S. R.

PROCURADORIA-GERAL DA REPÚBLICA

Comissão de Fiscalização de Dados do Sistema de Informações da República Portuguesa

Exmo. Senhor
Presidente da Comissão Parlamentar de Assuntos Constitucionais, Direitos, Liberdades e Garantias
Professor Dr. Pedro Bacelar de Vasconcelos

Lisboa, 15 de maio de 2017

Assunto: Parecer da "Comissão de Fiscalização de Dados do SIRP" sobre o Projecto de Lei nº 480/XIII/2ª(CDS-PP)

Satisfazendo o solicitado, remeto a VªExª parecer emitido pela "Comissão de Fiscalização de Dados do SIRP" sobre o Projecto de Lei nº 480/XIII/2ª(CDS-PP).

Informo que este parecer foi já antes enviado, a essa Comissão, por e-mail de 15/5.

575783
558 17052017

Com os meus melhores cumprimentos, Bem. pessoais,

(Adriano Cunha – Presidente da "Comissão de Fiscalização de Dados do SIRP")

Comissão de Fiscalização de Dados do
Sistema de Informações da República Portuguesa

Parecer 1/2017

Assunto: Apreciação do Projecto de Lei 480/XIII/2ª (CDS-PP)

A – Considerações preliminares

1. Pedido que determinou a elaboração do presente parecer

Através de mensagem electrónica recebida em **6 de Abril de 2017**, da **Comissão Parlamentar de Assuntos Constitucionais, Direitos, Liberdades e Garantias** da **Assembleia da República**, foi solicitada, a esta **Comissão de Fiscalização de Dados**, pelo **Presidente** da mesma Comissão da Assembleia da República, por **ofício** nº **349/1ª – CACDLG/2017**, datado de **5 de Abril de 2017**, a emissão de **parecer escrito** sobre o **Projecto de Lei nº 480/XIII/2ª (CDS-PP)**, relativo a «*Acesso a dados de tráfego, de localização ou outros dados conexos das comunicações por funcionários e agentes dos serviços de informações da República portuguesa*».

Pretendia-se, por outro lado, que a **Comissão de Fiscalização de Dados** apreciasse a referida iniciativa legislativa «*com a maior brevidade possível*».

Acontece, porém, que os meios de comunicação social se fizeram igualmente eco da possível entrega de um **projecto do PSD**, bem como de uma **Proposta de Lei do Governo** sobre o mesmo assunto, pelo que esta Comissão aguardou algum tempo pela respectiva apresentação.

Como tal, porém, não sucedeu até ao momento, então esta Comissão de apreciar, desde já, o **Projecto de Lei 480/XIII-2ª**, apresentado pelo **CDS-PP**, para não atrasar desnecessariamente a entrega do parecer solicitado pela Comissão **Parlamentar de Assuntos Constitucionais, Direitos, Liberdades e Garantias** da **Assembleia da República**.

Em seguida se indica, pois, a posição desta Comissão sobre o respectivo articulado, tendo fundamentalmente em conta as competências que a esta Comissão estão, por lei, atribuídas.

Este, pois, o **objecto** do presente Parecer.

2. Motivos determinantes do Projecto de Lei 489/XIII-2ª

2.1. O **Projecto de Lei 489/XIII-2ª** pretende **regular** a matéria de "*Acesso a dados de tráfego, de localização ou outros dados conexos das comunicações por funcionários e agentes dos serviços de informações da República Portuguesa*".

Um dos motivos determinantes da sua apresentação é, por um lado, procurar responder, pelo menos a algumas das preocupações expressas no **Acórdão 403/15**, de 27 de Agosto, do **Tribunal Constitucional**, que se pronunciou «*pela inconstitucionalidade da norma do n.º 2 do artigo 78.º do Decreto n.º 426/XII da Assembleia da República, que* "Aprova o Regime Jurídico do Sistema de Informações da República Portuguesa", *por violação do n.º 4 do artigo 34.º da CRP*».

Por outro lado, o Projecto de Lei em apreciação pretende acautelar formas eficazes de **prevenção** e **combate ao terrorismo** e **à criminalidade altamente organizada de natureza transnacional**.

2.2. A **Exposição de Motivos** do **Projecto de Lei 480/XIII-2ª** refere, a este propósito, de forma particularmente significativa (ênfase desta Comissão):

> "*O **acesso pelos serviços de informações da República Portuguesa a meios operacionais** foi consagrada expressamente, pela primeira vez, em **iniciativa legislativa do XIX Governo Constitucional** que visava aprovar um **novo regime jurídico do Sistema de Informações da República Portuguesa**, idealmente consagrando em forma de lei determinadas garantias fundamentais, previstas quer na Carta Europeia dos Direitos Fundamentais quer na Convenção Europeia dos Direitos do Homem.*
>
> *Idealmente, dizíamos, pois **assim não entendeu o Tribunal Constitucional, que considerou inconstitucional a formulação da norma que previa o acesso a dados conservados pelas operadoras de telecomunicações - os denominados metadados** -, e cuja **utilidade**, no que concerne aos **crimes de sabotagem, espionagem, terrorismo**, e **sua proliferação**, e **criminalidade altamente organizada de natureza transnacional é inegável**.*
>
> *Sucede que **este acesso continua a ser incontornável**, seja pelo seu papel fundamental no contexto da **Estratégia Nacional de Combate ao Terrorismo**, aprovado pela **Resolução do Conselho de Ministros n.º 7-A/2015**, de 20 de fevereiro, seja na **prevenção de ameaças à segurança nacional e europeia em matéria de terrorismo**.*
>
> *E a verdade é que, após a prolação do **Acórdão n.º 403/2015**, de 27 de Agosto, **não houve qualquer outra iniciativa legislativa nesse sentido, apesar de as ameaças não terem diminuído**, como bem assinalou o **Conselho de Fiscalização do Sistema de Informações da República Portuguesa** (CF-SIRP), quer no parecer relativo ao ano de 2015 quer no correspondente ao primeiro semestre de 2016 (...).*
>
> *E não é menos verdade que, como também sublinha o CF-SIRP,* "as ameaças que os serviços de informações visam detetar e prevenir não desapareceram nem diminuíram", *insistindo na* "grande conveniência em dotar os serviços, em particular o SIS" ***de meios que lhe permitam detetar tais ameaças**, dentro de um espírito de "integral respeito dos*

direitos, liberdades e garantias" e de "todos os limites constitucionais e legais à atuação dos serviços".

Por outro lado, também é muito importante que os ***serviços tenham capacidade para cooperar, em igualdade de circunstâncias, com serviços congéneres*** *dos nossos parceiros europeus - e dos demais países "que respeitam as exigências do Estado de direito democrático" -* ***na deteção e prevenção de ameaças terroristas****.*

De resto, a ***exposição europeia ao terrorismo*** *há muito que deixou de estar no domínio das hipóteses ou das probabilidades –* ***é um facto, uma realidade que a Europa tem de enfrentar e, sobretudo, prevenir e combater****, e Portugal não é exceção.*

Apesar de, até hoje, Portugal ter tido a felicidade de escapar a atos terroristas, a ***ameaça paira também sob Portugal*** *e pode acontecer quando menos se espera, onde menos se espera. Por isso mesmo, é essencial dotar o país de todos os mecanismos ao seu alcance para o evitar,* ***trabalhando na prevenção e repressão do terrorismo****.*

Acresce o facto de os ***movimentos e atos terroristas terem abandonado as formas mais convencionais de se expressarem*** *– seja porque já não se concentram numa determinada reivindicação ou causa específica, seja porque deixaram de se dirigir a alvos facilmente identificáveis e concretos, seja porque o modus operandi deixou de ser padronizado, seja porque deixou de se fundar numa organização concentrada e particularizada, agora muito mais pulverizada e assente numa base inorgânica.* ***Razão por que se torna bastante mais difícil o seu combate e, por isso mesmo, bastante mais exigente a sua prevenção****."*

3. Posição desta Comissão quanto às preocupações subjacentes ao Projecto de Lei em apreciação

3.1. É este, naturalmente, um conjunto de preocupações a que esta Comissão é sensível.

Por um lado, o **fenómeno do terrorismo** assumiu, nos últimos tempos, em solo europeu, uma **particular virulência**, com inúmeras vítimas a lamentar em sucessivos atentados perpetrados em países diversos, próximos ou distantes entre si.

Não se trata, pois, de acautelar a ocorrência de possíveis situações abstractas de atentados, **mas de prevenir a sua efectiva realização, com um tempo de reacção cada vez mais encurtado** por parte das entidades encarregues da sua repressão.

3.2. Por outro lado, os **agentes** de actos criminosos desta natureza **deslocam-se cada vez mais rapidamente através do solo europeu**, planeando, por vezes, as suas **acções terroristas** num pais, deslocando-se através de outro(s) e acabando por realizá-las ainda num terceiro país.

O **combate** a este tipo de actividade criminosa deixou, por isso, **de ser possível de assegurar isoladamente**, implicando uma **cooperação estreita** entre diferentes entidades, designadamente **Serviços de Informações** e **autoridades judiciárias** de diversos países, particularmente europeus.

Ter-se-á, também, de ter em conta que o **tipo de atentados** desta natureza se tem grandemente **diversificado, quanto ao seu *modus operandi***, sendo difícil, por isso, prever a **forma** que poderão assumir no futuro.

Do mesmo modo, assiste-se, ultimamente, à intervenção de **pequenas células de terroristas**, ou mesmo de **actores isolados**, o que torna particularmente difícil a sua **detecção antecipada** e **possível neutralização**, sendo frequente que os agentes tenham a **nacionalidade**, ou **residam** nos países em que praticam a sua actividade criminosa, ou, então, em **países limítrofes**, o que naturalmente facilita e permite a sua rápida **mobilidade transfronteiriça**.

3.3. Ora, tudo isto exige uma **partilha estreita e permanente de informação não só entre Serviços de Informações, mas,** sobretudo, **entre estes e as autoridades judiciárias,** não só para garantir uma adequada **prevenção** da ocorrência de atentados, mas também, quando estes infelizmente ocorram, capazes de garantir a adequada e rápida **repressão** e **punição** dos seus responsáveis.

3.4. Sendo certo, por outro lado, que se revela de fundamental importância para a localização e acompanhamento das deslocações de eventuais suspeitos, por território europeu, o **acesso a um determinado conjunto de dados por parte dos Serviços de Informações europeus**, nos quais os Serviços de Informações portugueses se integram, designadamente **dados de tráfego** relativos a comunicações em que intervenham.

Ora, a este propósito, convém ter presente que os **Serviços de Informações portugueses** são, neste momento, de todos aqueles que integram o chamado **Clube de Berna** (grupo informal de serviços de informações de segurança europeus), integrado por **todos os países da União Europeia**, a **Noruega** e a **Suíça, os únicos em relação aos quais a lei não prevê a possibilidade de acesso a dados de tráfego**, também por vezes chamados de **metadados**, o que deixa os mesmos Serviços numa situação de particular vulnerabilidade.

A este propósito, a **eficácia** de uma **cooperação efectiva de serviços de informações europeus** poderá resultar grandemente prejudicada por uma tal limitação, ainda que de natureza constitucional, uma vez que a força de uma tal cooperação europeia depende, no fundo, da capacidade de resiliência do seu elo mais fraco.

Compreende-se, por isso, a preocupação do Projecto de Lei 480/XIII-2ª em procurar superar os constrangimentos com que, neste domínio, se confrontam os Serviços de Informações nacionais.

B – O Acórdão 403/15 do Tribunal Constitucional

4. Preocupações expressas no Acórdão 403/15 do Tribunal Constitucional

4.1. Antes de entrar na análise do **Projecto de Lei 480/XIII-2ª**, importa referir algumas das principais preocupações expressas no **Acórdão 403/15** do Tribunal Constitucional, a que o mesmo Projecto procura dar resposta.

Será, assim, mais fácil avaliar, posteriormente, se as alterações legislativas agora propostas permitirão, eventualmente, ultrapassar as objecções formuladas pelo mesmo Tribunal Constitucional ao **Decreto n.º 426/XII** da Assembleia da República, que «*Aprova o Regime Jurídico do Sistema de Informações da República Portuguesa*».

É o que se procurará fazer de seguida.

4.2. Convirá ter em conta, a este propósito, que o mesmo aresto, datado de **27 de Agosto de 2015**, foi votado por apenas **7 dos Juízes Conselheiros** que integravam a então composição do Tribunal Constitucional.

Teve, ainda, o mesmo aresto, **2 declarações de voto**: uma delas (Conselheira Maria Lúcia Amaral), votou a decisão, mas não alguns dos respectivos fundamentos, a outra (Conselheiro José António Teles Pereira), votou contra o entendimento que fez vencimento.

Por outro lado, cabe salientar, também, que **4 dos Juízes Conselheiros** que participaram na votação do referido Acórdão já terminaram o seu mandato no Tribunal Constitucional, apenas permanecendo, por isso, **3 dos Juízes Conselheiros** que intervieram na sua discussão.

É, por isso, **difícil antecipar** qual a posição que o Tribunal Constitucional virá a tomar, na sua actual composição, em matéria tão delicada quanto esta, se a mesma matéria voltar a ser submetida à sua apreciação.

