada de natureza transnacional.

Ou seja, visa uma atividade destinada à salvaguarda de bens e valores constitucionalmente protegidos, desde logo o valor da segurança. Como se afirma na Declaração de Voto da Conselheira Maria Lúcia Amaral no Acórdão do Tribunal Constitucional 403/2015, «A existência de Serviços de Informações da República (...) numa ordem, como a nossa, de Estado de direito democrático, justifica-se pela necessidade de salvaguardar bens jurídicos, coletivos e individuais, que ocupam na axiologia constitucional um lugar não menor que os bens tutelados por normas penais incriminadoras».

Acresce, ainda, que as informações bancárias que sejam acedidas pelos serviços de informação para as finalidades legalmente previstas, e mediante autorização judicial,

\_

<sup>&</sup>lt;sup>14</sup> Como resulta do disposto no artigo 18.º da Constituição, a restrição de certos direitos fundamentais é admissível para salvaguarda de outros direitos constitucionalmente protegidos, devendo essas restrições limitarse ao necessário para alcançar os objetivos visados.



apenas se destinam a utilização no âmbito da atividade desenvolvida pelos serviços de informação<sup>15</sup>.

Nessa medida, afigura-se que o âmbito subjetivo de conhecimento dos dados bancários que sejam acedidos é restrito.

Por outro lado, não se deverá desconsiderar que, para além das informações em causa poderem ser sujeitas ao regime de segredo de Estado, o que restringe claramente o acesso a tais informações, os funcionários daqueles serviços encontram-se sujeitos ao dever de sigilo, nos termos expressos no art. 28º da Lei 30/84 e no art. 5º nº 3 da Lei 9/2007.<sup>16</sup>

Ao que será ainda de aditar a consideração de que a comunicação e a utilização daqueles dados em violação do que se dispõe no nº 2 do art. 5º constitui crime, conforme previsto no nº 5 do art. 5º.

Salvo melhor opinião, cremos poder concluir-se que, sendo admitida a possibilidade de restrições ao sigilo bancário, as limitações que decorrem do acesso às informações bancárias pelos serviços de informação são justificadas por relevantes valores também constitucionalmente protegidos.

Ainda que como se dispõe no nº 3 do art. 32º da Lei 30/84, de 5 de setembro, aqueles serviços devam comunicar às entidades competentes para a investigação ou instrução de factos indiciários da prática de crimes contra a segurança do Estado. Com efeito, tais comunicações destinam-se igualmente à salvaguarda, pelas normas incriminadoras, de valores constitucionalmente tutelados, para além de que estão em causa domínios em que o acesso àquelas informações é legalmente previsto. Não se afigurando, assim, que o alargamento do conhecimento desses dados, por via de tais comunicações, conflitue com a natureza e justificação constitucional do sigilo bancário.

<sup>&</sup>lt;sup>16</sup> Que estabelece que «Toda a atividade de pesquisa, análise, interpretação, classificação e conservação de informações desenvolvida no âmbito do SIRP está sujeita ao dever de sigilo, nos termos definidos pela Lei Quadro do SIRP».



Cremos dever ainda considerar-se que a atividade desenvolvida pelos serviços de informação se encontra, também ela, sujeita a regimes de segredo – não apenas, e eventualmente, a segredo de Estado, como, igualmente, a sigilo profissional.

Por outro lado, mostra-se também assegurada a vertente da exigência de previsão de garantias que acautelem os valores tutelados pelo sigilo bancário.

Com efeito, para além da exigência de autorização judicial para o acesso e da exigência de fundamentação das razões que aconselham a medida (al. b) do nº 1 do art. 5º B), esta só pode ser autorizada «quando não exista outro meio que permita a salvaguarda eficaz e atempada dos bens jurídicos a proteger e houver razões para crer que o acesso aos dados solicitados é indispensável, adequada e proporcional para prevenir os crimes previstos na alínea c) do nº 2 do art. 2º 17» (nº 3 do art. 5º).

Termos em que se afigura que o acesso a informação bancária não suscitará questões de desconformidade constitucional.

## b. Informação fiscal - Sigilo Fiscal

O sigilo fiscal cessa nas diferentes situações previstas no art. 64º da Lei Geral Tributária<sup>18</sup>, sendo a sua proteção constitucional «manifestamente inferior quando comparada à de outros segredos, como é o caso do médico ou religioso (...). O segredo fiscal

<sup>&</sup>lt;sup>17</sup> Como adiante se anotará, o nº 3 do art. 5º contém manifesto lapso quando se refere ao nº 2 do art. 5º.

<sup>18 «2 -</sup> O dever de sigilo cessa em caso de: a) Autorização do contribuinte para a revelação da sua situação tributária; b) Cooperação legal da administração tributária com outras entidades públicas, na medida dos seus poderes; c) Assistência mútua e cooperação da administração tributária com as administrações tributárias de outros países resultante de convenções internacionais a que o Estado Português esteja vinculado, sempre que estiver prevista reciprocidade; d) Colaboração com a justiça nos termos do Código de Processo Civil e Código de Processo Penal; e) Confirmação do número de identificação fiscal e domicílio fiscal às entidades legalmente competentes para a realização do registo comercial, predial ou automóvel».



não é pois tutelado entre nós como um segredo absoluto, enquadrando-se os interesses que com ele se pretendem proteger numa dimensão da privacidade do cidadão situada fora do núcleo da intimidade privada e familiar que a lei protege para proporcionar «garantias efetivas contra a utilização abusiva ou contrária à dignidade humana»<sup>19</sup>.

Aplicam-se quanto ao sigilo fiscal, e salvo melhor opinião, os considerandos tecidos quanto ao sigilo bancário, dada a similitude da intensidade da sua tutela constitucional.

Assim, reafirmando os argumentos aduzidos no ponto anterior, cremos que se poderá concluir que o acesso a informação fiscal pelos serviços de informação, previsto pelo projeto de lei, não suscitará também reservas de constitucionalidade.

