ASSEMBLEIA DA REPÚBLICA

CONSELHO DE FISCALIZAÇÃO DO SISTEMA DE INFORMAÇÕES DA REPÚBLICA PORTUGUESA

PARECER

1. A Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias solicitou a este Conselho de Fiscalização (CFSIRP) o seu parecer sobre o **Projeto de Lei n.º 480/XIII-2.ª (CDS-PP)** – ***"Acesso a dados de tráfego, de localização ou outros dados conexos das comunicações por funcionários e agentes dos serviços de informações da República portuguesa"***.

É o seguinte o *articulado* do referido Projeto de Lei:

> **«Artigo 1.º (Objeto)**
> A presente lei altera a Lei n.º 30/84, de 5 de Setembro (Lei Quadro do Sistema de Informações da República Portuguesa) e a Lei n.º 62/2013, de 26 de Agosto (Lei de Organização do Sistrema Judiciário) estabelecendo a competência e o procedimento de acesso por funcionários e agentes dos serviços de informações da República Portuguesa, mediante autorização judicial prévia a cargo da secção especial para autorização de acesso a informação e a dados do Supremo Tribunal de Justiça, a dados de tráfego, de localização ou outros dados conexos das comunicações, para cumprimento das atribuições legais desses serviços.
>
> **Artigo 2.º (Alteração à Lei n.º 30/84, de 5 de Setembro)**
> Os artigos 2.º e 5.º da Lei n.º 30/84, de 5 de Setembro, passam a ter a seguinte redação:
>
> "Artigo 2.º [...]
> 1 – .....
> 2 — Aos serviços de informações incumbe desenvolver, no respeito da Constituição e da lei, atividades de recolha, processamento, exploração e difusão de informações:
> a) Necessárias à salvaguarda da independência nacional, dos interesses nacionais e da segurança interna e externa do Estado Português;
> b) Que contribuam para garantir as condições de segurança dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de Direito e adequadas a prevenir a prática de atos que, pela

sua natureza, possam alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido.
c) Adequadas a prevenir a sabotagem, a espionagem, o terrorismo e sua proliferação, nos termos da lei de combate ao terrorismo, e a criminalidade altamente organizada de natureza transnacional.

Artigo 5.º [...]

1 - Os funcionários e agentes, civis ou militares, têm acesso, mediante autorização judicial a conceder nos termos da presente lei, a informação e registos relevantes para a prossecução das suas competências, contidos em ficheiros de entidades públicas, nos termos de protocolo, ouvida a Comissão Nacional de Proteção de Dados no quadro das suas competências próprias.
2 - Os funcionários e agentes dos serviços de informações do SIS e do SIED podem, para efeitos do disposto na alínea c) do n.º 2 do artigo 2.º, e no seu exclusivo âmbito, aceder a informação bancária, a informação fiscal, a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização.
3 - A autorização referida no número 1 é concedida quando não exista outro meio que permita a salvaguarda eficaz e atempada dos bens jurídicos a proteger e houver razões para crer que o acesso aos dados solicitados é indispensável, adequada e proporcional para prevenir a prática dos crimes previstos na alínea c) do n.º 2 do artigo 5.º.
4 - Para cada pedido deve ser emitida uma única autorização, que pode combinar várias medidas no âmbito da mesma ação.
5 – O funcionário e agente que comunicar ou fizer uso de informações e de dados em violação do disposto no n.º 2 será punido com pena de prisão até 3 anos, se pena mais grave não lhe for aplicável, independentemente da medida disciplinar que ao caso couber".

Artigo 3.º (Alteração à Lei n.º 62/2013, de 26 de Agosto)

Os artigos 47.º e 66.º da Lei n.º 62/2013, de 26 de Agosto, passam a ter a seguinte redação:

"Artigo 47.º [...]

1- (...).
2 – Dentro da secção em matéria penal funciona uma secção especial para autorização de acesso a informação e a dados.
3 - A secção especial referida no número anterior é constituída por três juízes da secção penal do Supremo Tribunal de Justiça, anual e

sucessivamente designados, cabendo a um juiz as funções de relator e aos outros juízes as funções de adjuntos.
4 – (anterior n.º 2).
5 – (anterior n.º 3).

Artigo 66º [...]

1 – (...).
2 – (...).
3 – O Procurador-Geral da República designa anualmente um procurador-geral-adjunto junto da secção especial para autorização de acesso a informação e a dados.
4 – (anterior n.º 3).

Artigo 4.º (Aditamento à Lei n.º 30/84, de 5 de Setembro)
São aditados os artigos 5.º-A e 5.º-B à Lei n.º 30/84, de 5 de Setembro, com a seguinte redação:

"Artigo 5.º-A (Competência para a concessão de autorização)
A competência para a concessão da autorização prevista no artigo 5.º pertence ao coletivo de juízes da secção especial para autorização de acesso a informação e a dados do Supremo Tribunal de Justiça, a requerimento do procurador-geral-adjunto junto da mesma secção, sem prejuízo do disposto na presente lei.

Artigo 5.º-B (Procedimento do pedido de autorização)
1 - O pedido de acesso às informações e aos dados a que alude o n.º 2, do artigo 5.º, é apresentado por escrito pelos Diretores do SIS ou do SIED ao procurador-geral adjunto junto da secção especial para autorização de acesso a informação e a dados do Supremo Tribunal de Justiça e contém os seguintes elementos:

a) Indicação concreta da ação operacional a realizar e das medidas requeridas;
b) Factos que suportam o pedido, finalidades que o fundamentam e razões que aconselham a adoção das medidas requeridas;
c) Identificação da pessoa ou pessoas, caso sejam conhecidas, envolvidas nos factos referidos na alínea anterior e afetadas pelas medidas e indicação do local onde as mesmas devam ser realizadas;
d) Duração das medidas requeridas, que não pode exceder o prazo máximo de três meses, prorrogáveis mediante autorização expressa.