4.3. O **Tribunal Constitucional** começou por delimitar o **objecto** do pedido de fiscalização preventiva de constitucionalidade, que então lhe foi submetido, da seguinte forma (cfr. nº 6 do Acórdão 403/15):

> "*...a norma, constante do n.º 2 do artigo 78.º do Decreto n.º 426/XII, nos termos da qual, os oficiais de informações do SIS e do SIED podem, para efeitos do disposto na alínea c) do n.º 2 do artigo 4.º, e no seu exclusivo âmbito, aceder a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização, sempre que sejam necessários, adequados e proporcionais, numa sociedade democrática, para cumprimento das atribuições legais dos serviços de informações, mediante a autorização prévia e obrigatória da Comissão de Controlo Prévio, na sequência de pedido devidamente fundamentado.*"

Uma tal delimitação permitiu-lhe concluir, desde logo (cfr. *ibidem*):

- o pedido de fiscalização preventiva da constitucionalidade da normação contida no n.º 2 do artigo 78.º **não abrangia a possibilidade de acesso** dos oficiais de informações do SIS e SIED **a informação bancária e fiscal**, prevista no Decreto n.º 426/XII, pelo que a mesma não foi, então, apreciada;

- haver uma **relação de correspondência** entre os dados a que se pretendia aceder e aqueles compreendidos no conceito de **dados de tráfego**, tal como acolhido na Lei 41/2004, de 18 de Agosto;

- o tratamento dos ***dados de localização***, que fornecem a posição geográfica do equipamento terminal de um utilizador e que se destinam a permitir a transmissão das comunicações, mormente no âmbito de sistemas de telecomunicações móveis, **encontrava-se abrangido pelo conceito de *dados de tráfego***, aplicando-se-lhes a mesma Lei 41/2004;

- diferentemente, **outros *dados de localização***, decorrentes da capacidade de tratamento que as redes móveis digitais possam deter, previstos no artigo 7.º da Lei 41/2004, **porque não conexos com a transmissão de comunicações, não se encontravam compreendidos na norma objeto do pedido** e, correspondentemente, no âmbito da cognição do Tribunal.

4.4. O Acórdão 403/15 traçou, em seguida (cfr. nº 7 do mesmo aresto), a evolução histórica do **Sistema de Informações da República Portuguesa (SIRP)**, referindo que a respectiva actividade está especificamente limitada por alguns **princípios fundamentais**, inscritos nos nºs 1 e 3 do art. 3º e nº 1 do art. 4º da Lei 30/84 (Lei Quadro do SIRP):

- **princípio da constitucionalidade e da legalidade** ("*a atividade dos serviços de informações está sujeita ao escrupuloso respeito pela Constituição e pela lei, designadamente em matéria de proteção dos direitos fundamentais das pessoas, especialmente frente à utilização de dados informatizados*");

- **princípio da exclusividade** ("*a atividade dos serviços está rigorosamente limitada às suas atribuições, não podendo desenvolver uma atividade de produção de informações em domínio que não lhe tenha sido concedido*"); e, por último,

- **princípio da especialidade** ("*a atividade dos serviços de informações reduz-se ao seu estrito âmbito, não podendo a sua atividade confundir-se com a atividade própria de outros organismos, como no domínio da atividade dos tribunais ou da atividade policial*").

Salientou, por outro lado, o Tribunal Constitucional, a importância dada à protecção dos direitos, liberdades e garantias dos cidadãos.

Referiu, ainda, «... *que a separação da atividade de informações das atividades policial e de investigação criminal resulta, além de fatores históricos, de princípios e valores eminentes da nossa ordem jurídica*».

4.5. O **Acórdão 403/15** debruçou-se, mais adiante, sobre o **pensamento legislativo** que esteve na base da apresentação do Decreto 426/XII (cfr. nº 8 do mesmo aresto), que apresenta preocupações idênticas às do Projecto de Lei agora em apreciação do CDS-PP, como se viu já (cfr. supra nº 2 deste Parecer) (ênfase desta Comissão):

> "*No contexto da recente **Estratégia Nacional de Combate ao Terrorismo**, aprovado pela **Resolução do Conselho de Ministros n.º 7-A/2015**, de 20 de fevereiro, e dos **desafios colocados pelas novas ameaças à segurança nacional**, surge como incontornável o **acesso a meios operacionais consagrados pela primeira vez de modo transparente e expresso na lei positiva**, indo ao encontro do **padrão de garantias** quer*

da Carta Europeia dos Direitos Fundamentais quer da Convenção Europeia dos Direitos do Homem.

Neste contexto, e ***em linha com a maior parte dos Estados-Membros da União Europeia, prevê-se o acesso aos metadados****, isto é, o* ***acesso a dados conservados pelas operadoras de telecomunicações, o que se rodeia de especiais regras para salvaguardar integralmente os direitos dos cidadãos, em especial o direito à privacidade****. Efetivamente, admite-se, no artigo 78.º da presente proposta lei, a* ***possibilidade de acesso a dados de base, de localização e de tráfego****, eventualmente considerados «dados pessoais» para os efeitos do artigo 35.º da Constituição (CRP),* ***mas não a «ingerência nas comunicações», prevista no n.º 4 do artigo 34.º da CRP, do domínio do processo penal*** *(âmbito, este, vedado aos serviços de informações, indiretamente, atentos os limites que a lei impõe à atividade do SIRP, ao impedir os serviços de informações de desenvolver ações próprias dos tribunais, do Ministério Público e das polícias).*

O regime de acesso garante a finalidade vinculada à prevenção de fenómenos graves*, como o* ***terrorismo****, a* ***espionagem****, a* ***sabotagem*** *e a* ***criminalidade altamente organizada****, e, mesmo nestes casos, é* ***limitada ao estritamente adequado, necessário e proporcional numa sociedade democrática****. Para o efeito, é criada uma entidade própria, a* ***Comissão de Controlo Prévio*** *(cfr. os artigos 35.º a 38.º), que concede a autorização prévia do acesso à informação e dados necessários, numa dada operação, segundo um exigente procedimento legal, que visa a sindicância do acesso a dados pessoais que possa por em causa a reserva da intimidade da vida privada, a efetuar por três juízes.*

O que se pretende é, não um acesso a conteúdos de comunicações *(escritas ou de voz),* ***por intrusão ou ingerência nas comunicações, mas o acesso autorizado a dados (de base, de localização e de tráfego), que são solicitados às entidades legitimamente responsáveis pelo seu tratamento, que os fornecem por determinação, e apenas nesse***

*caso, **daquela comissão de juízes**, nos termos da presente lei, matéria que tem melhor inserção sistemática em sede do artigo 78.º (Acesso a dados e informação)."*

4.6. Em seguida, o **Acórdão 403/15** aborda o conceito de **dados resultantes do serviço de telecomunicações** (cfr. nº 9 do mesmo aresto), dividindo-os, de acordo com doutrina firmada pelo **Conselho Consultivo da Procuradoria-Geral da República** e por jurisprudência consolidada do **Tribunal Constitucional**, em **três categorias** (ênfase desta Comissão):

« *(...) os dados relativos à conexão à rede, ditos **dados de base**; os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência), **dados de tráfego**; dados relativos ao conteúdo da comunicação ou da mensagem, **dados de conteúdo***»

Considerou, ainda, no que tangia ao objecto do pedido que lhe havia sido submetido, que se tratava fundamentalmente de **dados de tráfego** e de **dados de localização** (cfr. *ibidem*) (ênfase desta Comissão):

"*Ora, importa enquadrar os dados em causa na norma objeto do presente recurso numa das categorias enunciadas. Reportando-se os mesmos aos "**dados de tráfego**", "**dados de localização**" ou a outros "**dados conexos" das comunicações** - como a própria lei enuncia - **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**, dúvidas não restam que os mesmos se podem qualificar como **dados de tráfego**, por respeitarem «aos próprios elementos funcionais da comunicação, reportando-se à direção, destino, via e trajeto de uma determinada mensagem». São dados, pois, que **identificam** ou **permitem identificar a comunicação** e, uma vez*

conservados, ***possibilitam a identificação das comunicações entre emitente e destinatário, a data,*** *o* ***tempo*** *e a* ***frequência das ligações efetuadas.***

No que toca aos ***dados de localização,*** *consistem em dados tratados numa rede de comunicações eletrónicas que indiquem a* ***posição geográfica do equipamento terminal*** *de um utilizador de um serviço de telecomunicações, podendo incidir sobre a latitude, longitude ou altitude do equipamento, sobre a direção da deslocação, sobre a identificação da célula de rede em que o equipamento está localizado em determinado momento e sobre a hora de registo da informação de localização. Como acima se referiu, ao delimitar o objeto do recurso, tem-se considerado que* ***os mesmos estão também incluídos no conceito mais amplo de "dados de tráfego"*** *(assim, Catarina Sarmento e Castro, Direito da Informática, Privacidade e Dados Pessoais, Almedina, 2005, pág. 181). E é nesse sentido que a* ***Lei n.º 32/2008,*** *de 17 de julho, que regula a conservação e transmissão dos dados de tráfego e de localização,* ***reserva a mesma disciplina jurídica para ambos.***"

4.7. O **Acórdão 403/15** considera, mais adiante, que, quer a **ingerência nos dados de conteúdo, quer de tráfego**, acaba por levantar problemas no que respeita à eventual **violação da privacidade** das pessoas envolvidas (cfr. nº 12 do mesmo aresto) (ênfase da Comissão):

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

Com efeito, ***mesmo que não haja acesso ao conteúdo, a interconexão entre dados de tráfego pode fornecer um perfil complexo e completo da pessoa em questão*** *– com quem mais conversa, que lugares frequenta, quais os seus horários, etc. (...)*

Isto mostra claramente que ***a manipulação ilegal ou ilegítima do conteúdo e das circunstâncias da comunicação pode violar a privacidade dos interlocutores intervenientes****, atentando ou pondo em risco esferas nucleares das pessoas, das suas vidas, ou dimensões do seu modo de ser e estar. De sorte que* ***a possibilidade de se aceder aos dados das comunicações colide com um conjunto de valores associados à vida privada que fundamentam e legitimam a proteção jurídico-constitucional.***"

Debruça-se, em seguida, sobra a jurisprudência constitucional em matéria do **direito à reserva sobre a intimidade da vida privada** (cfr. nº 12 do mesmo aresto) e do chamado **direito à autodeterminação comunicativa** (cfr. nº 13 do mesmo aresto).

4.8. Quanto a este último direito, acaba por concluir que a «... *autodeterminação comunicativa é protegida no artigo 34.º da CRP através da inviolabilidade das comunicações*» (cfr. nº 14 do Acórdão 403/15).

E, mais adiante, considera que a proibição do nº 4 do art. 34º da Constituição (cfr. nº 15 do mesmo aresto) **abrange não só os dados de conteúdo, mas também os de tráfego**, embora já não eventualmente os **de base e de localização de equipamento** (ênfase desta Comissão):

"*Ora, há um largo consenso na doutrina e na jurisprudência, de resto não se conhece posição contrária, no sentido de* ***se incluir os dados de tráfego no conceito de comunicações constitucionalmente relevante para a proibição de ingerência****. Quer dizer:* ***o âmbito de proteção do artigo 34.º, n.º 4 abrange não apenas o conteúdo das telecomunicações, mas também os dados de tráfego****. (...)*

O Tribunal Constitucional também já teve oportunidade de se pronunciar expressamente sobre este aspeto, ***tendo também equiparado a proteção dos dados de tráfego à proteção constitucionalmente concedida aos dados de conteúdo****. (...)*

Já quanto aos dados de base *(v.g. número de telefone, endereço eletrónico, contrato de ligação à rede)* ***e aos dados de localização de equipamento, quando não dão suporte a uma concreta comunicação, não são objeto de proteção do direito ao sigilo das comunicações*** *(cfr. Acórdão n.º 486/2009). De facto, se o objeto de proteção é uma comunicação individual, então os dados que não pressuponham uma concreta comunicação, que não façam parte do processo de comunicação, ainda que protegidos pela reserva da vida privada – artigo 26.º da CRP – não estão cobertos pela tutela do sigilo das comunicações.*

Por tudo isso, também se entende que ***a área de proteção do sigilo das comunicações consagrada no n.º 4 do artigo 34.º da CRP, compreende tanto o conteúdo da comunicação como os dados de tráfego atinentes ao processo de comunicação****. Na verdade, o acesso aos dados de tráfego pode constituir uma ingerência gravosa na vida privada das pessoas, já que se pode aceder a informações relativas a todas as chamadas efetuadas, incluindo as chamadas para as linhas de serviço de emergência/SOS/similares, ao número de chamadas, aos números de telefone chamados, à hora de início e duração de cada chamada e às respetivas unidades de contagem.*"

4.9. O **Acórdão 403/15** reconhece, todavia (cfr. nº 16 do mesmo aresto), que o «... ***direito à inviolabilidade das comunicações não é pois um direito absoluto****, visto que a Constituição autoriza uma intervenção normativa do legislador, para salvaguarda de outros valores constitucionais, nomeadamente de bens jurídicos dotados de dignidade penal (de bens jurídico-penais), ao serviço dos quais se encontra o processo criminal.*» (ênfase desta Comissão).

No entanto, «... *a intervenção normativa abstrata do legislador ordinário só pode ocorrer nos termos autorizados pela norma constitucional e nos casos nela previstos*».

Ora, «... *o **tipo de restrições ao direito à inviolabilidade das comunicações que é admitido pelo n.º 4 do artigo 34.º da CRP é muito mais exigente do que as restrições toleradas por outros direitos fundamentais em que se protegem os mesmos bens jurídicos** (dignidade da pessoa, desenvolvimento da personalidade, garantia da privacidade, autodeterminação comunicativa). **Contrariamente ao que se verifica em alguns desses direitos**, em que, através da expressão "nos termos da lei", se atribui uma competência genérica de regulação que pode ser interpretada como incluindo poderes de restrição, **a norma permissiva do n.º 4 do artigo 34.º autoriza a restrição do direito à inviolabilidade das comunicações apenas em determinado domínio normativo: "em matéria de processo criminal"**. Através deste segmento normativo, a autorização constitucional expressa para a restrição do direito à inviolabilidade das comunicações é completada com a **discriminação dos fins e interesses** a prosseguir com a lei restritiva ou com o **critério** que deve balizar a intervenção do legislador ordinário*» (cfr. *ibidem*) (ênfase desta Comissão).

De modo que, «... *a **enunciação constitucional expressa** da matéria em que há autorização para uma intervenção legislativa limitadora do âmbito de proteção do direito à inviolabilidade das comunicações **constitui também uma garantia de que tais restrições não estão autorizadas noutras matérias e para outras finalidades***».

4.10. O **Acórdão 403/15** entendeu, assim (cfr. nº 17 do mesmo aresto) (ênfase desta Comissão):

> "*17. Ao definir o campo de incidência da lei restritiva do direito à inviolabilidade das comunicações pela "**matéria de processo criminal**" a Constituição ponderou e tomou posição (em parte) sobre o conflito entre os bens jurídicos protegidos por aquele direito fundamental e os valores comunitários, especialmente os da segurança, a cuja realização se dirige o processo penal. Não obstante as **restrições legais ao direito à inviolabilidade das comunicações** que o legislador está autorizado a estabelecer deverem obedecer à ponderação do **princípio da proporcionalidade**, **a preferência***

abstrata pelo valor da segurança em prejuízo da privacidade das comunicações só pode valer em matéria de processo penal."