## c. Acesso a dados de tráfego, de localização ou outros conexos das comunicações

Como referido, o projeto de lei retoma, também quanto a esta matéria, a norma constante do art. 78° do Decreto 426/XII da Assembleia da República, inovando, no que parece ser uma tentativa de ultrapassar questões de desconformidade constitucional, ao introduzir a exigência de autorização judicial a conceder por um coletivo de juízes de uma secção especial do STJ, e normas procedimentais relativas ao pedido de autorização e de transmissão, tratamento, manutenção e destruição das informações e dados a que foi dada autorização de acesso (arts. 5°A, 5° B e 5° C).

Os fundamentos constitucionais invocados no Acórdão 403/2015 do Tribunal Constitucional suscitam, contudo, dúvidas sobre se o sistema que o projeto de lei pretende criar permite ultrapassar a interpretação que determinou a decisão do Tribunal Constitucional de julgar inconstitucional o nº 2 do citado art. 78º, por violação do nº 4 do art. 34º da Constituição da República.

\_

<sup>&</sup>lt;sup>19</sup> Acórdão do TRE, Proc. 353/15.6JAAVR-A.P1, de 7/4/2016.



Na verdade, o referido aresto não fundou o juízo de inconstitucionalidade apenas na consideração da natureza administrativa da Comissão de Controlo Prévio prevista no Decreto 426/XIII e na não equivalência dos seus poderes *a uma intervenção em processo penal*.

Foi também fundamento da decisão de inconstitucionalidade a não conformação da norma do nº 2 do art. 78º do Decreto nº 426/XII da Assembleia da República, no respeitante ao acesso aos dados de tráfego, à previsão constitucional do nº 4 do art. 34º da CRP.

Com efeito, o referido aresto concluiu que «a proibição de ingerência nas comunicações, constante do artigo 34º da CRP, abrange os dados de tráfego» e que «Na verdade 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 controlo que estabelece, colocam o acesso aos dados de tráfego fora do âmbito da investigação criminal». Acrescentando, por referência às atribuições do SIRP e às finalidades do acesso pretendido, que « [Ora], a caracterização dessa concreta actividade como recolha de "informações" para efeitos de "prevenção" dissocia-a, de forma clara e precisa, da atividade própria da investigação criminal. (...)»

Concluindo o Acórdão, depois de analisar a relação entre "informações" e "investigação criminal" que «o legislador teve a preocupação de distinguir, em sentido material e orgânico, as duas atividades» distinção radical «[que] impede os oficiais de informação de intervirem no processo penal. As informações [...] 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 a 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».



Acentua, ainda, aquele aresto, que, enquanto a recolha de informações no âmbito da investigação criminal, porque dirigida a "um crime já praticado" «é sempre feita num contexto previamente delimitado pelo objeto desse processo, apenas se recolhendo informações no contexto da investigação de um específico facto e em relação a específicos sujeitos tidos como suspeitos», no âmbito da atuação preventiva dos serviços de informação as suas funções de recolha e tratamento de informações «não se orientam para uma actividade investigatória de crimes praticados ou em execução».

Concluindo assim que «As ações de prevenção do SIRP são, pois, procedimentos administrativos que, devendo respeitar os direitos, liberdades e garantias (...) não obedecem aso princípios jurídico-constitucionais conformadores do processo penal, proclamados no art. 32º da CRP».

Conclusão que assume maior impacto quando relacionada com a consideração de que a atribuição ao SIRP da possibilidade de acesso aos dados das comunicações (dados de tráfego, no que ora releva quanto ao acesso pretendido), não se insere nos limites constitucionalmente admitidos pelo nº 4 do art. 34º da CRP de restrição aos direitos fundamentais, pois, «Ao definir o campo de incidência da lei restritiva do direito à inviolabilidade das comunicações peça "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».

Após se pronunciar quanto à eventual existência de matérias em que o valor da segurança sobreleva os valores próprios do direito à inviolabilidade da comunicações cuja não inclusão



no âmbito da restrição a estes direitos pudessem contrariar o plano ordenador do sistema jurídico-constitucional, que o legislador constitucional ao longo das revisões constitucionais «deixou inalterados os termos da norma permissiva de ingerência nas telecomunicações, estabelecida na 2ª parte do nº 4 do art. 34, e o seu alcance restrito a "matéria de processo criminal"», o Tribunal Constitucional conclui que «Nada autoriza, pois, a admitir uma eventual extensão do âmbito da ressalva final do nº 4 do art. 34º - para a qual, aliás, o intérprete, neste contexto concreto, não dispõe de instrumentos metodológicos adequados».

A posição assumida pelo Tribunal Constitucional parece limitar a margem de atuação do legislador ordinário em sede de atribuição ao SIRP da possibilidade de acesso aos dados de comunicações, tal como previsto pelo art. 5° n° 2 do projeto de lei, mesmo quando essa possibilidade seja, como é, apenas dirigida a prevenir «a sabotagem, a espionagem, o terrorismo e a sua proliferação, nos termos da lei de combate ao terrorismo, e a criminalidade altamente organizada de natureza transnacional» (art. 2° n° 2, al. c) do projeto de lei).

Neste particular segmento da conformação constitucional da proposta, o projeto de lei não parece ultrapassar as dificuldades apontadas pelo Tribunal Constitucional, na leitura que faz da previsão do nº 4 do art. 34º da CRP, na medida em que, mantendo-se a natureza e as atribuições do SIRP inalteradas, bem como, no essencial, as finalidades do acesso aos dados de comunicações, mantém-se, igualmente, por reporte à perspetiva do Acórdão 403/2015, a ausência do contexto processual penal em que a CRP admite a ingerência nas comunicações.

De qualquer modo, não poderá desconsiderar-se a posição assumida nas duas Declarações de Voto constantes do Acórdão do Tribunal Constitucional, que, ainda que em graus diferenciados, direcionam a leitura do nº 4 do art. 34º da CRP no sentido de permitir a inclusão no seu âmbito normativo da atividade de prevenção do SIRP, no



contexto dirigido aos fenómenos criminais contidos no agora nº 2, al. c) do art. 2º do projeto de lei.

Na verdade, afigura-se relevante a posição assumida naquelas Declarações no sentido de que uma interpretação integrada daquele normativo constitucional admite o acesso pelo SIRP aos dados das comunicações.

Demonstra-se também relevante, do ponto de vista jurídico-constitucional, a abordagem relativa às garantias de controlo e fiscalização da intervenção do SIRP nas comunicações – segmento da questão que, podendo não estar absolutamente ultrapassado pelo projeto, pese embora a exigência de autorização judicial e normatização de procedimentos destinados a garantir a legalidade da intervenção, poderá, contudo, ser melhorado com a previsão de garantias acrescidas de controlo da atuação dos serviços de informação.

Com efeito, a Declaração de Voto da Conselheira Maria Lúcia Amaral coloca a desconformidade constitucional da norma que foi objeto de apreciação nas questões relativas à inexistência de *um sistema de controlo interno quanto ao cumprimento dos limites legais das interceções de comunicações que fosse, ele também, protector da ameaça da liberdade que aquela interceção representa,* não se cumprindo, assim, as exigências decorrentes do nº 2 do art. 18º da CRP <sup>20</sup>.

-

A norma não definia com a precisão necessária os limites da intervenção administrativa na liberdade individual, pois ao se dizer que a intervenção seria legítima quando implicasse a adoção de meios «necessário, adequados e proporcionais, numa sociedade democrática, para o cumprimento das atribuições legais dos serviços de informação», equivale praticamente a dizer que toda a ponderação quanto à proporcionalidade da intervenção seria por inteiro devolvida à administração; (...) por outro lado, dizer-se que tal intervenção só seria possível para efeitos do disposto no nº 2 do art. 4º significava, pela amplitude e indeterminação da habilitação que era conferida à administração, que a intervenção desta última seria legítima numa tão vasta plêiade de circunstâncias que se tornaria praticamente impossível delimitar os factores da sua não



Questões que poderão, contudo, ser objeto de maior aprofundamento e aperfeiçoamento, no sentido da definição de uma estrutura de controlo interno e externo capaz de garantir a adequação da intervenção dos serviços de informação às exigências constitucionais.

O que poderá ser alcançado com a introdução, designadamente, das alterações que adiante se sugerem relativamente aos arts. 5° A, 5°B e 5°C que o projeto de Lei pretende aditar à Lei 30/84, bem como com o reforço da intervenção dos órgãos de fiscalização do SIRP.

Do ponto de vista da avaliação da natureza e finalidades da atividade dos serviços de informação, a Conselheira Maria Lúcia Amaral aceita que havendo afinidade valorativa ou teleológica entre as finalidades prosseguidas pelos serviços de informação e as normas penais incriminadoras (...) poder-se-ia concluir (...) que a autorização constitucional para restringir a inviolabilidade das telecomunicações em «matérias de processo criminal» se estenderia, por maioria de razão, ao SIRP.

Terminando por afirmar não ver «como possa retirar-se do sistema constitucional, no seu conjunto tomado, a proibição da existência de meios administrativos de defesa da Constituição, destinados a garantir a convivência adequada entre liberdade individual e segurança coletiva [e também individual], e por isso mesmo, capazes de ser abrangidos pela autorização constitucional constante da parte final do nº 4 do art. 34º da CRP.

A Declaração de Voto do Conselheiro Teles Pereira aprofunda a análise das diferentes vertentes da questão do acesso a dados de comunicação pelos serviços de

admissibilidade. Por ultimo, e na ausência de tais limites, a intervenção prévia da Comissão de Controlo Prévio não preencheria por si só a necessidade de controlo e fiscalização interna da intervenção administrativa, não constituindo um procedimento eficiente de controlo que prevenisse ou evitasse intromissões abusivas nas liberdades individuais.



informação, referindo **existir uma relação de complementaridade entre a atividade** dos Serviços de Informações e o processo penal.

Refere, designadamente, que «(...) Tratam-se de dois sistemas – de duas áreas da atividade do Estado – que, face ao que vai dito supra não podem, com propriedade, dizer-se enraizados em diferentes lugares, realidades e funções, respondendo a preocupações radicalmente – e sublinhamos o advérbio: radicalmente – diversas, no mais amplo e complexo sistema de segurança e justiça.

Na verdade, se o SIRP tem como finalidade assegurar, através dos dois Serviços de informações que o integram, no estreito respeito da Constituição e da lei, a produção de informações necessárias à salvaguarda da segurança interna e externa, da independência e interesses nacionais e da unidade e integridade do Estado (artigo 2º do Decreto n.º 426/XII) e se desenvolve atividades de recolha, processamento, exploração e difusão de informações necessárias à salvaguarda da independência nacional, dos interesses nacionais e da segurança interna e externa do Estado Português, informações que contribuam para garantir as condições de segurança dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade, informações adequadas 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 (artigo 44°, n.° 2 do Decreto n.° 426/XII), sendo isto assim, dizíamos, forçoso é concluir, desde logo, que se posiciona, a atividade de produção de informações, no âmbito da tutela preventiva de bens jurídicos protegidos pelo Direito Penal, no sentido de referenciáveis a ele, bens estes instrumentalmente servidos pelo direito processual penal.

Não é isto o mesmo – é forçoso, desde já, dizê-lo – que fazer coincidir a sua atividade (a produção de informações) com a que se desenvolve no processo penal. O que aqui se afirma é uma relação de complementaridade, são conexões, não uma identidade, tanto mais que ao pessoal do SIRP é vedado exercer poderes, praticar atos ou desenvolver atividades do



âmbito ou da competência específica dos tribunais, do Ministério Público ou das entidades com funções policiais (artigo 5°, n.° 2 do Decreto n.° 426/XII). (...)

A atividade do SIRP é objeto, como já dissemos, de fiscalização externa especializada (i) do Conselho de Fiscalização do SIRP, composto por três cidadãos de reconhecida idoneidade, eleitos Assembleia da República; (ii) da Comissão de Fiscalização de Dados do SIRP, composta por três magistrados do Ministério Público nomeados pelo Procurador-Geral da República, com sede na Procuradoria-Geral da República; e, agora, (iii) da Comissão de Controlo Prévio, composta por três magistrados judiciais, designados pelo Conselho Superior da Magistratura, de entre juízes conselheiros do Supremo Tribunal de Justiça, com, pelo menos, três anos de serviço nessa qualidade (artigos 20., 21°, 29° e 35° do Decreto n.º 426/XII).