E, mais adiante, acrescenta, na minha linha o Acórdão em apreciação (ênfase desta Comissão):

"***Nada autoriza, pois, a admitir uma eventual extensão do âmbito da ressalva final do n.º 4 do artigo 34.º*** *- para a qual, aliás, o intérprete, neste contexto concreto, não dispõe de instrumentos metodológicos adequados.*

De facto, a referência ao processo criminal não é apenas uma indicação teleológica, mas também a localização da restrição à proibição de ingerência numa área estruturada normativamente em termos de oferecer garantias bastantes contra intromissões abusivas. ***Ao autorizar a ingerência das autoridades públicas nos meios de comunicação apenas em matéria de processo penal****, e não para quaisquer outros efeitos,* ***a Constituição quis garantir que o acesso a esses meios, para salvaguarda dos valores da "justiça" e da "segurança", fosse efetuado através de um instrumento processual que também proteja os direitos fundamentais das pessoas****. (...)*

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

Por outro lado, a ***referência ao processo criminal implica que a intervenção restritiva careça de prévia autorização judicial****. (...)*

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

4.11. Em face destes pressupostos, o **Acórdão 403/15** acabou por entender, quanto à caracterização da **actividade de recolha de informação** por parte dos Serviços que integram o SIRP (cfr. nº 19 do mesmo aresto):

"*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 de controlo que estabelece,* ***colocam o acesso aos dados de tráfego fora do âmbito da investigação criminal****.*

A remissão que o n.º 2 do artigo 78.º do Decreto 426/XII faz para a alínea c) do n.º 2 do artigo 4.º, que descreve as atribuições do SIRP, ***indica a finalidade do acesso aos dados de trafego: recolha, processamento, exploração*** *e* ***difusão de informações adequadas a prevenir a sabotagem****, a* ***espionagem****, o* ***terrorismo****, a* ***criminalidade altamente organizada de natureza transnacional*** *e a* ***prática de atos que possam alterar ou destruir o Estado de Direito democrático****.*

Ora, a caracterização dessa concreta atividade como ***recolha de "informações" para efeitos de "prevenção" dissocia-a, de forma clara e precisa, da atividade própria de investigação criminal****. A investigação criminal, di-lo a própria lei - artigo 1.º da Lei n.º 49/2008, de 27 de agosto - «compreende o conjunto de diligências que, nos termos da*

lei processual penal, se destinam a averiguar a existência de um crime, determinar ou seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo». E mesmo a circunstância dos dados de tráfego se reconduzirem a crimes tipificados no ordenamento jurídico-penal ***não permite que se caracterize a "recolha de informação" como um ato de "recolha de provas" ou que a "ação preventiva" configure uma "atividade processual"****.*

Não obstante existir uma relação entre informações e investigação criminal*, o* ***legislador teve a preocupação de distinguir****, em sentido material e orgânico,* ***as duas actividades****. (...)*

Há, pois, uma ***distinção radical entre informações e investigação criminal, o 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 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****.*

De facto, iniciando-se o processo penal com a notitia criminis, ***a recolha de informações para esse fim tem que se dirigir a um crime já praticado****. (...)*

Diferente é a configuração da atuação "preventiva" dos serviços de informações, à qual corresponderá um acesso aos dados que pode abranger um universo de pessoas muito mais vasto, precisamente por não estar ainda pré-ordenado à investigação de um facto concreto e delimitado. ***As funções de recolha e tratamento de informações a levar a cabo pelo SIRP, porque preventivas, não se orientam para uma atividade investigatória de crimes praticados ou em execução. Não são atos de polícia judiciária, destinada à investigação criminal****. (...)*

*Os **procedimentos preventivos dessa natureza**, desvinculados da dependência funcional a uma autoridade judiciária, **não fazem parte da investigação criminal**. A Lei Fundamental enquadra essas ações no **direito constitucional da polícia** – artigo 272.º –, não como atividade auxiliar da realização da justiça, mas apenas como "medidas de polícia" de caráter preventivo. **A atividade relativa à produção de informações pelo SIRP destinadas a previr os crimes contra a segurança do Estado, soberania nacional e realização do Estado de Direito, pode ser abrangida por esse preceito** (cfr. Jorge Miranda e Rui Medeiros, ob. cit., págs. 663 e 664), **mas, porque não se dirige à descoberta da autoria de um crime, não reveste a natureza de investigação criminal.** As **ações de prevenção do SIRP** são, pois, procedimentos administrativos que, devendo respeitar os direitos, liberdades e garantias (artigo 5.º do Decreto n.º 426/XII), **não obedecem aos princípios jurídico-constitucionais conformadores do processo penal**, proclamados no artigo 32.º da CRP."*

4.12. Por outro lado, o **Acórdão 403/15** acabou, também, por entender, que a proposta criação de uma **Comissão de Controlo Prévio**, prevista pelo Decreto 426/XII, não resolvia o problema da intervenção de uma **autoridade judiciária** exigida pelo texto constitucional (cfr. nº 20 do mesmo aresto) (ênfase desta Comissão):

*"**20.** E não é a intervenção da **Comissão de Controlo Prévio** que tem a virtualidade de judicializar o acesso aos dados de tráfego. A titularidade do processo penal é atribuída às **autoridades judiciárias competentes** – Ministério Público, juiz de instrução criminal e juiz de julgamento (cfr. alínea b) do artigo 1.º do CPP) e **aquela Comissão tem a natureza de órgão administrativo não inserido jurídico normativamente na organização judicial, pese embora a qualidade dos seus membros**. De facto, **do ponto de vista formal ou orgânico, não exerce a função judicial** e, **do ponto de vista material, não exerce a função jurisdicional**. (...).*

*Ora, **é precisamente a falta de intervenção de uma entidade judicial**, exigida pelo artigo 32.º, n.º 4, da CRP no que se refere à intervenção nos direitos e liberdades das pessoas, **que demonstra não se poder configurar a atuação de acesso aos dados de comunicações privadas por parte dos oficiais dos serviços de informação como integrando um "processo criminal"**. É certo que, nos termos do artigo 35.º do Decreto n.º 426/XII, a Comissão de Controlo Prévio é 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. No entanto, e **independentemente da sua concreta composição, a comissão de controlo prévio configura um órgão administrativo** e neste ponto é irrelevante saber se é composta por magistrados judiciais, **já que os mesmos atuam, não na veste de entidade judicial, mas como membros da referida comissão administrativa**. De facto, não é específica atividade profissional dos membros que compõem um determinado órgão que muda a natureza do mesmo, transformando-o de órgão administrativo em órgão judicial.*

Nem o sistema de autorização prévia dada pela referida Comissão para acesso e manutenção dos dados de tráfego se poderia equiparar ao controlo existente num processo penal**. De facto, este último, no que toca ao acesso aos presentes dados, assegura garantias não só no que respeita ao acesso, mas ainda no que toca ao **tratamento, manutenção** e **destruição** ou **cancelamento dos mesmos, definindo inclusivamente prazos máximos perentórios para o efeito**. Neste contexto, vigoram as garantias do Código de Processo Penal e da já mencionada Lei n.º 32/2008 que, depois de especificar, no artigo 2.º, n.º 1, alínea f), quais as autoridades competentes para acederem aos dados de tráfego das comunicações (no qual não consta qualquer serviço de informações), estabelece várias **garantias** no que toca ao tratamento e conservação de todos esses dados, sendo nota comum a todo o **acesso, tratamento, conservação** e **extinção, a intervenção de um juiz** (assim, artigos 7.º e 9.º e artigo 11.º, que estabelece sobre destruição de dados). **Todavia, esta intensidade de controlo não é levada a cabo pela referida Comissão de Controlo Prévio, que se limita a conceder um "visto"

prévio de autorização, após o que deixa de ter qualquer intervenção durante as atividades de acesso aos dados em causa."

4.13. O **Acórdão 403/15** considerou, ainda, quanto às **garantias de actuação** da designada **Comissão de Controlo Prévio** (cfr. nº 21 do mesmo aresto) (ênfase desta Comissão):

"*21. Aliás, independentemente da questão da reserva de juiz em processo penal, a **falta das mencionadas garantias verifica-se ainda no que toca à atuação da referida Comissão de Controlo Prévio**. De facto, **da lei não resulta com suficiente determinação quais os casos ou circunstâncias em que a referida Comissão pode conceder a autorização de acesso aos dados**, nem se estabelece com clareza quais as **garantias dos visados** no que toca à **duração da autorização de acesso** ou à **eliminação dos dados**.*

*Ora, uma **atividade de acesso aos dados de tráfego**, levada a cabo sem conhecimento dos visados, exige **regras claras e determinadas** que permitam saber até onde pode ir a ingerência, para que haja a **necessária segurança jurídica** no que toca às **restrições** possíveis aos seus direitos. De facto, **onde a atividade e poderes são exercidos em segredo, maior é o risco de arbitrariedade**, já que os indivíduos não têm conhecimento nem controlam a atividade de ingerência em concreto. (...)*

*Desta jurisprudência decorrem, pois, várias exigências para uma norma que, como a presente, permita o acesso a dados de tráfego das comunicações de indivíduos sem o seu consentimento ou conhecimento. Em primeiro lugar, **a lei deve empregar termos suficientemente claros** para possibilitar a todos os cidadãos terem conhecimento das **circunstâncias** e dos **requisitos** que permitem ao poder público aceder aos dados em causa, sendo que os **requisitos para o efeito devem ser claramente determinados**; deve ainda fazer menção, com precisão, dos **casos específicos em que o acesso deve ter lugar**, prever a **fixação de um limite de duração da medida**, e das **regras** e **prazos para***

***eliminação dos dados de tráfego**. Só assim se poderá falar de uma **ingerência determinável** e que garanta segurança jurídica aos interessados."*

4.14. O **Acórdão 403/15** concluiu, por isso, quanto a este ponto (cfr. nº 22 do mesmo aresto) (ênfase desta Comissão):

> "*22. Mas, se assim é, há que reconhecer que, para além da impossibilidade de compatibilização com a norma do n.º 4 do artigo 34.º da CRP, a norma do n.º 2 do artigo 78.º do Decreto n.º 426/XII **não contém densidade suficiente para, num domínio de lei restritiva, possibilitar a fiscalização da legalidade** e a **defesa dos direitos e interesses dos cidadãos**. Com efeito, a norma não satisfaz suficientemente, como contrapartida do acesso aos dados de tráfego, as **exigências de determinabilidade que são garantidas em matéria de processo criminal, devolvendo para a esfera administrativa ponderações que deveriam constar da lei**.*
>
> *Desde logo, e quanto aos **pressupostos da concessão da autorização de acesso aos dados**, a lei estabelece que o acesso aos dados de tráfego de comunicações tem lugar nos casos previstos na alínea c) do n.º 2 do artigo 4.º, que respeitam à prevenção de sabotagem, espionagem, 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. **Mas a parte final da norma não oferece suficiente segurança jurídica aos potenciais lesados, já que resulta indeterminado o que podem constituir «atos que, pela sua natureza, possam alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido»**. Assim, não se pode considerar que a lei tenha determinado de forma suficientemente precisa os casos em que a ingerência possa ter lugar. Trata-se, aliás, de uma **verdadeira indeterminabilidade**, que pode ser facilmente manipulável para permitir um acesso arbitrário aos dados de tráfego das comunicações.*

Depois, porque delimita as condições em que o acesso a dados de tráfego pode ter lugar por parte dos oficiais de informações do SIRP da seguinte forma: «sempre que sejam ***necessários, adequados*** *e* ***proporcionais, numa sociedade democrática, para o cumprimento das atribuições legais dos serviços de informações****». Ora, a referência às* ***exigências de necessidade, adequação*** *e* ***proporcionalidade em sentido estrito****, quando reportada à atuação dos oficiais de informações em matéria de dados e informações,* ***não representa mais do que um afloramento de um parâmetro de juridicidade da Administração****, tal como se encontra genericamente consagrado no artigo 266.º, n.º 2, da Constituição, e é, nesse plano, inteiramente redundante na medida em que se trata de um princípio material conformador de toda e qualquer atividade administrativa. (...)*

Assim, no artigo 78.º do Decreto, ***para além de os casos que permitem o acesso aos dados de tráfego não resultarem suficientemente determinados****, o mesmo se pode dizer das* ***condições de acesso****, já que dele não resulta quais os* ***critérios*** *a que se deve atender para aferir se a ingerência estadual, num determinado caso, é "****necessária, adequada*** *e* ***proporcional, numa sociedade democrática****".*

Por outro lado, e ainda quanto às situações de facto cuja ocorrência depende a possibilidade legal de intervenção da Comissão de Controlo Prévio, a norma objeto de fiscalização, em conjugação com a alínea c) do n.º 2 do artigo 37.º do Decreto, ***não impede que se autorize a recolha e análise de informação sem referência a alvos concretos****. Muito pelo contrário, ele deixa espaço para que o acesso a dados seja feito de forma bastante alargada de modo a detetar padrões de conduta que possam reconduzir os cidadãos a potenciais suspeitos de crime."*

4.15. O **Acórdão 403/15** é, ainda, crítico quanto ao **procedimento de acesso à informação**, reportando-se, por outro lado, ao trabalho desenvolvido por esta **Comissão de Fiscalização de Dados**, embora sem mostrar conhecer, em pormenor, os

exactos termos em que a intervenção desta normalmente se processa (cfr. nº 23 do mesmo aresto) (ênfase desta Comissão):