A esta primeira nota – diríamos estática – acresce a mais importante imagem dinâmica dos serviços de informações, visto que a sua atividade passa, em boa medida, por reunir informações destinadas a prevenir a ocorrência de factos previstos e punidos na lei penal, designadamente em matéria de criminalidade grave e altamente organizada, informações essas que, para além de se destinarem aos decisores políticos competentes, são também destinadas – quando a matéria diga respeito à respetiva área de atuação – às entidades competentes de investigação criminal."

Aprofundando a análise no domínio dos princípios da proporcionalidade e da proibição do excesso afirma que «Testando a norma do artigo 78°, n° 2 do Decreto n° 426/XII face ao referido princípio, a primeira nota que se colhe – para além da legitimidade de princípio (fim legítimo) de uma intervenção legislativa consistente na alocação de meios de atuação aos Serviços de Informações, protagonistas de uma função do Estado que a Constituição expressamente refere – para além disto, dizíamos, colhe-se a ideia de uma manifesta adequação da medida legislativa à prossecução do fim a que se destina (obtenção de informações relevantes para a atividade dos Serviços integrados no SIRP). A obtenção de "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" é manifestamente adequada – no contexto da atuação dos serviços de informações – ao funcionamento do ciclo de produção de informações, permitindo, designadamente, estabelecer a (essencial) conexão entre pessoas e lugares que aqueles Serviços tenham por carecidos de análise. Sublinhar-se-á aqui, relativamente ao fenómeno terrorista contemporâneo, enquanto ameaça bem presente nas sociedades dos nossos dias, o desenvolvimento deste em rede, através de conexões (contactos) entre pessoas em pontos geográficos afastados, em termos que tornam intuitiva, como matéria-prima informacional, a deteção e relacionação desses contactos.

A necessidade ou exigibilidade, por sua vez, traduzida na impossibilidade de adoção de medidas menos intrusivas com os mesmos efeitos na prossecução do fim visado, também deve ter-se aqui por estabelecida, uma vez que aos Serviços de Informações será, hoje mais ainda do que até agora, imprescindível a recolha dos identificados dados de tráfego, precisamente para estabelecimento das apontadas conexões entre informações dispersas, em vista da formação de um quadro informacional coerente. Trata-se, basicamente, de propiciar acesso a elementos determinantes para a alimentação e regular constituição e funcionamento do ciclo de produção de informações. E é este um resultado que não poderia obter-se por via menos intrusiva, certamente inalcançável através dos vagos e imprecisos dados de base. Os instrumentos resultantes daquele n.º 2 traduzem, assim, a já assinalada "menor desvantagem possível" no (necessário) sacrifício de algo na esfera pessoal de reserva de intimidade, entendida como direito à autodeterminação informativa.»

Terminando por responder às questões de constitucionalidade suscitadas nos seguintes termos: «(1) à primeira questão – deve o acesso aos metadados considerar-se uma ingerência nas telecomunicações para os efeitos previstos na norma constitucional? – responderia que o acesso aos dados de tráfego pelos oficiais de informações do SIRP, nos termos do artigo 78°, n° 2 do Decreto n.º 426/XII, constitui uma ingerência nas



telecomunicações, sendo esta, todavia, permitida pela norma do nº 4 do artigo 34º da CRP, interpretada, através de uma redução teleológica, por forma a incluir a atividade dos Serviços de Informações, ao lado da atividade de investigação criminal, na exceção à proibição de princípio ali consagrada; (2) à segunda questão – pode considerar-se que a autorização prévia e obrigatória da Comissão de Controlo Prévio equivale ao controlo existente no processo criminal? – responderia que a referida autorização da Comissão de Controlo Prévio representa um mecanismo de controlo concreto da necessidade, adequação e proporcionalidade da interceção de dados, que a Constituição impõe, e assume, no particular contexto da atuação do SIRP, um papel equivalente, por proximidade axiológica, ao do juiz no processo penal, o qual, nos concretos termos constantes do Decreto n.º 426/XII, entendo não contrariar as exigências da Lei Fundamental.»

Cremos que a posição defendida em ambas as Declarações de Voto relativamente à admissibilidade constitucional de acesso pelos serviços de informação aos dados das comunicações não poderá, pois, deixar de ser levada em conta como referencial jurisprudencial de uma visão interpretativa conforme à Constituição.

Não podendo deixar de se anotar que o projeto de lei direciona algum esforço no sentido de alcançar uma maior conformação do sistema que se pretende aprovar às exigências constitucionais de delimitação da legalidade da intervenção, na perspetiva do controlo, ainda que apenas externo, da sua necessidade, adequação e proporcionalidade.

Com efeito, o nº 3 do art. 5º prescreve que a autorização judicial de acesso é concedida quando não exista outro meio que permita a salvaguarda eficaz e atempada dos bens jurídicos a proteger e houver razões para crer que o acesso aos dados solicitados é indispensável, adequada e proporcional para prevenir a prática dos crimes previstos na alínea c) do nº 2 do art. 2º.



Delimitação que, conjugada com o disposto no art. 5º B, em especial no nº 1, se afigura poder constituir, se alterado nalguns aspetos, como adiante se referirá quanto a este artigo, um quadro procedimental capaz de garantir um adequado controlo da legalidade da intervenção requerida e do seu concreto desenvolvimento por parte dos serviços de informação.

Por outro lado, a intervenção do Ministério Público, na perspetiva da defesa da legalidade, configura-se também como um factor da maior relevância no âmbito das exigências constitucionais de efetiva garantia das exigências constitucionais da necessidade, adequação e proporcionalidade da ingerência.

**d.** Em termos de direito comparado, assinala-se o regime legal relativo ao acesso do *Centro Nacional de Inteligencia* espanhol a dados de comunicações, constante da LEY ORGANICA 2/2002, de 6 de mayo, reguladora do controlo judicial prévio daquela entidade, e no qual o projeto de lei em apreço parece ter-se inspirado.

Dispõe-se no nº 1 do artigo único daquele diploma que «El Secretario de Estado Director del Centro Nacional de Inteligencia deberá solicitar al Magistrado del Tribunal Supremo competente, conforme la Ley Orgánica del Poder Judicial, autorización para la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, siempre que tales medidas resulten necesarias para el cumplimiento de las funciones asignadas al Centro».



Sendo certo que, as finalidades da atividade do *Centro Nacional de Inteligencia*, embora genericamente coincidentes com as finalidades do SIRP, são elencadas na lei com menor especificação no que tange à prevenção de atividades criminosas<sup>21</sup>.

Não se olvida que a norma Constitucional espanhola poderá permitir uma interpretação mais abrangente que o nº 4 do art. 34º da Constituição portuguesa, pois ali se determina que «Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial»<sup>22</sup>

Estipulando o nº 2 do art. 55º da Constituição Espanhola que «Una ley orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas».

**4.2.2.** Ainda sobre o nº 3 do art.5°, **anota-se que existe evidente lapso de redação na** referência à alínea c) do nº 2 do art. 5°, pois todo o contexto normativo indica que a remissão pretendida respeita à alínea c) do nº 2 do art. 2°.

<sup>&</sup>lt;sup>21</sup>LEY 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia – Art. 1º «El Centro Nacional de Inteligencia es el Organismo público responsable de facilitar al Presidente del Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones».

<sup>&</sup>lt;sup>22</sup> Art. 18° n° 3.



### 4.2.3 - N° 5 do art. 5°

Mantém-se a norma incriminadora ora prevista no nº 2 do art. 5º da lei 30/84, ainda que com diferente âmbito objetivo, na medida em que o que se incrimina é a utilização das informações e dados em violação do nº 2 <sup>23</sup>.

Para além do que supra se referiu, anota-se que o preceito deixa sem previsão incriminadora a utilização indevida de outras informações e dados a que os sujeitos passivos da norma têm acesso por força do disposto na abrangente previsão do nº 1 do art. 5°.

Na verdade, o nº 2 do art. 5º apenas respeita às informações bancárias, fiscais e dados de comunicações, enquanto a norma do nº 1 se refere, sem qualquer delimitação, às informações e registos contidos em ficheiros de entidades públicas que sejam relevantes para o exercício das competências dos funcionários e agentes que às mesmas podem aceder. Menção que tem um âmbito e um objeto necessariamente mais abrangente do que a norma do nº 2.

Ora, se a delimitação incriminadora prevista no nº 2 do atual art. 5º se poderá justificar por o nº 1 ter um âmbito objetivo e subjetivo diverso do previsto no projeto, não se vislumbra, contudo, que, na atual configuração da norma, se justifique a limitação da incriminação a um concreto tipo de informações e dados. Pois que todas as informações a que se refere o nº 1, e nas quais se incluem as reguladas no nº 2, têm apenas como finalidade a prossecução das competências dos funcionários e agentes que a elas acederam.

<sup>&</sup>lt;sup>23</sup> O funcionário e agente que comunicar ou fizer uso de informações e de dados em violação do disposto no n.º 2 será punido com pena de prisão até 3 anos, se pena mais grave não lhe for aplicável, independentemente da medida disciplinar que ao caso couber.



Estando em causa a violação do mesmo tipo de bens e valores jurídicos, não se vislumbram razões para que tais comportamentos, quando respeitem a outro tipo de informações e dados, não mereçam idêntica tutela penal.

## 5. Alterações à Lei 62/2013, de 26 de agosto - Lei da organização do sistema judiciário

**5.1.** Em conformidade com o regime previsto no art. 5° A, que o projeto de lei pretende aditar à Lei 30/84, relativo à *competência para a concessão de autorização* (judicial)<sup>24</sup>, o art. 3° do projeto prevê a introdução de alterações aos n°s 2 e 3 do art. 47° e ao n° 3 do 66° da Lei 62/2013, de 26 de agosto.

Prevê, assim, que na secção em matéria penal do STJ funcione uma secção especial para autorização de acesso à informação e a dados, composta por três juízes daquela secção penal, que serão anual e sucessivamente designados.

Prevê-se, ainda, que o Procurador-Geral da República designa anualmente um procurador-geral adjunto junto da secção especial.

Ao coletivo de juízes daquela secção competirá, de acordo com a norma do art. 5º A que se pretende aditar à Lei 30/84, a concessão da autorização prevista no art. 5º, a requerimento do procurador-geral adjunto junto da mesma secção, sem prejuízo do disposto na presente lei.

**5.1.1-** A opção do projeto de lei de criação de uma secção especial na secção em matéria penal do STJ constitui também, salvo melhor opinião, uma tentativa de ultrapassar as questões de desconformidade constitucional aduzidas no Acórdão do

<sup>24</sup> «A competência para a concessão da autorização prevista no artigo 5.º pertence ao coletivo de juízes da secção especial para autorização de acesso a informação e a dados do Supremo Tribunal de Justiça, a requerimento do procurador-geral-adjunto junto da mesma secção, sem prejuízo do disposto na presente lei».



Tribunal Constitucional 403/2015 quanto, por um lado, à natureza administrativa da Comissão de Controlo Prévio prevista no Decreto 426/XII da Assembleia da República, e de aproximar a natureza e finalidades de acesso às informações e dados de comunicações à delimitação constitucional de permissão desse acesso em matéria de processo criminal.

A opção não suscita particulares comentários, atentos os valores em causa e a criação, por esta via, em conjugação com o procedimento que se pretende instituir (art. 5° B), ainda que, como referido, com a introdução de alterações de pendor mais garantistico, e, bem assim, os pressupostos da concessão de autorização (n° 3 do art. 5°).

Por outro lado, a possível alternância anual dos juízes que compõem aquela secção afigura-se adequada a impedir considerações espúrias quanto às autorizações concedidas.