> "***23.*** *Acresce, por fim, que a norma do n.º 2 do artigo 78.º, no contexto jurídico-sistemático em que está inserida,* ***não torna claro e explícito todo o procedimento de acessso, a duração do acesso*** *e a* ***eliminação dos dados de tráfego recolhidos****.*
>
> *De facto,* ***daquela norma, nem de qualquer outra do Decreto, resulta como é feito o acesso aos dados****. Mais uma vez se impõe o contraponto com a* ***Lei n.º 32/2008****, que determina, no n.º 3 do artigo 7.º, como é feita a transmissão de dados por parte das operadoras no contexto do processo penal: «****processa-se mediante comunicação eletrónica, nos termos das condições técnicas e de segurança fixadas em portaria conjunta*** *dos membros do Governo responsáveis pelas áreas da administração interna, da justiça e das comunicações, que devem observar um* ***grau de codificação e proteção o mais elevado possível****, de acordo com o estado da técnica ao momento da transmissão,* ***incluindo métodos de codificação, encriptação*** *ou* ***outros adequados****». Ora, o Decreto n.º 426/XII* ***nada menciona no que toca à forma de comunicação dos dados****, nem remete esta matéria para qualquer outra regulamentação.*
>
> ***E quanto ao tempo durante o qual é permitido o acesso aos dados, verifica-se a mesma falta de segurança jurídica****. Nos termos do artigo 37.º, n.º 2, alínea d), do Decreto, o* ***prazo de acesso não pode exceder três meses, mas pode ser estendido, mediante autorização expressa. Porém, a lei não contém qualquer limite para tal prorrogação, nem estabelece em que condições pode ser autorizada a referida prorrogação****. A lei prevê assim, a partir do momento em que a Comissão de Controlo Prévio dá a sua autorização, uma possibilidade de acesso aos dados de tráfego sem qualquer limite máximo de tempo. Assim, tal como decidiu o TEDH no caso Valenzuela c. Espanha, acima referido,* ***a falta de menção de prazo específico de duração da medida gera incerteza para os destinatários da mesma****, pelo que não se pode considerar, também por aqui, que a* ***lei cumpra a exigência de determinabilidade****.*

Idêntica incerteza pode apontar-se no que respeita à eliminação dos dados *- que corresponderia, aliás, a uma exigência do direito à autodeterminação comunicativa, na vertente do "direito ao esquecimento". No Decreto n.º 426/XII* ***não se especifica qualquer prazo para a manutenção ou eliminação obrigatória dos dados****. De resto, são escassas e incertas as possibilidades previstas referentes à eliminação dos dados. O artigo 37.º, n.º 8, prevê a possibilidade da Comissão de Controlo Prévio, em coletivo,* ***participar à Comissão de Fiscalização «os elementos conducentes à destruição imediata desses dados ou informações»****. Todavia,* ***sem a previsão legal de um acompanhamento constante por essa Comissão, fica por saber como chega ao seu conhecimento a existência de dados que devem ser eliminados****. Por seu turno, o* ***Secretário-Geral*** *tem poderes para ordenar a* ***destruição imediata de todos os dados e informações*** *recolhidos mediante a autorização prevista no presente artigo,* ***«sempre que não tenham relação com o objeto ou finalidades da mesma»*** *(artigo 37.º, n.º 7). Assim, na prática,* ***a fiscalização da manutenção de dados é apenas levada a cabo pela Comissão de Fiscalização do SIRP que, em regra, exerce a sua atividade fiscalizadora dos centros de dados por amostragem*** *(artigo 30.º, n.º 1). A única norma que se refere a um "dever" de eliminação de dados consta do artigo 30.º, n.º 3, de acordo com a qual a referida Comissão de Fiscalização «deve ordenar o cancelamento ou retificação de dados recolhidos que envolvam violação dos direitos, liberdades e garantias consignados na Constituição e na lei». Não se estipula, porém, em que condições ou em que prazos tem lugar uma fiscalização conducente a esta avaliação e correspondente destruição dos dados. No mais, qualquer possibilidade de eliminação ou destruição de dados estará sempre dependente do conhecimento e pedido dos visados, nos termos do artigo 32.º. Ora,* ***a falta de prazos perentórios de eliminação de dados****, ou de* ***procedimentos periódicos obrigatórios destinados a averiguar a necessidade de manutenção de todos os dados existentes****, bem como de* ***clara determinação do momento ou condições em que a manutenção dos dados deixa de ser necessária****, também não oferece suficiente segurança à defesa dos direitos e interesses dos cidadãos."*

4.16. O Acórdão 403/15 acaba, assim, por concluir (cfr. nº 24 do mesmo aresto) (ênfase desta Comissão):

> "*24. De todo o exposto resulta, assim, que,* ***independentemente da natureza específica do órgão "Comissão de Controlo Prévio", a atuação do mesmo não se afigura equiparável ao controlo jurisdicional existente em processo penal em matéria de direitos fundamentais****. De facto, este último, no que toca à ingerência nas comunicações, assegura* ***garantias*** *não só no que respeita ao* ***acesso****, mas ainda no que toca ao* ***tratamento, manutenção*** *e* ***destruição*** *ou* ***cancelamento dos dados, definindo inclusivamente prazos máximos perentórios para o efeito****. Neste contexto, vigoram as* ***garantias do Código de Processo Penal*** *e da* ***Lei n.º 32/2008*** *que estabelece várias garantias no que toca ao tratamento e conservação de todos esses dados, sendo nota comum a todo o* ***acesso, tratamento, conservação*** *e* ***extinção****, a* ***intervenção de um juiz*** *(cfr. artigos 7.º, 9.º e 11.º). Esta intensidade de controlo não é levada a cabo pela referida* ***Comissão de Controlo Prévio****, que se limita a conceder um* ***«visto» prévio de autorização****, após o que não exerce qualquer acompanhamento durante as atividades de acesso aos dados em causa. Neste ponto se vê, pois, também que a* ***institucionalização do controlo prévio mencionado em nada se pode considerar equiparável ao oferecido em matéria de processo penal****.*
>
> *Enfim, importa reconhecer que 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****. Assim, as razões que justificaram a exceção expressamente mencionada no n.º 4 do artigo 34.º da CRP, que se prendiam, precisamente, com as específicas garantias existentes em processo criminal, não se verificam no presente caso.*

Por conseguinte, também a resposta à segunda questão que foi colocada pelo Requerente neste processo é seguramente negativa: ***a Comissão Prévia de Controlo é um órgão administrativo que não tem poderes equivalentes a uma intervenção em processo criminal.***"

4.17. Para além desta ampla referência ao teor do **Acórdão 403/15**, crê-se, todavia, de contemplar também referência a alguns aspectos mais salientes das declarações de voto que o acompanham, porque poderão vir a merecer, se houver lugar a uma ulterior intervenção do Tribunal Constitucional nesta matéria, eventual ponderação por parte dos actuais Juízes Conselheiros que o integram.

E começaremos pela declaração de voto da **Conselheira Maria Lúcia Amaral**, que, como acima indicado, discordou de alguns dos fundamentos invocados na posição do Acórdão que fez vencimento, votando, no entanto, a decisão. Refere, designadamente, a mesma Juíza Conselheira (ênfase desta Comissão):

"*3. Creio, no entanto, que* ***não é deste modo que se deve entender o conceito constitucional de «autorização para restringir [um direito fundamental]».*** *Penso que quando a Constituição remete para a lei, indicando a possibilidade legal de limitação de um certo direito para um certo fim, não está a prever nenhuma «exceção» a nenhuma «regra» ou «norma». A complexidade da ordenação constitucional dos direitos fundamentais, e da sua relação com a lei, não se deixa reduzir a tão simples termos.* ***Quando a Constituição remete para a lei, indicando a finalidade de uma restrição a um direito,*** *o que está a fazer é coisa diversa:* ***está a antecipar a possibilidade de ocorrência futura de conflitos entre o direito que consagra e outros «interesses» ou «valores» constitucionalmente protegidos, devolvendo ao legislador ordinário a tarefa necessária de resolução acertada desse conflito.*** *No caso, em que se autorizou o legislador a restringir a inviolabilidade do segredo das telecomunicações «em matéria de processo criminal», previu-se a possibilidade de ocorrência futura de*

um conflito entre tal inviolabilidade, expressão da liberdade das pessoas, e a necessidade de preservação de valores comunitários fundamentais, expressos, nos termos da Constituição, por leis penais incriminadoras, aplicadas por intermédio das normas pertinentes de processo criminal. Além disso, e porque a incriminação de comportamentos e a sua concretização pelas normas de processo significam também elas próprias, como bem se sabe, restrições à liberdade (do destinatário das incriminações), ***a autorização constitucional expressa para restringir a inviolabilidade do sigilo das telecomunicações em matéria de processo criminal significa também a necessidade, constitucionalmente reconhecida, de fazer concordar a liberdade de uns*** *(os titulares do direito à inviolabilidade das telecomunicações)* ***com a liberdade de outros*** *(os titulares dos direitos que a CRP confere a quem é arguido em processo criminal).*

4. *A* ***existência de Serviços de Informações da República – cujos fundamentos constitucionais o Tribunal pura e simplesmente não aborda –, 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****. Todavia, da aplicação das normas que enformem o sistema de organização dos serviços da informações, ou da definição das suas competências, não decorrem – pela natureza mesma desses serviços – uma ameaça lesiva da liberdade individual que seja, pela sua intensidade, equiparável àquela que emerge, inevitavelmente, da aplicação das normas de processo criminal. Assim, e* ***havendo afinidade valorativa ou teleológica entre as finalidades prosseguidas pelos serviços de informação e as normas penais incriminadoras*** *– e decorrendo da aplicação das primeiras uma potencialidade de agressão da liberdade individual em todo o caso menor do que aquela que ocorre com a mera adjetivação das segundas – poder-se-ia concluir, se tivesse sido outra a posição conceptual e metódica de que se partisse,* ***que a autorização constitucional para restringir a inviolabilidade das telecomunicações em «matérias de processo criminal» se estenderia, por maioria de razão, aos Serviços de Informações da República.***

Impedir a extensão por razões meramente textuais, ultrapassáveis pelo acrescento de algumas palavras à parte final do n.º 4 do artigo 34.º feito em processo de revisão constitucional, não me parece convincente: creio que os caminhos de uma hermenêutica constitucional adequada não passam pelo método estrito de uma «textualidade» como esta, que ergue em objeto de «interpretação» preceitos [e incisos desses preceitos] isoladamente tomados, sem consideração pelo lugar que ocupam no sistema axiológico da Constituição. ***Impedir a extensão por razões valorativas*** *– que, por isso mesmo, permaneceriam para além de uma decisão parlamentar tomada pela maioria qualificada a que se refere o n.º 1 do artigo 286.º da CRP –* ***implicaria demonstrar que só a função jurisdicional do Estado estaria apta para resolver em concreto o conflito entre a liberdade e a segurança que a necessidade de interceção de dados de tráfego das telecomunicações implica. Ora, a meu ver, essa demonstração não pode ser feita. Não vejo 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 n.º 4 do artigo 34.º da CRP.*** *(...)*

A regulação, por lei, dos Serviços de Informações da República, a incluir no sistema de competências desses mesmos serviços a possibilidade de interceção dos dados de tráfego de telecomunicações, teria assim que, *pelo menos,* ***tornar tão claras e precisas quanto possível as circunstâncias em que o acesso a esses dados seria legítimo, de modo a não deixar à administração a liberdade de ponderar – sem quaisquer limites legais – da necessidade da interceção.*** *Esta é uma exigência que decorre, desde logo da primeira frase do n.º 2 do artigo 18.º da CRP, uma vez ser a reserva de lei, que aí se consagra, não apenas formal mas também material.* ***A intervenção agressiva da administração na esfera da liberdade dos privados não pode deixar de ser balizada por certos critérios a definir por lei, de modo a que seja a lei a distinguir, com um mínimo de precisão, a intervenção administrativa legítima da ilegítima. Depois,*** *e*

ainda nos termos do n.º 2 do artigo 18.º da CRP, ***tal intervenção não poderia deixar de ser proporcionada, limitando-se ao necessário para «salvaguardar outros direitos ou interesses constitucionalmente protegidos».*** *Por isso mesmo,* ***a lei reguladora do sistema dos Serviços de Informações da República****, a incluir na competência dos seus órgãos ou agentes a possibilidade de interceção dos dados de tráfego das telecomunicações,* ***ter-se-ia que munir de um sistema interno de controlo quanto ao cumprimento dos limites legais dessas interceções que fosse, ele também, protetor da ameaça da liberdade que a referida interceção sempre representa.***"

4.18. Vejamos, por último, alguns dos aspectos da posição expressa na segunda declaração de voto ao Acórdão 403/15, do **Conselheiro Teles Pereira**.