Quanto a este aspeto, afigura-se, no entanto, que a redação da norma do nº 3 poderá não permitir uma clara interpretação no sentido da possibilidade, ou não, de designação dos mesmos juízes para aquela secção especial, embora o vocábulo "sucessivamente" pareça indicar que a nomeação não deverá recair sobre os mesmos juízes que ali exerceram funções no período anual anterior.

Cremos dever ainda anotar que a denominação da secção especial – secção especial para autorização de acesso a informação e a dados – poderá revelar-se demasiado genérica e passível de suscitar dúvidas sobre a concreta abrangência das suas competências.

Nessa medida, e não se vislumbrando que se pretenda atribuir àquela secção outra competência que não seja a de apreciar e decidir os pedidos de autorização de acesso aos dados a que se refere o art. 5º da Lei 30/84, que se pretende aprovar, afigura-se ser de ponderar uma melhor concretização deste aspeto, sugerindo-se o aditamento do seguinte segmento na parte final do nº 2 do art. 47º:



- "2. Dentro da secção em matéria penal funciona uma secção especial para autorização de acesso a informação e a dados *pelos serviços de informação da República* ".
- **5.1.2.** A alteração proposta para o nº 3 do art. 66º da Lei 62/2013 não suscita, também, particulares comentários, sem prejuízo de se anotar que **não resulta claro da norma** proposta se a designação do procurador-geral adjunto junto da secção especial se deve fazer de entre os procuradores-gerais adjuntos que integram o quadro a que se refere o nº 1 do art. 66º, ou se pode ser feita de entre os demais procuradores-gerais adjuntos.

Por outro lado, não poderá também deixar de se salientar que no Supremo Tribunal de Justiça o Ministério Público é representado pelo Procurador-Geral da República (nº 1 alínea a) do art. 3º do Estatuto do Ministério Público) e que, nos termos do nº 1 do art. 13º do Estatuto, a coadjuvação e a substituição do Procurador-Geral Adjunto no STJ são asseguradas por procuradores-gerais-adjuntos, em número constante de quadro a fixar por portaria do Ministro da Justiça, sob proposta do Conselho Superior do Ministério Público.

Pelo que (e sem prejuízo do que adiante se referirá quanto à intervenção do Procurador-Geral da República no procedimento, e tendo apenas como referente a norma ora proposta), cremos que se justifica a clarificação da norma proposta quanto ao aspeto salientado, definindo-se especificamente se o Procurador-Geral Adjunto na mesma referido é designado de entre os Procuradores-Gerais Adjuntos que integram o quadro legal no STJ, ou se, ao contrário, está em causa designação de entre os demais procuradores-gerais adjuntos.

## 6. Art. 5° A- Competência para a concessão de autorização

**6.1.** Define-se que a autorização prevista no art. 5º pertence ao coletivo de juízes da secção especial do STJ, a requerimento do procurador-Geral adjunto junto da mesma secção, sem prejuízo do disposto na presente lei.



A previsão do art. 5º A suscita-nos dúvidas quanto ao alcance do segmento final " sem prejuízo do disposto na presente lei".

Na verdade, o que se define na norma é uma regra de competência para autorização de acesso a um concreto universo de dados e informações – que se pressupõe serem os previstos no art. 5°-, num regime de exclusividade de competência cujo exercício está sujeito a princípios e pressupostos expressamente previstos na lei.

Não se alcançando do regime que se pretende instituir, designadamente das normas procedimentais, qualquer exceção à competência atribuída à secção especial que se pretende criar.

Ausência de exceções que parece retirar sentido àquela ressalva legal.

O referido segmento só será compreensível se o que se pretende salvaguardar é o acesso a outros dados e informações que não integrem o âmbito do art. 5°.

O que convoca a questão, já acima enunciada, da incongruência entre a redação do nº 1 e os nº 2 e 3 do art. 5º e do nº 1 do art. 5º B quanto às informações e dados que estão efetivamente sujeitas a autorização judicial e ao respetivo procedimento.

Pelo que se afigura **dever ser ponderada a não manutenção do segmento referenciado,** ou, a ser mantido, clarificar-se a matéria relativa às concretas informações e dados que estão sujeitas a autorização judicial e, que, nessa estrita medida, integram a competência da secção especial do STJ.

**6.2.** Define-se que a competência para a concessão de autorização é exercida a requerimento do procurador-geral adjunto junto da secção especial.

Por sua vez, o nº 1 do art. 5º B estabelece que o pedido de acesso *é apresentado por escrito pelos Diretores do SIS ou do SIED* ao procurador-geral adjunto junto daquela secção especial.



Da conjugação destas duas normas não resulta claro se o procurador-geral adjunto que recebe o pedido e requer a concessão de autorização deve, no respetivo requerimento, tomar posição de natureza substantiva sobre o pedido formulado, quer quanto à completude do pedido, por referência aos elementos que obrigatoriamente deve conter (descritos nas diversas alíneas do nº 1 do art. 5º B), quer quanto à justificação do mesmo, designadamente por referência aos pressupostos substantivos previstos no nº 3 do art. 5º, quer, ainda, quanto ao sentido da decisão a proferir.

A intervenção de um magistrado do Ministério Público no procedimento, de natureza judicial, mostra-se essencial no sistema pretendido. Não podendo, porém, essa intervenção deixar de assumir natureza substantiva, e não apenas de mera formalidade.

Pelo que se justifica que a sua intervenção seja densificada, no sentido de se prever a emissão de pronúncia quanto ao pedido formulado, sua conformação legal e procedimental, justificação, indispensabilidade, adequação e proporcionalidade aos fins pretendidos. Sugestão de redação que adiante se efetuará.

6.2.1. Sem prejuízo da apreciação feita quanto à concreta proposta do projeto de lei e à necessidade de clarificação e densificação nos termos sugeridos, entende-se que o sistema previsto poderá ser reponderado no sentido de prever a intervenção do Procurador-Geral da República no procedimento de autorização, tal como sugerido na análise da Proposta de Lei 79/XIII, relativa à mesma matéria e em discussão conjunta na Assembleia da República.

Assim, de modo a permitir uma apreciação integrada, face, desde logo, ao sistema procedimental estruturado ali proposto, permitimo-nos, com a devida vénia, remeter para a análise e sugestões feitas a propósito daquela Proposta de Lei relativamente à intervenção do Ministério Público /Procurador/a-Geral da República no procedimento de autorização de acesso a dados de comunicações pelo SIRP.



## 7. Art. 5º B- Procedimento do pedido de autorização

- **7.1.** O projeto pretende adicionar um novo normativo artigo 5.º-B que regula o "procedimento do pedido de autorização", em síntese, nos seguintes termos:
- **1.º** O pedido é efetuado pelos Diretores do SIS ou do SIED ao Procurador-Geral Adjunto junto do Supremo Tribunal de Justiça contendo;
- **a.** A indicação concreta da ação operacional a realizar e das medidas requeridas;
- **b.** Os factos que suportam o pedido, finalidades que o fundamentam e razões que aconselham a adoção das medidas requeridas;
- **c.** A identificação da pessoa ou pessoas, caso sejam conhecidas, envolvidas nos factos referidos na alínea anterior e afetadas pelas medidas e indicação do local onde as mesmas devam ser realizadas;
- **d.** A duração das medidas requeridas, que não pode exceder o prazo máximo de três meses, prorrogáveis mediante autorização expressa.
- **2.º** O PGA apresenta o pedido ao STJ que decide em 48 horas ou, em caso de urgência, em 24 horas
- **3.º** O Secretário-Geral ordena a destruição imediata de todos os dados e informação recolhidos sempre que não tenham relação com o objeto ou finalidades da mesma.
- **4.º** O STJ pode determinar o cancelamento de quaisquer procedimentos de acesso a informação e a dados.

Como acima se referiu, este procedimento aplica-se aos dados previstos no n.º 2 do artigo 5.º, ou seja, "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".

Para além do diferente enquadramento constitucional – como acima foi analisado – e que, só por si, justifica um controlo mais apertado no que se refere à obtenção de dados de tráfego e localização celular das comunicações, na prática existe uma diferença fundamental entre esta e a obtenção de informação bancária e fiscal. Enquanto estes últimos são fornecidos, em regra, num momento único, os dados de comunicações, podendo também referir-se a um período já decorrido, podem implicar a recolha para o futuro, durante o período pretendido.

Esta última vertente – que os assemelha a "escutas" - apela a um controlo jurisdicional mais regular, devendo tomar-se como referência o procedimento de fiscalização judicial do acesso a dados de telecomunicações - cuja formulação atual decorreu de uma larga jurisprudência constitucional que tem sedimentado as regras necessárias para que se possa considerar a fiscalização efetiva.

Assim, no que se refere aos dados de comunicações a recolher durante um certo período, a principal lacuna do projeto reside na ausência de acompanhamento periódico dos dados recolhidos.

Embora o regime previsto no artigo 188.º do CPP se aplique aos dados de conteúdo, sendo a obtenção e junção aos autos de dados de localização ou de tráfego regulados pelo n.º 2 do artigo 189º do mesmo diploma, entendemos que existem dois elementos que devem estar presentes no caso em análise para uma efetiva fiscalização judicial do acesso aos dados de comunicações:

- a) A fiscalização periódica dos dados obtidos;
- b) A competência judicial para ordenar a destruição dos dado alheios às finalidades visadas.



Nos termos dos n.º 1, 3 e 4 do artigo 188.º do CPP "O órgão de polícia criminal que efectuar a intercepção e a gravação a que se refere o artigo anterior lavra o correspondente auto e elabora relatório no qual indica as passagens relevantes para a prova, descreve de modo sucinto o respectivo conteúdo e explica o seu alcance para a descoberta da verdade" e "leva ao conhecimento do Ministério Público, de 15 em 15 dias a partir do início da primeira intercepção efectuada no processo, os correspondentes suportes técnicos, bem como os respectivos autos e relatórios" que, por sua vez, "leva ao conhecimento do juiz os elementos referidos no número anterior no prazo máximo de quarenta e oito horas".

Esta fiscalização periódica no âmbito do período de autorização geral - de 3 meses prorrogáveis - é absolutamente essencial para que o tribunal confirme se os pressupostos que determinaram o acesso aos dados - constantes da fundamentação do pedido e que configuram suspeitas - se verificam efetivamente.

Se, uma vez recebidos os dados, se concluir que os mesmos não se relacionam com as finalidades visadas, terá de se permitir ao tribunal ordenar a imediata cessação do respetivo acesso.

No mesmo sentido, a elaboração de um relatório pela entidade que recebe os dados de comunicações é essencial para que a decisão judicial possa ser esclarecida. Veja-se que os dados obtidos podem ser apenas listagens de números e de comunicações as quais, sem um esclarecimento pelos serviços, podem ser ininteligíveis, frustrando o controlo jurisdicional.

Associados a esta apresentação periódica dos dados encontram-se dois poderes fundamentais que devem ser atribuídos expressamente ao tribunal: a destruição imediata dos suportes técnicos e relatórios injustificados e, se for o caso, a imediata cessação de acesso aos dados, em termos similares aos previstos no n.º 6 do artigo 188.º.



Este poder não pode ser atribuído ao Secretário-Geral, ou seja, à entidade fiscalizada, sob pena de não existir qualquer fiscalização de eventuais abusos ou desvios às finalidades que determinaram a autorização.

Por fim, e como já acima referido, entendemos que o Ministério Público não deverá ter uma mera função formal de "transmissão do pedido", devendo assumir integralmente a sua função de controlo da legalidade, pronunciando-se sobre qualquer pedido de acesso a dados, bem como sempre que se justificar a destruição de dados ou a cessação do respetivo acesso.