Refere este Juiz Conselheiro, a propósito da **revisão constitucional de 1997** (ênfase desta Comissão):

"***Consistiu esta alteração de 1997****, pois, e* ***sem qualquer indício*** *– sublinhamo-lo desde já –* ***de se ter visado algo mais do que o acesso pelas autoridades ao próprio conteúdo da comunicação, na integração no texto constitucional, em paralelo à correspondência em sentido clássico*** *(o correio em suporte físico: as cartas, as encomendas postais e o telégrafo)* ***e às telecomunicações existentes*** *(basicamente o telefone, eventualmente já o fax e a telecópia), que correspondiam aos meios de comunicação clássicos pensados como a realidade existente em 1976,* ***de outros meios equivalentes, os "demais meios de comunicação",*** *abrindo a previsão do artigo a uma evolução, já fortemente pressentida em 1997, para novas realidades técnicas comunicacionais entre as pessoas.* ***Estas, todavia, mantiveram no texto constitucional*** *(no artigo 34º, nº 4)* ***o sentido essencial que, então*** *(em 1997),* ***lhes era atribuído: fundamentalmente o correspondente ao conteúdo da própria comunicação*** *(os* ***dados de conteúdo****, numa terminologia que posteriormente se tornou usual),* ***não tanto, então em 1997, com um sentido, que possamos considerar claro, de abarcar outros dados***

***respeitantes à comunicação**, concretamente o que no futuro viria a ser qualificado como **dados de tráfego**, enquanto elementos que nada aportassem quanto ao conteúdo, em si mesmo, do ato comunicacional. A doutrina propendia, então (continuamos a referir o momento histórico da revisão de 1997), **a associar a ideia de ingerência nas telecomunicações, essencialmente, à interceção das palavras trocadas entre os intervenientes**. (...)*

*O que aqui se pretende sublinhar, sem menosprezar o significado do elemento evolutivo que a questão dos dados de tráfego assumiu posteriormente, é, tão-somente, **a circunstância do nº 4 do artigo 34º da CRP não se ter formado num quadro em que a questão do acesso aos dados circunstanciais da comunicação se colocasse exatamente com o mesmo sentido do próprio acesso ao conteúdo da comunicação**, e já então a questão do acesso das autoridades aos **dados de tráfego** havia sido equacionada, por exemplo, na jurisprudência do Tribunal Europeu dos Direitos do Homem, no Acórdão Malone v. Reino Unido, de 1984, a respeito do trecho do artigo 8.º, nº 2 da Convenção que exige que a ingerência das autoridades esteja "prevista na lei" (...). Ou seja, o que aqui se pretende afirmar é, tão-só, que **o texto constitucional, não se tendo cristalizado numa fase (inicial) de "indiferença valorativa" pelo que hoje chamamos dados de tráfego, não assimilou logo para estes um grau de proteção absolutamente idêntico ao dos dados de conteúdo**."*

4.19. Mais adiante, refere, também, o Conselheiro Teles Pereira, na sua declaração de voto (ênfase desta Comissão):

"*6. A **discussão no plano constitucional – no quadro de uma democracia constitucional – da atividade dos Serviços de Informações, convoca ao debate**, necessariamente, os valores **Segurança** e **Democracia**, colocados em paralelo, **assumindo a existência de uma tensão existencial permanente entre a adoção de políticas públicas promotoras de segurança e os valores democráticos** – os valores*

próprios de um Estado de direito democrático –, ***concretamente aqueles que se expressam no exercício de direitos fundamentais****. Trata-se neste domínio, essencialmente, de responder a um desafio: o* ***desafio da perspetivação da Segurança, no sentido decorrente do artigo 27º, nº 1 da CRP*** *("[t]odos têm direito à liberdade e à segurança"),* ***enquanto obrigação prestacional do Estado aos cidadãos, numa relação de tensão entre valores constitucionais****. E, com efeito, todos reconheceremos que a* ***prestação de Segurança pelo Estado suscita frequentemente questões complexas de compatibilização*** *(mesmo de tensão existencial)* ***entre direitos, apresentando-se como um domínio de eleição na atuação do princípio da proporcionalidade****, com o sentido que o nosso texto constitucional confere a este: "[a] lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos e interesses constitucionalmente protegidos" (artigo 18º, nº 2 da Constituição). (...)*

Vale, a respeito da promoção da segurança como valor constitucional, o entendimento da Constituição, do espaço vivencial por ela desenhado, como envolvendo uma ***proteção ativa do modelo democrático que expressa, funcionando o texto constitucional como "contrato social" contendo cláusulas, explícitas e implícitas, de autodefesa****, através das quais se constrói o conteúdo de uma* ***função de "proteção da Constituição"*** *(fórmula que a Constituição alemã expressamente inclui no seu texto – Verfassungsschutz),* ***que legítima, além da tutela penal propriamente dita, o que se pode designar como "proteção administrativa da Constituição"****. Trata-se aqui do que a Doutrina constitucional germânica identifica como "[...]* ***institutos e faculdades para a defesa da ordem fundamental livre e democrática*** *[...]",* ***englobando a atividade dos serviços de informações****, ou seja: "[...] a* ***recolha*** *e* ***tratamento de informações*** *[...]* ***em âmbitos que antecedem as ameaças concretas para os bens jurídicos protegidos****. Tal recolha e avaliação abarca [...] a* ***vigilância de pessoas*** *e* ***organizações suspeitas de atividades contrárias à Constituição****" (Erhard Denninger, "Stretbare Demokratie und Schutz der Verfassung", in Benda, Maihofer, Vogel, Hesse, Heyde, Handbuch des Verfassungs Rechts, 2ª ed., Berlim, 1994, p. 699). Corresponde esta forma especial de*

proteção, a atividade que a concretiza, ao domínio primordial de atuação dos Serviços de Informações, corresponde, enfim, à ***função de produção de informações****.*

Assim, podemos caracterizar a intencionalidade desse conteúdo funcional (a tal ***atividade de proteção da Constituição****, não de proteção ou de defesa do Estado aparelho de poder)* ***como um sistema estruturada em vista do desencadear de mecanismos de alerta prévio, uma função sequencialmente referida ainda a um momento anterior ao da entrada em jogo*** *– rectius, da adjetivação –* ***da tutela penal, mas que, nem por isso, deixa de estar ligada aos valores específicos*** *(aos tipos)* ***abarcados pela lei penal, e de poder mesmo vir a entroncar na adjetivação penal****. É que,* ***num Estado de direito democrático, fora de um quadro de referenciação aos valores subjacentes à tutela penal*** *– fora dos mínimos éticos e dos valores jurídico-constitucionalmente reconhecidos em que esta assenta (v. Jorge de Figueiredo Dias, Direito Penal, Parte Geral, Tomo I, 2ª ed., Coimbra, 2007, p. 120, § 25) –* ***não existe qualquer intervenção legítima de proteção do espaço constitucional****. Pelo contrário, existirá um uso abusivo e ilegítimo dessa função protectiva. Defender-se-á algo, eventualmente defender-se-á o poder (algum poder circunstancial), mas isso nada tem que ver com a proteção de uma "****ordem fundamental livre e democrática****". E é esta que legitima – e só ela legitima – a tarefa de "proteção da Constituição". Esta – esta* ***atividade exercida num espaço de legitimidade constitucional*** *– situar-se-á, pois,* ***na antecâmara da tutela penal, numa fase ainda larvar desta, e atuará onde os respetivos valores, mesmo que em termos difusos e ainda com um significado ambíguo, já estejam demonstravelmente presentes, já tenham, enfim, sido colocados nalgum tipo de insegurança existencial minimamente concretizada e individualizada****. E será este mínimo de concretização e de individualização de uma ameaça, que também poderíamos caracterizar através da ideia de* ***risco****, reportada aos valores elencados no nº 2 do artigo 4º do Decreto nº 426/XII (todos eles reportáveis, por sua vez, à tutela penal), que os Serviços de Informações sujeitarão à apreciação da Comissão de Controlo Prévio, na lógica de funcionamento do nº 2 do artigo 78º do mesmo Decreto,*

recaindo sobre eles (sobre os Serviços de Informação) o ónus de demonstrar os pressupostos mencionados na norma.

Assim, numa espécie de síntese conclusiva, diremos que ***a atividade de proteção da Constituição incidirá sobre condutas individuais ou coletivas que contenham uma potencialidade, não negligenciável, de menoscabo, mesmo que embrionário, dos valores próprios de uma "ordem fundamental livre e democrática", quando esse desvalor seja reportável ao elenco do nº 2 do artigo 4º do Decreto nº 426/XII e potencie, ou torne racionalmente expectável, uma evolução que, em última análise, nos conduza a condutas penalmente típicas, referenciáveis aos valores estruturantes dessa "ordem fundamental livre e democrática" – em particular o terrorismo (ao qual se refere a Lei nº 52/2003, de 22 de agosto) a espionagem e outros dos crimes contra o Estado, fundamentalmente os elencados no Título V do Código Penal,*** *constituindo estes exemplos paradigmáticos que justificam essa intervenção precoce correspondem ao espaço de referência da defesa da Constituição.*

Simplificando, diremos que a compressão que uma determinada política pública, promotora do valor segurança, possa induzir numa posição jusfundamental, justificar-se-á – só se justificará – se essa compressão for efetivamente referida à promoção desse valor constitucional, sendo necessária à implementação dele e, entre as opções possíveis, ***representar o mínimo de compressão necessário à salvaguarda desse valor****. É este, fundamentalmente, "metido numa casca de noz", o sentido do* ***princípio da proporcionalidade*** *e a aplicação deste aos valores segurança e liberdade, colocando frequentemente problemas delicados, não convoca um modelo analítico distinto do que subjaz ao artigo 18º, nº 2 da Constituição, concretizado nas chamadas "quatro regras da proporcionalidade":* ***prossecução de um fim legítimo, adequação a esse fim, necessidade*** *e* ***proporcionalidade em sentido estrito****, em que se determina, comparando diretamente as situações em confronto, se a restrição representa um ganho líquido relativamente à sua não adoção."*

4.20. O Conselheiro Teles Pereira aborda, ainda, na sua declaração de voto, de forma circunstanciada, a **função de produção de informações**, referindo a citação de Richard Posner a propósito do conceito de "*intelligence*", segundo a qual, "[*o*] ***objetivo da 'produção de informações'*** [*the goal of intelligence*] ***é o conhecimento das intenções e das capacidades de inimigos potenciais***" (*Preventing Surprise Attacks. Intelligence Reform in the Wake of 9/11*, Nova York, Oxford, 2005, p. 99)".

E, sobre o conceito de "***dados de tráfego***", não deixa de salientar a importância do **contexto de aquisição deste tipo de informação** e as **diferenças** daí decorrentes para a protecção dos direitos individuais das pessoas (ênfase desta Comissão):

> "*Ora, os* ***dados de tráfego*** *aqui em causa são (contêm)* ***informação em si mesmos, permitem o estabelecimento de conexões entre pessoas e situações, tomando como ponto de partida a existência pretérita de uma determinada comunicação, esgotando-se o seu sentido numa extrapolação analítica realizada com base na existência dessa comunicação e das relações que ela indica, não com base no conteúdo da própria comunicação****. Tal circunstância introduz, desde logo, o elemento central – por vezes objeto de confusão numa discussão superficial – da caracterização dos dados de tráfego, qualificados como* ***metadados****, referidos, como aqui sucede, às telecomunicações,* ***distinguindo (separando) estes do próprio conteúdo da comunicação (a mensagem em si mesma)****. É com este sentido, num debate que envolve frequentemente a ponderação do significado do acesso das autoridades públicas aos chamados metadados (se entendidos como dados de tráfego), que se contrapõe, quando – como aqui sucede – está em causa, tão-somente, o acesso a estes, o sentido de uma "****análise do tráfego contra a análise do conteúdo****" ("traffic versus content analysis"),* ***reconduzindo a uma dimensão mais atenuada o potencial de compressão de direitos, mesmo de afetação da autodeterminação informacional, envolvido por um acesso exclusivo aos metadados*** *(cfr. Amitai Etzioni, Privacy in a Cyber Age. Policy and Practice, Nova York, 2015, pp. 132/133).* ***Esse acesso não deixa, todavia, de consubstanciar uma intromissão na privacidade*** *e, por isso mesmo, não dispensa o seu*

tratamento como tal: como intromissão numa dimensão específica do direito à privacidade. (...)

É ainda relevante sublinhar o ***contexto da aquisição deste tipo de informação*** *(dos ditos* ***metadados****). Pode tratar-se (i) de uma* ***aquisição de informação em larga escala, por transferência integral, para alguma autoridade pública, dos registos existentes num operador****, ou pode tratar-se (ii) duma* ***transferência individualizada, realizada (autorizada e controlada) caso a caso, com base numa suspeita concreta e individualizada****. É relevante a distinção porque* ***colocam as duas situações problemas muito distintos****. Notamos que à primeira situação correspondem os programas de recolha de dados, pela NSA – National Security Agency, à escala global, vindos a público em 2013 (no âmbito do chamado caso Snowden), basicamente o programa "Bulk Collection of Telephone Metadata", referido à recolha e conservação, pela NSA, dos registos de comunicações telefónicas efetuadas e recebidas nos Estados Unidos, o programa "PRISM" dedicado à recolha, igualmente pela NSA, de comunicações eletrónicas de determinados fornecedores de serviços on line, caso da Google e do Facebook, este programa dirigido, fundamentalmente a "não-americanos" e o programa "TEMPORA", mantido pelo Government Communications Headquarters (GCHQ) do Reino Unido (cfr., quanto à caracterização dos dois primeiros Programas, Amitai Etzioni, Privacy in a Cyber Age..., cit., p. 123/125 e quanto ao programa "TEMPORA", "A simple guide to GCHQ's internet surveillance programme Tempora", in Wired.co.UK, http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora101). E notamos, que a* ***segunda situação*** *– a* ***obtenção de dados de tráfego caso a caso –, desde logo pela sua escala, dimensão individualizada e especificamente motivada por factos concretos, controlados exteriormente ao interessado na aquisição da informação, não contém o perigo da verdadeira "pesca de arrastão" à escala global****, que conduziu o Tribunal de Justiça da União Europeia, no Caso Digital Rights Ireland, Ltd (C-293/12), Acórdão de 8 de abril de 2014, a considerar inválida a "Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços*

de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE".

Estava em causa nesta situação, com efeito, a conservação pelos operadores, obrigatoriamente, de dados de tráfego por um período mínimo de seis meses e máximo de dois anos, a qual, incidindo sobre todas as comunicações, indiferenciadamente à escala global europeia, comportava uma ingerência, não substanciada em indícios concretos e atendíveis, "nos direitos fundamentais de quase toda a população europeia" (v. os pontos 56 e 58 do Acórdão). Ora, ***este fator de perigo desaparece*** *(no específico sentido em que o Tribunal de Justiça o enunciou)* ***quando o que ocorre é, tão-somente, a prestação de uma informação pelo operador de telecomunicações, em suporte de papel, quanto às chamadas realizadas por um determinado número e à localização espacial dessas chamadas (do equipamento com o qual foram realizadas) por referência a uma antena que distribuiu o sinal. Mais ainda, quando essa informação só é obtida em situações individualizadas, baseadas na existência de indícios consistentes, necessariamente referidos a pressupostos específicos exigentes, controlados caso a caso por uma entidade independente, cuja atuação visa, precisamente, limitar o acesso aos dados e a sua utilização ao estritamente necessário para se alcançar o objetivo prosseguido num espaço de legitimidade legal e constitucional.***

Serve isto para deixar clara a absoluta falta de paralelismo de situações de recolha de dados abstratos em massa com a situação suscitada nesta fiscalização preventiva, desde logo pela incomensurável diferença de escala envolvida, que induz perigos totalmente distintos. *Com efeito, trata-se aqui – e só disso se trata – dos dados individualizados de um caso concreto (que têm de pressupor a existência de um "caso concreto" no serviço de informações que a eles pretende aceder), quando nessas outras situações se tratava da transferência em bloco de grandes massas de dados, desligados de casos concretos, no intuito de, algures no futuro, serem estes dados confrontados com hipotéticos casos concretos. Aqui, no particular contexto do tipo de dados de tráfego relativos a telecomunicações, previstos no nº 2 do artigo 78.º do Decreto n.º*

426/XII, além da dimensão individualizada destes, sempre sujeita a um controlo prévio condicionante assente em pressupostos de base restritiva, verificamos que ***a ulterior conservação pelos Serviços de Informações dos dados cumulativamente gerados pelos acessos autorizados no passado, os dados acumulados ao longo do tempo, sempre será controlada pela Comissão de Fiscalização de Dados do SIRP*** *(o órgão de fiscalização externo com origem na Magistratura do Ministério Público, prevista nos artigos 29º a 34º do Decreto nº 426/XII),* ***com a efetiva possibilidade de cancelamento do que seja indevidamente conservado ou incluído nos centros de dados dos dois Serviços****. Existe, pois, na lógica de funcionamento do sistema – na lógica de funcionamento do SIRP – uma* ***salvaguarda de controlo externo das potencialidades desvaliosas da concentração de grandes massas de informação referida a pessoas****.*"

4.21. O Conselheiro Teles Pereira, na sua declaração de voto, reconhece que a jurisprudência do Tribunal Constitucional aproximou a protecção dos "***dados de tráfego***" da concedida aos "***dados de conteúdo***".