Assim, sem prejuízo do que acima se referiu quanto à intervenção do Procurador-Geral da República no procedimento, e que se assinalará igualmente na sugestão que se segue, sugerimos que o artigo 5.º B tenha a seguinte redação:

Artigo 5.°-B

(Procedimento do pedido de autorização)

- 1 O pedido de acesso às informações e aos dados a que alude o n.º 2, do artigo 5.º, é apresentado por escrito pelos Diretores do SIS ou do SIED ao procurador-geral adjunto junto da secção especial para autorização de acesso a informação e a dados do Supremo Tribunal de Justiça e contém os seguintes elementos:
- a) Indicação concreta da ação operacional a realizar e das medidas requeridas;
- b) Factos que suportam o pedido, finalidades que o fundamentam e razões que aconselham a adoção das medidas requeridas;
- c) Identificação da pessoa ou pessoas, caso sejam conhecidas, envolvidas nos factos referidos na alínea anterior e afetadas pelas medidas e indicação do local onde as mesmas devam ser realizadas;



- d) Duração das medidas requeridas, que não pode exceder o prazo máximo de três meses, prorrogáveis mediante autorização expressa.
- 2 O Procurador-Geral Adjunto/O Procurador-Geral da República apresenta de imediato o pedido, juntamente com o seu parecer, ao coletivo de juízes que profere decisão de concessão ou de denegação da autorização por despacho fundamentado, proferido no prazo máximo de 48 horas.
- 3 Em situações de urgência, devidamente fundamentadas no pedido dos serviços de informações, pode ser solicitada a redução para 24 horas do prazo previsto no número anterior.
- 4 No que se refere aos dados de dados de tráfego, de localização ou outros dados conexos das comunicações, os serviços que procedem à análise dos dados e informações recebidas lavram o correspondente auto e elaboram relatório no qual descrevem de modo sucinto o respetivo conteúdo e, fundamentadamente, explicam o seu alcance para as finalidades que determinaram o respetivo acesso.
- 5 Os autos e relatórios previstos no número anterior são remetidos ao Procuradorgeral adjunto/O Procurador-Geral da República de 15 em 15 dias a partir do início da primeira receção de dados e informações que os apresenta ao coletivos de juízes que determina, ouvido o Ministério Público, a destruição imediata dos dados e informações alheios às finalidades que determinaram o respetivo acesso.
- 6 O procedimento previsto no presente artigo é coberto pelo regime do segredo de Estado nos termos do artigo 32.º.
- 7 Sempre que o Secretário-Geral constata que os dados e informação recolhidos não tenham relação com o objeto ou finalidades da mesma apresenta de imediato ao STJ para os efeitos previstos no n.º 5 do presente normativo.
- 8 Por decisão do coletivo de juízes, pode ser determinado o cancelamento de quaisquer procedimentos de acesso a informação e a dados previstos no n.º 2 do artigo 5.º, bem como



participados à Comissão de Fiscalização de Dados do SIRP os elementos conducentes à destruição imediata dos respetivos dados ou informações.

## 8. Art. 5º C- Transmissão, tratamento, manutenção e destruição das informações e dados

**8.1**. O projeto pretende adicionar um novo normativo - artigo 5.º C – que regula o modo de transmissão, tratamento, manutenção e destruição das informações e dados.

Desde logo, cumpre referir que, ao se mencionar "dados" naturalmente se está a excluir a aplicação deste normativo à informação bancária e fiscal.

Assim, no que se refere à transmissão dos dados de comunicações, **nada temos a opor** a que se recorra ao regime previsto na Lei 32/2008, de 17 de julho, e legislação complementar, até por ser a estrutura existente de relacionamento entre o sistema judicial e os operadores de telecomunicações privados.

No entanto, para melhor clarificação e segurança jurídica, sugerimos que se mencione expressamente o regime legal acima referido.

No que se refere à manutenção e destruição das informações e dados, trata-se de uma vertente essencial do quadro legal do tratamento dos dados que, em nosso entender, não pode simplesmente ser remetido para a lei geral.

Reconhecendo que os dados obtidos ao abrigo deste sistema legal, ao serem incorporados nas bases de dados gerais dos sistemas de informação, são abrangidos pelo sistema geral de preservação e destruição dos dados, revela-se essencial, salvo melhor entendimento, que o Supremo Tribunal de Justiça, tal como já defendido no comentário ao artigo 5.º B, no encerramento do período de obtenção dos dados determine a imediata destruição daqueles que não se adequam às finalidades a que se destinaram.



Apenas aos restantes – cuja pertinência para as finalidades a que se destinaram foi validada pelo tribunal - se devem aplicar as regras gerais que atribuem aos próprios órgãos dos sistemas de informação e às respetivas entidades de fiscalização a responsabilidade de determinar a preservação e destruição dos dados.

Assim, sugerimos a seguinte redação da norma:

Artigo 5.º-C

(Transmissão, tratamento, manutenção e destruição das informações e dados)

- 1. A transmissão dos dados previstos no n.º 2 do artigo 5.º é feita por comunicação eletrónica, de acordo com o disposto na Lei 32/2008, de 17 de julho, e legislação complementar, que estabelecem os termos das condições técnicas e de segurança em que se processa a comunicação eletrónica para efeitos da transmissão de dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado.
- 2 Sem prejuízo do disposto no número anterior, as entidades às quais incumbe garantir a proteção e segurança dos dados devem assegurar-se que a transmissão dos dados previstos no n.º 2 do artigo 5.º respeita 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.
- 3 O disposto nos números anteriores não prejudica a observância dos princípios nem o cumprimento das regras aplicáveis previstos nas Leis n.ºs 67/98, de 26 de Outubro e 41/2004, de 18 de Agosto.
- 4 A qualquer momento e, obrigatoriamente, no final do período de recolha dos dados, o STJ determina, oficiosamente ou a requerimento do procurador-geral



adjunto, a destruição daqueles que não sejam estritamente necessários para os fins a que se destinam.

5. Sem prejuízo do acompanhamento permanente da Comissão de Fiscalização de Dados do SIRP e do disposto nos números anteriores, as demais regras sobre a transmissão, o tratamento, a manutenção e a destruição das informações e dados identificados na presente Lei são estabelecidas por legislação especial".

Lisboa, 2 de junho de 2017