Não deixou, contudo, de igualmente salientar, a este propósito (ênfase desta Comissão):

"*Todavia, a* ***aproximação da proteção dos dados de tráfego àquela que se concede aos dados de conteúdo não esconde uma evidência*** *que se impõe intuitivamente:* ***é diversa a afetação da reserva da intimidade da vida privada na recolha ou interceção de dados de base, de dados de tráfego ou de dados de conteúdo****. Nesta classificação/enumeração sequencial esconde-se uma* ***inegável progressão de intensidade****.(...)*

As apontadas diferenças não esgotam a sua relevância na distinção entre os dados de base e os demais dados decorrentes do serviço de telecomunicações. Elas estendem-se à ***distinção entre os dados de tráfego*** *e os* ***dados de conteúdo****.* ***Sendo verdade que,***

como atrás se concluiu, ***a Constituição aproxima estes no sentido de ambos encontrarem acolhimento no artigo 34.º da CRP, mas tal não significa que lhes imponha, necessariamente, um tratamento rigorosamente idêntico.*** *(...)*

A principal razão pela qual terá de ser diferente o tratamento final a conceder aos dados de tráfego, face aos dados de conteúdo, é fácil de compreender: ***sabendo que as restrições legais permitidas pelo artigo 34º da CRP estão sempre sujeitas ao princípio da proporcionalidade*** *(neste sentido, cfr. Jorge Miranda e Rui Medeiros, Constituição da República Portuguesa Anotada, cit., Tomo I, pág. 774), é por demais evidente que* ***qualquer ponderação de proporcionalidade tem, necessariamente, de considerar,*** *em um dos pratos da balança, a* ***intensidade da lesão,*** *e que, consequentemente,* ***quanto menor a lesão, maior é o leque de atividades que podem ser consideradas legitimadas pela aferição de proporcionalidade.***

Esta diferença é importante, designadamente, para compreender que, como melhor se analisará adiante, as ***posições deste Tribunal sobre a proporcionalidade das restrições de direitos a propósito das escutas telefónicas*** *(dos dados de conteúdo), designadamente nos Acórdãos n.º 426/05 e n.º 4/06,* ***não são imediata e automaticamente transponíveis,*** *por ser relevante a falta de uma total identidade de razão,* ***para a recolha individualizada, caso a caso*** *– e é o que aqui está em causa –,* ***de dados de tráfego.***

4.22. O Conselheiro Teles Pereira sublinha, por outro lado, a **relação de complementaridade entre a actividade dos Serviços de Informações** e o **processo penal**, salientando, nesta matéria (ênfase desta Comissão):

"***10.1.*** *A primeira prende-se com o que poderíamos chamar de* ***geografia sistemática dos Serviços dedicados à função de produção de informações e do processo criminal.*** *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 44º, n.º 2 do Decreto n.º 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 5º, n.º 2 do Decreto n.º 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., 21º, 29º e 35º 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**."*

4.23. O Conselheiro Teles Pereira analisa, em seguida, o problema do acesso a "*dados de tráfego*" pelos Serviços de Informações à luz do **princípio da proporcionalidade** e **da proibição do excesso**, referindo, a este propósito (ênfase desta Comissão):

"*11.2. Testando a norma do artigo 78º, nº 2 do Decreto nº 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."*

4.24. Relativamente ao conceito de **verificação da proporcionalidade em sentido estrito**, refere, por outro lado, o Conselheiro Teles Pereira (ênfase desta Comissão):

> "*11.3. É mais complexa, no entanto – desde já se adianta –, a verificação da* ***proporcionalidade em sentido estrito****. Para concluir no sentido da "justa medida" da solução legislativa, importa considerar: (i) a* ***espécie de informação obtida****; (ii) a* ***escala da informação****; (iii) o* ***funcionamento das comissões de fiscalização****; e, face ao quadro precedente, concluindo, (iv) o* ***sentido das exigências de proporcionalidade****.*
>
> *A* ***espécie de informação obtida*** *é, como já se referiu,* ***pela sua natureza, limitada*** *(dados de tráfego) e, pese embora afete uma projeção da reserva da intimidade da vida privada,* ***não afeta esse tipo de informação, longe disso, essa intimidade projetiva, com uma intensidade igual ou mesmo equivalente à afetada pela informação resultante dos próprios dados de conteúdo****, que permanecem – é essa a opção do legislador português – inacessíveis aos Serviços de Informações.*
>
> *Mais importante para apurar o sentido da proporcionalidade é, todavia, o que designamos pela* ***escala da informação****. Como já referimos, atualmente, o debate internacional sobre a privacidade das comunicações tem como principais alvos sistemas muito complexos, alguns deles já referidos neste texto. Em tais casos, trata-se da* ***recolha sistemática de informações, realizada em massa****, com ténue ou sem qualquer circunscrição de pessoas, tempo e lugares, sem uma prévia verificação da utilidade concreta da grande maioria da informação recolhida, tendo em vista o seu tratamento posterior e assentando na expectativa da sua utilidade futura, para estabelecimento de conexões entre pessoas que venham a ser suspeitas de ameaçar ou de lesar os interesses do Estado. Tal recolha de informações é, na sua escala, absolutamente dissociada do que se prevê no artigo 78.º, n.º 2 do Decreto n.º 426/XII:* ***tão-só, um acesso pontual, delimitado por circunstâncias concretas, que tem de ser previamente solicitado a uma comissão independente, alegando e justificando a necessidade, adequação e proporcionalidade do acesso, por referência às atribuições legais dos Serviços de Informações****.*

Por outro lado, como já se assinalou, a atividade do SIRP é ***fiscalizada por três comissões independentes****, sendo que a sua atuação garante – especificamente a da* ***Comissão de Fiscalização de Dados do SIRP*** *– o* ***apagamento dos dados que não interessam à atividade dos serviços, por serem ou terem deixado de ser úteis****. Ademais – e é este um ponto de particular importância –, centrando a nossa atenção na* ***Comissão de Controlo Prévio****, à qual cabe em exclusivo autorizar o acesso aos dados de tráfego, é visível o esforço do legislador em encontrar um* ***justo equilíbrio dos interesses em jogo****. Tratando-se de uma comissão administrativa, não de um tribunal, a sua* ***composição por magistrados judiciais*** *visa importar para aquela Comissão uma particular cultura profissional de isenção, imparcialidade, independência e o saber, apurado pela longa experiência profissional, da aplicação do direito à luz dos princípios fundamentais do sistema jurídico, incluindo o da proporcionalidade. Aliás, é precisamente no n.º 2 do artigo 78.º do Decreto n.º 426/XII que repousa a chave do respeito pela proporcionalidade em cada concreta autorização a conceder, pois ali se prevê a aplicação do princípio, em cada adjetivação de pedidos de acesso formulados pelos Serviços de Informações.*

Acresce que, considerando o momento de atuação do SIRP, o ***legislador terá sentido grande dificuldade, ou mesmo encontrado barreira intransponível, na construção de um controlo jurisdicional*** *(isto é, propriamente, por um tribunal),* ***num momento em que não existe e poderá não vir a existir processo judicial****. E a solução que encontrou – que copia soluções existentes em diversos países da União Europeia, caso da Alemanha e do Reino Unido (cfr. Carlos Ruiz Miguel, "Problemas Actuales del Derecho de los Servicios de Inteligência", in Anuario de Derecho Constitucional Y Parlamentário, ano 2003, nº 15, p. 166) –, a solução encontrada, dizíamos, num compromisso possível com os interesses em jogo, consistiu na* ***criação de uma comissão administrativa (mas de feição para-judicial) que, na maior medida possível, replicasse o sentido profundo do controlo que, na sua dimensão mais literal, o n.º 4 do artigo 34.º entrega aos tribunais****. Precisamente a respeito da natureza de uma entidade de controlo do acesso aos dados de tráfego, salienta-se que o Acórdão, já referido neste*

*texto, do **Tribunal de Justiça** no Caso Digital Rights Ireland, Ltd (C-293/12), decisão de 8 de abril de 2014 – que invalidou a Diretiva n.º 2006/24/CE, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações – este Acórdão, dizíamos, tomou posição expressa no sentido do **controlo prévio não ter que assumir, necessariamente, natureza jurisdicional**, apontando a **necessidade de** "[...] **um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente cuja decisão vise limitar o acesso aos dados e a sua utilização ao estritamente necessário para se alcançar o objetivo prosseguido e ocorra na sequência de um pedido fundamentado** destas autoridades, apresentado no âmbito de **procedimentos de prevenção, de deteção** ou **de uma ação penal** [...]" (trecho do ponto 62 do Acórdão; destaque acrescentado), condições que o Decreto ora em apreciação, ao prever a Comissão de Controlo Prévio (e ao estabelecer os termos da respetiva atuação) assegura.*

*Por fim, não se esquecendo a profundidade com que o Tribunal tem entendido a necessidade de controlo da informação resultante da interceção de comunicações, não se pode deixar de notar que **nem todas as exigências implicadas na realização de escutas** (cfr., designadamente, os Acórdãos do Tribunal nº 426/2005 e nº 4/2006) **fazem sentido quando apenas estão em causa os dados de tráfego**. Ali, importa atentar no conteúdo das informações, para o mais rapidamente possível aferir da sua relevância, eliminando rapidamente o resultado lesivo (isto é, destruindo as escutas) na parte inútil, precisamente por respeito ao princípio da proporcionalidade, momentos e necessidades que não se reproduzem quando apenas estão em causa dados de tráfego.*

*Tudo visto e sopesado, afigura-se que **a solução encontrada pelo legislador implica**, usando o critério do Acórdão nº 187/2001, **efeitos restritivos ou lesivos que se apresentam, todavia, numa relação "calibrada" – de justa medida – com os fins prosseguidos**, ponderando aqueles efeitos face às medidas possíveis, tudo à luz do reconhecimento e outorga ao legislador do "crédito de confiança" que lhe é devido."*

4.25. E o Conselheiro Teles Pereira conclui, pois, a sua declaração de voto referindo (ênfase desta Comissão):

> "***12.*** *Aqui chegado, retomando as questões/dúvidas formuladas pelo Requerente no artigo 7º do pedido de fiscalização, responder-lhes-ia 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 78º, nº 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.*"

C – Apreciação na especialidade do Projecto de Lei 480/XIII-2ª

5. Artigo 1º do Projecto de Lei 480/XIII-2ª

5.1. O **artigo 1º** do Projecto de Lei estabelece o **modo** como se pretende proceder às alterações legislativas propostas: alteração da **Lei 30/84**, de 5 de Setembro (**Lei Quadro do Sistema de Informações da República Portuguesa**), bem como da **Lei 62/2013**, de 26 de Agosto (**Lei de Organização do Sistema Judiciário**).

A introdução de alterações à **Lei 30/84** (Lei-Quadro do SIRP) é um modelo possível de intervenção legislativa, na esteira, aliás, da iniciativa legislativa (**Decreto 426/XII** da Assembleia da República), que determinou a prolação do **Acórdão 403/15** do Tribunal Constitucional, a que acima se aludiu.

Mas não é a única. Pode, com efeito, conceber-se a introdução de alterações legislativas, como as propostas, em **lei extravagante de natureza penal**, por exemplo, no âmbito da **Lei 52/2003**, de 22 de Agosto (Lei de Combate ao Terrorismo) ou mesmo da **Lei 25/2008**, de 5 de Junho (Lei do Combate ao Branqueamento de Capitais e do Financiamento ao Terrorismo).

Por um lado, por esta via, acentuar-se-ia o escopo principal de **combate ao terrorismo**, que está na base das alterações legislativas propostas.

Por outro, talvez se revelasse mais fácil incluir, num diploma extravagante, uma disposição relativa à necessidade de uma sua **avaliação posterior**, tendo em vista comprovar a justeza e eficácia das suas disposições, bem como suprir eventuais problemas decorrentes da sua aplicação.

Ora, uma tal revisão será seguramente mais fácil num diploma extravagante, do que numa Lei-Quadro como a **Lei-Quadro do SIRP**, lei orgânica com um processo de aprovação agravado (cfr. art. 166°, n° 2, alínea q) e 168°, n° 5 da Constituição).

5.2. Segundo o art. 1° do Projecto de Lei em apreciação, a nova lei pretende estabelecer «... *a competência e o procedimento de acesso por funcionários e agentes dos serviços de informações da República Portuguesa ... a dados de tráfego, de localização ou outros dados conexos das comunicações ...*».

Define, pois, **quem deverá aceder** («... *funcionários e agentes dos Serviços de Informações da República Portuguesa*»).

Define, também, **o tipo de informação** a que se acede (os chamados metadados - «... *dados de tráfego, de localização ou outros dados conexos das comunicações ...*»).

Define, ainda, a **finalidade da recolha** («... *cumprimento das atribuições legais desses serviços*»).

Define, por último, a **forma de autorização** desse acesso («... *mediante autorização judicial prévia a cargo de secção especial para autorização de acesso a informações e a dados do Supremo Tribunal de Justiça...*»).

Tal como está formulado, o **artigo 1°** do Projecto de Lei 480/XIII-2ª não suscita reparos a esta Comissão.

6. Artigo 2º do Projecto de Lei 480/XIII-2ª

6.1. Alteração ao artigo 2º da Lei 30/84

O Projecto de Lei em apreciação pretende introduzir alterações no **número 2 do artigo 2º** da Lei 30/84.

Julga-se, todavia, que a **alínea a)** do respectivo articulado deverá incluir ainda uma referência, como na actual versão da Lei-Quadro do SIRP, à noção de «... *unidade e integridade do Estado*».

Quanto à **alínea b),** sugere-se a substituição de «*cidadãos*», por «***pessoas***», uma vez que as condições de segurança devem aplicar-se a todos os que se encontrem sujeitos à jurisdição do Estado português, independentemente da respectiva nacionalidade, ou falta dela.

A **alínea c)** reporta-se aos 4 **fenómenos criminais particularmente graves**, cuja prevenção justifica a produção de informações por parte dos Serviços que integram o SIRP: **sabotagem, espionagem, terrorismo e sua proliferação, criminalidade altamente organizada de natureza transnacional**.

Este elenco merece, pela sua delimitação, a concordância desta Comissão.

6.2. Alteração ao artigo 5º da Lei 30/84

6.2.1. As alterações propostas para o **art. 5º** da Lei-Quadro do SIRP suscitam algumas dúvidas a esta Comissão,

Com efeito, na sua redacção actual, o referido art. 5º ocupa-se do **acesso a dados e informações, detidos por Serviços de Segurança, por parte de** «***funcionários e agentes, civis ou militares, que exercem funções policiais***».

No entanto, na redacção agora proposta do Projecto de Lei em apreciação, ao que se crê inspirada pelo art. 78º, nº 1, do Decreto 426/XII, parece pretender-se que a disposição em causa se passe a aplicar apenas a **pessoal dos próprios Serviços de Informações**.

Ficaria, assim, sem regulamentação expressa, o **acesso a dados dos Serviços de Informações por parte de pessoal exterior aos mesmos Serviços** («*funcionários e agentes, civis ou militares, que exercem funções policiais*»), o que se considera de todo inconveniente.

6.2.2. A ser correcta esta interpretação, o **número 1** da disposição proposta para substituir o artº 5º da Lei-Quadro do SIRP deveria reportar-se a «*funcionários e agentes dos serviços de informações do SIS e do SIED*» (como se encontra, por exemplo, no número 2 do mesmo artigo do Projecto de Lei em apreciação). De outra forma, não se vê por que razão a matéria contida neste número 1 do Projecto de Lei em apreciação deverá constar da Lei-Quadro do SIRP.

Por outro lado, há que referir que o acesso 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 Protecção de Dados no quadro das suas competências próprias*» não chegou a ser apreciado pelo Tribunal Constitucional, no Acórdão 403/15, a que atrás se fez referência, sendo duvidoso que, em face do **princípio da finalidade da recolha**, previsto no art. 5º, nº 1, alínea b) da Lei 67/98, de 26 de Outubro, tal acesso venha a ser viabilizado pela CNPD.

6.2.3. O **número 2** do mesmo art. 5° prevê o acesso a **informação bancária e fiscal**, matéria que, como se viu, não foi também tratada pelo Tribunal Constitucional no **Acórdão 403/15** (cfr. supra n° 4.3. do presente Parecer).

A disposição delimita, por outro lado, o restante tipo de informação a que se pretende aceder: «... ***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 hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização***».

O Tribunal Constitucional considerou, como se viu, que os **dados de tráfego** e **de localização** deverão estar sujeitos à mesma disciplina jurídica (cfr. supra n° 4.6. do Presente Parecer), muito embora apenas os primeiros (**dados de tráfego**, tal como os dados de conteúdo), se possam encontrar abrangidos pela **proibição** constante do art. 34°, n° 4 da Constituição, mas já não os segundos (dados de localização) (cfr. supra n° 4.8. do presente Parecer).

Trata-se, na redacção do Projecto de Lei em apreciação para o número 2 do art. 5° da Lei-Quadro do SIRP, de precisão que corresponde *grosso modo* ao conteúdo do n° 2 do art. 78° do Decreto 426/XII, a que atrás se fez referência (cfr. por exemplo supra 4.3. do presente Parecer).

Por isso, para além das observações feitas sobre informação bancária e fiscal, a presente disposição não suscita reparos a esta Comissão, tendo havido o cuidado de prever que o acesso à informação, por parte dos funcionários e agentes dos Serviços que integram o SIRP, deva ter lugar «... ***para efeitos do disposto na alínea c) do n° 2 do artigo 2°, e no seu exclusivo âmbito***».

É duvidoso, porém, que, desta forma, se haja respondido cabalmente às principais objecções suscitadas pelo Tribunal Constitucional no seu Acórdão 403/15 (cfr. designadamente supra nºs 4.9., 4.10. e 4.11. do presente Parecer).

6.2.4. A redacção proposta para **o número 3** do art. 5º da Lei-Quadro do SIRP também suscita dúvidas a esta Comissão.

Com efeito, esta disposição parece ter em vista determinar que o acesso à informação, por parte dos Serviços de Informações, seja uma medida de último recurso («... *quando não exista outro meio que permita a salvaguarda eficaz e atempada dos bens jurídicos a proteger* ...»).

Nessa medida, justificar-se-ia que esta disposição se reportasse quer à **autorização referida no número 1** (acesso a ficheiros detidos por entidades públicas), **quer à referida no número 2** (acesso a informação bancária e fiscal, dados de tráfego, localização ou outros dados conexos das comunicações).

A redacção proposta procura, por outro lado, circunscrever o acesso à informação em função do **respeito pelo princípio da proporcionalidade** e pelo **princípio da finalidade do acesso**, embora, certamente por lapso, se refira o artigo 5º, **em vez do artigo 2º** da Lei-Quadro do SIRP («... *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 artigo 5º*»).

6.2.5. Esta Comissão vê virtualidades na preocupação expressa na redacção proposta para o **número 4** do art. 5º da Lei-Quadro do SIRP: **uma autorização para cada pedido**, embora combinando várias medidas no âmbito da mesma acção.

Uma tal preocupação poderá, no entanto, vir a revelar-se, por vezes, de difícil execução prática: uma autorização por pessoa sujeita à medida de ingerência? Uma autorização por acção a desenvolver relativamente a um mesmo quadro factual?

Talvez conviesse, por isso, precisar um pouco melhor o sentido da disposição em causa.

6.2.6. O **número 5** da redacção proposta para o art. 5º da Lei-Quadro do SIRP suscita, da mesma forma, dúvidas a esta Comissão.

Pretende-se, aqui, como tudo parece indicar, prever a situação de **funcionário** ou **agente dos Serviços de Informações** comunicar ou fazer uso de **informações** e de **dados** que lhe tenham sido confiados?

Deverá, por outro lado, tal violação contemplar, apenas, a situação prevista no **número 2** desta disposição, ou igualmente a prevista no **número 1**?

Crê-se que a solução deveria ser idêntica para ambos os casos.

De qualquer modo, haverá que ver como se poderá compatibilizar esta disposição com o disposto nos nºs 4 e 5 do art. 28º da Lei-Quadro do SIRP, que se mantém em vigor e que prevê uma moldura penal diferente.

7. Artigo 3º do Projecto de Lei 480/XIII-2ª

7.1. Alteração ao art. 47º da Lei 62/13

7.1.1. O **artigo 3º** do Projecto de Lei em apreciação introduz alterações aos **arts. 47º** e **66º** da **Lei 62/13**, de 26 de Agosto (**Lei da Organização do Sistema Judiciário**).

O **art. 47º** respeita á **organização** do **Supremo Tribunal de Justiça**, pretendendo-se, agora, a criação de uma **secção especial para autorização de acesso a informação e a dados**, dentro da **secção em matéria criminal** do mesmo Supremo Tribunal.

A referida secção especial será constituída por **3 juízes** da secção criminal do Supremo Tribunal de Justiça, **anual** e **sucessivamente designados**, cabendo a um juiz as funções de relator e aos outros juízes as funções de adjuntos.

7.1.2. A redacção proposta pretende, ao que se julga, responder às várias objecções suscitadas no Acórdão 403/15 do Tribunal Constitucional, relativas à criação de uma **Comissão de Controlo Prévio**, prevista no Decreto 426/XII.

Como se viu (cfr. supra nºs 4.12. do presente Parecer), o Tribunal Constitucional considerou, então, que «... *aquela Comissão tem a natureza de órgão administrativo não inserido jurídico normativamente na organização judicial, pese embora a qualidade dos seus membros. De facto, do ponto de vista formal ou orgânico, não exerce a função judicial e, do ponto de vista material, não exerce a função jurisdicional*» (cfr. ainda nºs 4.13., 4.16., 4.22. e 4.24 do presente Parecer).

A solução agora encontrada parece, todavia, satisfazer estas preocupações do Tribunal Constitucional, uma vez que se prevê a intervenção de uma **secção do Supremo Tribunal de Justiça, composta por juízes conselheiros em funções no mesmo Tribunal**, assegurando, pois, os necessários requisitos de **independência** e **imparcialidade** que devem caracterizar a respectiva actuação.

7.1.3. Algumas dúvidas poderão colocar-se, porém, quanto à eficácia do modelo proposto.

Desde logo, o **mandato** previsto («*anual e sucessivamente designados* ...»). Pode este mandato ser renovado? Por quantas vezes?

Por outro lado, se não for renovável o mandato, como assegurar que os magistrados envolvidos possam, no decurso apenas de 1 ano, dispor de tempo suficiente para assegurar uma adequada especialização da sua intervenção?

Chegará, por outro lado, uma altura em que, não havendo renovação de mandato, se acabará por esgotar a possibilidade de designação de novos Juízes Conselheiros para esta secção, uma vez que todos os Juízes Conselheiros da secção criminal do Supremo Tribunal de Justiça terão nela já participado.

Ora, como compatibilizar uma tal solução com a necessidade de assegurar o devido respeito pelo segredo de Estado e pela desejável participação de um conjunto limitado de pessoas neste processo de autorização?

Cabe, também, perguntar se as funções de relator são desempenhadas sempre pelo mesmo magistrado ou se serão objecto de rotação entre os 3 membros da secção.

7.1.4. Por último, coloca-se o problema da própria praticabilidade da solução. Prevê-se, no Projecto de Lei em apreciação, como se verá mais adiante, **tempos de reacção muito curtos** para esta secção especializada do Supremo Tribunal de Justiça (entre 24h e 48h). Ora, muitos Juízes Conselheiros nem sequer residem em Lisboa, não estando, por isso, facilmente acessíveis para intervenção em espaço de tempo tão exíguo. E durante o período de férias judiciais, como se deverá proceder?

Para além de haver necessidade de assegurar, no mesmo período de tempo, uma adequada articulação com o Ministério Público, como se verá também.

Questões, pois, que conviria ponderar devidamente em sede legislativa.

Importa, por último, estabelecer, nas disposições transitórias, um **prazo para a designação deste colectivo de Juízes Conselheiros** após a entrada em vigor da nova lei, de forma a que o início de vigência das alterações propostas não resulte prejudicada com a ausência de tal designação.

7.2. Alteração ao art. 66º da Lei 62/13

O Projecto de Lei em apreciação prevê, também, uma alteração ao **art. 66º** da **Lei 62/13**, no âmbito da representação do **Ministério Público** no **Supremo Tribunal de Justiça**, estabelecendo-se, à semelhança do que acontece com os Juízes Conselheiros que integram a secção especializada a que atrás se fez referência, que o Procurador-Geral da República designará anualmente um **Procurador-Geral Adjunto** para actuar junto da mesma secção.

Suscitam-se, aqui, porém, algumas das objecções atrás enunciadas quanto à eficácia da solução, uma vez que o referido magistrado do Ministério Público poderá de ter de intervir em qualquer altura, pelo que terá de estar disponível para tanto.

Por outro lado, a possibilidade da substituição anual deste magistrado poderá acarretar considerável prejuízo para a sua eficácia, prejudicando a recolha da necessária experiência no exercício destas funções.

E o problema decorrente da observância do período de férias judiciais também se verifica aqui.

Conviria, por último, prever também, nas disposições transitórias, um prazo para a designação deste magistrado, após a entrada em vigor da nova lei.

8. Artigo 4º do Projecto de Lei 480/XIII-2ª

8.1. Aditamento do artigo 5º-A à Lei 30/84

8.1.1. O **artigo 4º** do Projecto de Lei em apreciação prevê o aditamento de três novos artigos à Lei 30/84 (Lei-Quadro do SIRP): os **artigos 5º-A, 5º-B** e **5º-C**.

Embora se compreenda a preocupação de clareza que poderá estar na base da técnica legislativa utilizada, talvez conviesse, porém, que todas as alterações à Lei 30/84 estivessem colocadas umas a seguir às outras, em vez de haver uma primeira referência a esta lei (cfr. artigo 2º do Projecto de Lei), uma alteração à Lei 62/13 (artigo 3º do Projecto) e, novamente, uma alteração à Lei 30/84 (artigo 4º do Projecto).

8.1.2. O aditamento do **artigo 5º-A** à Lei 30/84 não suscita reparos a esta Comissão,

Pretende-se, com efeito, precisar que a **competência para a concessão de autorização para o acesso**, quer a **informação contida em ficheiros de entidades públicas**, quer a **informação bancária** e **fiscal**, quer, ainda, a **dados de tráfego, de localização** ou **outros dados conexos das comunicações**, pertence ao **colectivo de 3 juízes** da secção especial para autorização de acesso a informação e a dados do Supremo Tribunal de Justiça.

Esclarece-se, todavia, que a **iniciativa** cabe ao magistrado do Ministério Público junto da mesma secção (« ... *a requerimento do procurador-geral adjunto* ...»), o que consagra uma solução de **partilha de responsabilidades entre ambas as magistraturas**, que se crê útil, por oferecer **acrescidas garantias de protecção** para as pessoas visadas com tal ingerência.

8.2. Aditamento do artigo 5º-B à Lei 30/84

8.2.1. Nos termos do **número 1** do novo **artigo 5º-B**, «*o **pedido de acesso às informações e aos dados a que alude o nº 2 do artigo 5º, é apresentado por escrito pelos Directores** 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 ...*» (cfr. art. 37º, nº 1 do Decreto 426/XII).

Estabelece-se, assim, pela sua particular danosidade, a **intervenção dos dirigentes máximos** dos dois Serviços de Informações nacionais no **pedido de acesso, devidamente apresentado por escrito**, a «*...informação bancária, informação fiscal, dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fotne, 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*» (cfr. número 2 da nova versão proposta para o artigo 5º da Lei-Quadro do SIRP, constante do artigo 2º do Projecto de Lei em apreciação).

8.2.2. Por outro lado, nos termos da mesma disposição, o pedido de acesso conterá os seguintes elementos (ênfase desta Comissão):

"*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 **afectadas 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*".

Crê-se que a **definição dos elementos** que deverão acompanhar o pedido de acesso, constantes já do art. 37°, n° 2, Decreto 426/XII, revelam uma preocupação de rigor, que cabe, aqui, assinalar.

Conviria, todavia, ponderar a necessidade de uma **acrescida preocupação de fundamentação** relativamente aos **pedidos de renovação das medidas requeridas**, de forma a evitar que as razões apontadas se limitem a reproduzir fundamentação anteriormente apresentada, sem qualquer preocupação de fundamentação adicional.

E, também, definir, se possível, um **prazo limite** para a renovação destas medidas.

8.2.3. O **número 4** do novo artigo 5°-B, estabelece que a **decisão de concessão** ou de **denegação do acesso à informação** pretendida é do **colectivo de juízes** e não já, como constava do n° 3 do art. 37° do Decreto 426/XII, do juiz a quem o pedido houvesse sido distribuído (embora, em casos de particular complexidade, se previsse a intervenção do colectivo de juízes). Acentua-se, desta forma, o **carácter colegial** da intervenção da secção especial do Supremo Tribunal de Justiça que se ocupa destes pedidos.

Por outro lado, estabelece-se que a decisão deve ser proferida no **prazo máximo de 48 horas**, o que pretende vincar a natureza urgente deste tipo de intervenção (o n° 4 do art. 37° do Decreto 426/XII previa, a este propósito, um prazo normal de intervenção mais longo, de 72 horas).

8.2.4. De sublinhar, todavia, que o **número 5** do mesmo artigo veio contemplar a redução, para **24 horas**, do prazo máximo para a decisão judicial ser proferida, «*em situações de urgência, devidamente fundamentadas no pedido dos serviços de informações...*».

Uma tal situação de urgência encontrava-se igualmente contemplada no nº 5 do art. 37º do Decreto 426/XII.

8.2.6. O **número 6** do novo artigo 5º-B, à semelhança do já estabelecido no nº 6 do art. 37º do Decreto 426/XII, veio, compreensivelmente determinar, dado o tipo de informação a que se pretende aceder, que «... *o procedimento previsto no presente artigo é coberto pelo regime do segredo de Estado nos termos do artigo 32º*».

8.2.7. O **número 7** do novo artigo 5º-B, correspondente ao nº 7 do art. 37º do Decreto 426/XII, determina que o «*Secretário-Geral ordena a destruição imediata de todos os dados e informação recolhidos, mediante a autorização prevista no presente artigo, sempre que não tenham relação com o objecto ou finalidades da mesma*».

Compreende-se a razão desta disposição, destinada a prevenir que eventual informação recolhida, mas não relacionada com o objecto ou finalidade da autorização judicial concedida, possa vir a ser utilizada pelos Serviços de Informações, em vez de ser de imediato destruída, por extravasar de uma tal autorização (cfr., por exemplo, as preocupações expressas pelo Tribunal Constitucional, supra nº 4.15. do presente Parecer).

Julga-se, todavia, que se justifica haver um **registo** de tal destruição, devendo essa informação ser igualmente **comunicada**, não só ao **magistrado do Ministério Público** e ao **colectivo de juízes** que intervieram na autorização concedida, mas também a esta **Comissão de Fiscalização de Dados**, à semelhança do que se prevê para o **número 8** deste mesmo artigo 5º-B.

8.2.8. O **número 8** do novo artigo 5º-B, correspondente ao nº 8 do art. 37º do Decreto 426/XII, determina que «*por decisão do colectivo de juízes, pode ser determinado o cancelamento de quaisquer procedimentos de acesso a informação e a dados previstos no nº 2 do artigo 5º, bem como participados à Comissão de Fiscalização de Dados do SIRP os elementos conducentes à destruição imediata dos respectivos dados ou informações*».

Compreende-se a necessidade de prever uma tal disposição. Com efeito, ao colectivo de juízes cabe, não só **autorizar** ou **denegar o acesso** a determinado tipo de informação, prevista na nova redacção proposta para o artigo 5º da Lei-Quadro do SIRP, mas igualmente **prorrogar a duração das medidas requeridas** e **cancelar ou revogar a autorização previamente concedida** para o acesso a tal informação.

Julga-se, todavia, que se devia prever igualmente a possibilidade de o **magistrado do Ministério Público** poder **requerer**, ao colectivo de juízes, um tal **cancelamento**, uma vez que lhe coube requerer inicialmente a autorização para o acesso a esta informação.

Por outro lado, a comunicação da **decisão de cancelamento**, a esta **Comissão de Fiscalização de Dados, de quaisquer procedimentos de acesso a informação e a dados** previstos no nº 2 do art. 5º só fará sentido se a informação recolhida tiver, entretanto, sido **integrada nas bases de dados** de qualquer um dos Serviços de Informações nacionais.

De outra forma, caberá eventualmente ao **Conselho de Fiscalização do SIRP** velar por que esta informação, constante de outros suportes de informação, seja efectivamente destruída.

8.3. Aditamento do artigo 5º-C à Lei 30/84

8.3.1. Vejamos, por último, o **novo artigo 5º-C** proposto para a Lei-Quadro do SIRP, relativo à «*transmissão, tratamento, manutenção e destruição das informações e dados*».

Esta disposição procura responder a algumas das objecções feitas, pelo Acórdão 403/15, ao Decreto 426/XII, em matéria de **segurança de transmissão da informação e de dados** (cfr. designadamente supra nº 4.15. do presente Parecer).

Assim, o **número 1** desta disposição refere que «*a **transmissão dos dados** previstos no nº 2 do artigo 5º **é feita por comunicação electrónica, de acordo com o disposto nos diplomas que estabelecem os termos das condições técnicas e de segurança em que se processa a comunicação electrónica para efeitos da transmissão de dados de tráfego e de localização** relativos a pessoas singulares e a pessoas colectivas, **bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado***» (ênfase desta Comissão).

Este número não suscita objecções a esta Comissão.

8.3.2. O **número 2** desta disposição, dando seguimento a preocupação idêntica, refere, complementarmente, que «*sem prejuízo do disposto no número anterior, as **entidades** às quais incumba garantir a protecção e segurança dos dados **devem assegurar-se que a transmissão dos dados** previstos no nº 2 do artigo 5º **respeita um grau de codificação e***

***protecção o mais elevado possível**, de acordo com o estado da técnica ao momento da transmissão, **incluindo métodos de codificação, encriptação** ou **outros adequados**».*

Este número também não suscita reparos a esta Comissão.

8.3.3. Também não suscita reparos a esta Comissão o **número 3** desta disposição, que refere que «*o disposto nos números anteriores não prejudica a observância dos princípios nem o cumprimento das regras aplicáveis previstos nas Leis nºs 67/98, de 26 de Outubro e 41/2004, de 18 de Agosto*».

A **Lei 67/98**, de 26 de Outubro é a **Lei de Protecção de Dados Pessoais** e a **Lei 41/2004**, de 18 de Agosto, transpôs para a ordem jurídica nacional a **Directiva n.º 2002/58/CE**, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao **tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas**.

8.3.4. Finalmente, o **número 4** do novo artigo 5º-C da Lei 30/84 veio determinar que, «***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**»* (ênfase desta Comissão).

Ora, à semelhança do que anteriormente se expôs (cfr. supra nº 8.2.8. deste Parecer), a intervenção desta Comissão de Fiscalização de Dados está, em princípio, circunscrita a **informação constante das bases de dados** de ambos os Serviços de Informações.

De alguma forma, a referência à necessidade de **legislação especial** decorrerá das preocupações expressas pelo Tribunal Constitucional no Acórdão 403/15 (cfr. por exemplo supra, nº 4.15. do presente Parecer).

Todavia, grande parte destas preocupações, pelo menos na parte respeitante à informação constante das bases de dados dos Serviços de Informações, poderá ser devidamente acautelada no novo Regulamento dos Centros de Dados dos referidos Serviços, em curso de ultimação.

9. Conclusões

9.1. A apresentação do **Projecto de Lei 480/XIII-2ª** procura acautelar muitas das preocupações expressas pelo Tribunal Constitucional no seu **Acórdão 403/15**, que apreciou o art. 78º, nº 2 do Decreto 426/XII.

Assim, procurou-se delimitar, de forma mais criteriosa, o eventual **acesso**, por **funcionários** e **agentes** dos **Serviços de Informações da República Portuguesa** a **dados de tráfego**, de **localização** ou **outros dados conexos das comunicações**, especificando os **dados** a que se poderá aceder, embora sem deixar de salientar que se tratará de uma **medida de *ultima ratio***, quando não exista outro meio de intervenção possível, que permita atingir os mesmos objectivos.

Para o efeito, procurou-se precisar, melhor, as **finalidades** a prosseguir com tal acesso, quer **colectivas** (salvaguarda da independência nacional, dos interesses nacionais e da segurança interna e externa do Estado Português, bem como do adequado funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de Direito), quer **individuais** (segurança das pessoas).

Procurou-se, por outro lado, definir os **crimes** que especificamente se desejam prevenir com esta ingerência (crimes particularmente graves: **sabotagem, espionagem, terrorismo** e sua **proliferação** e a **criminalidade altamente organizada de natureza transnacional**).

Definiu-se, ainda, a **necessidade de intervenção das autoridades judiciárias no procedimento de autorização** e **no ulterior acompanhamento das medidas decretadas** (Ministério Público e colectivo de Juízes Conselheiros do Supremo Tribunal de Justiça, integrando uma secção especialmente criada para o efeito), bem como os **trâmites** a seguir para obter uma tal autorização.

Acautelaram-se, por último, **condições de segurança** na transmissão dos dados e informações, bem como as **situações** em que a informação recolhida deverá ser **destruída**.

Assim, embora com as sugestões de alteração propostas ao longo do presente Parecer, o Projecto de Lei em apreciação estará em condições de merecer parecer favorável por parte desta Comissão de Fiscalização de Dados.

9.2. É, porém, duvidoso que o Projecto de Lei 480/XIII satisfaça integralmente as exigências estabelecidas pelo Tribunal Constitucional no seu **Acórdão 403/15**, relativamente à interpretação que fez do art. 34°, n° 4 da Constituição, designadamente sobre os conceitos de «*ingerência nas comunicações*» e dos «*casos previstos na lei em matéria de processo criminal*».

É bem certo que a redacção deste preceito é praticamente idêntica à versão originária da Constituição, com excepção do termo «*demais meios de comunicação*».

É, por isso, duvidoso, como expresso na declaração de voto do Conselheiro Teles Pereira (cfr supra nº 4.18. do presente Parecer), que o legislador constitucional tenha tido em mente, quando redigiu o texto original da Constituição ou preparou a revisão constitucional de 1997, um conceito de **ingerência nas telecomunicações** que abrangesse não só **dados de conteúdo**, como, também, **dados de tráfego**.

9.3. É difícil de antever, pois, se o Tribunal Constitucional, na sua actual composição, manterá a rigorosa interpretação que fez vencimento no Acórdão 403/15, relativamente ao conceito de «*casos previstos na lei em matéria de processo criminal*», e à estrita separação entre actividade de produção de informações e processo criminal, que pouca, se é que alguma, flexibilidade deixa para uma qualquer hipótese de acesso a dados de tráfego, por parte dos Serviços de Informações nacionais, fora do quadro de uma eventual revisão da Constituição.

Ou se, pelo contrário, quererá explorar as virtualidades da ideia deixada pela Conselheira Maria Lúcia Amaral na sua declaração de voto, segundo a qual «... *havendo afinidade valorativa ou teleológica entre as finalidades prosseguidas pelos serviços de informações e as normas penais incriminadoras ... a autorização constitucional para restringir a inviolabilidade das telecomunicações em «matérias de processo criminal», se estenderia, por maioria de razão, aos Serviços de Informações da República*» (cfr. supra nº 4.17. do presente Parecer).

9.4. Ou, ainda, pegando na noção de «***actos administrativos de defesa da Constituição***», a que alude a Conselheira Maria Lúcia Amaral na sua declaração de voto (cfr. supra nº 4.17. do presente Parecer), ou de «***protecção administrativa da Constituição***», a que alude o Conselheiro Teles Pereira na sua declaração de voto, o Tribunal Constitucional

virá a reconhecer a **produção de informações** como «*um sistema estruturado em vista do desencadear de mecanismos de alerta prévio, uma função sequencialmente referida ainda a um momento anterior ao da entrada em jogo – rectius, da adjectivação – da tutela penal, mas que, nem por isso, deixa de estar ligada aos valores específicos (aos tipos) abarcados pela lei penal, e de poder mesmo vir a entroncar na adjectivação penal*» (cfr. supra nº 4.19. do presente Parecer).

Acabando, assim, por reconhecer alguma virtualidade na ideia (cfr. supra nº 4.22. do presente Parecer), de que «... *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 nº 426/XII e se desenvolve actividades 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 44º, n.º 2 do Decreto n.º 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 5º, n.º 2 do Decreto n.º 426/XII)».

Sobretudo se atentar que se não trata de recolha de informação em larga escala, mas de **recolha individualizada** e que, como tal, **com menor incidência, e de menor intensidade, na protecção da reserva da vida privada das pessoas objecto de ingerência**.

Estas, pois, as observações que o Projecto de Lei 480/XIII-2ª, em apreciação, suscita a esta Comissão.

Lisboa, 15 de Maio de 2017

A Comissão de Fiscalização de Dados

José Manuel Santos Pais