4 – O coletivo de juízes profere decisão de concessão ou de denegação da autorização por despacho fundamentado, proferido no prazo máximo de 48 horas.

5 - Em situações de urgência, devidamente fundamentadas no pedido dos serviços de informações, pode ser solicitada a redução para 24 horas do prazo previsto no número anterior.
6 - O procedimento previsto no presente artigo é coberto pelo regime do segredo de Estado nos termos do artigo 32.º.
7 - 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 objeto ou finalidades da mesma.
8 - Por decisão do coletivo de juízes, pode ser determinado o cancelamento de quaisquer procedimentos de acesso a informação e a dados previstos no n.º 2 do artigo 5.º, bem como participados à Comissão de Fiscalização de Dados do SIRP os elementos conducentes à destruição imediata dos respetivos dados ou informações.

Artigo 5.º-C (Transmissão, tratamento, manutenção e destruição das informações e dados)

1 — A transmissão dos dados previstos no n.º 2 do artigo 5.º é feita por comunicação eletrónica, de acordo com o disposto nos diplomas que estabelecem os termos das condições técnicas e de segurança em que se processa a comunicação eletrónica para efeitos da transmissão de dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado.
2 — Sem prejuízo do disposto no número anterior, as entidades às quais incumbe garantir a proteção e segurança dos dados devem assegurar-se que a transmissão dos dados previstos no n.º 2 do artigo 5.º respeita um grau de codificação e proteção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados.
3 — O disposto nos números anteriores não prejudica a observância dos princípios nem o cumprimento das regras aplicáveis previstos nas Leis n.ºs 67/98, de 26 de Outubro e 41/2004, de 18 de Agosto.
4 - 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".

Artigo 5.º (Entrada em vigor)

A presente lei entra em vigor no dia seguinte ao da sua publicação.»

2. Posteriormente, a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias solicitou também a este Conselho de Fiscalização (CFSIRP) o seu parecer sobre a **Proposta de Lei n.º 79/XIII/2.ªGOV**– ***"Aprova o regime especial de acesso a dados de base e a dados de tráfego de comunicações eletrónicas pelo SIRP"***.

É o seguinte o *articulado* da referida Proposta de Lei n.º 79/XIII:

«Artigo 1.º **Objeto e definições**

1 - A presente lei regula um procedimento especial de acesso a dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, sujeito a acompanhamento do Ministério Público e controlo judicial, que se mostrem estritamente necessários para a prossecução da atividade de produção de informações pelo Sistema de Informações da República Portuguesa (SIRP) relacionadas com a segurança interna, a defesa, a segurança do Estado e a prevenção da espionagem e do terrorismo.

2 - Para efeitos da presente lei, consideram-se «dados de telecomunicações e Internet»:

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

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

3 - Para efeitos da presente lei, no âmbito dos «dados de telecomunicações e Internet», consideram-se:

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

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

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

d) «Autoridades competentes», os dirigentes superiores e intermédios

do Serviço de Informações de Segurança (SIS) e do Serviço de Informações Estratégicas de Defesa (SIED).

4 - A conservação e transmissão pelos prestadores de serviços de comunicações eletrónicas dos dados tipificados nos números anteriores obedecem exclusivamente às finalidades previstas no n.º 1 e nos artigos 2.º e 3.º

5 - A transmissão dos dados pelos prestadores de serviços de comunicações eletrónicas às autoridades competentes do SIS e do SIED, nos termos do artigo 10.º, só pode ser autorizada e ordenada por despacho judicial fundamentado de acordo com o procedimento estatuído na presente lei.

Artigo 2.º **Acesso a dados de base e de localização de equipamento**

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

Artigo 3.º **Acesso a dados de tráfego**

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

Artigo 4.º **Comunicação ao Ministério Público e autorização judicial**

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

2 - O processo de autorização de acesso aos dados é sempre comunicado ao/à Procurador/a-Geral da República.

Artigo 5.º **Admissibilidade**

1 - O pedido só pode ser autorizado quando houver razões para crer que a diligência é necessária, adequada e proporcional, nos termos seguintes:
   a) Para a obtenção de informação sobre um alvo ou um intermediário determinado; ou
   b) Para a obtenção de informação que seria muito difícil ou impossível de obter de outra forma ou em tempo útil para responder a situação de urgência.

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

dados requeridos.

Artigo 6.º **Agravação**

1 - Quem, violando a proibição de ingerência do pessoal do SIRP na correspondência, nas telecomunicações e nos demais meios de comunicação, for condenado por qualquer dos crimes especialmente previstos nos artigos 193.º, 194.º e 384.º do Código Penal, nos artigos 6.º e 7.º da Lei n.º 109/2009, de 15 de setembro, e no artigo 44.º da Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto, é punido com a pena aplicável ao crime respetivo agravada de um terço nos seus limites mínimo e máximo.

2 - Ao membro do Gabinete da/o Secretária/o-Geral, ao pessoal dirigente e ao demais pessoal do SIRP que seja condenado por prática com dolo dos tipos de crime referidos no número anterior, pode o tribunal, ponderadas as circunstâncias do caso concreto, aplicar na sentença a pena acessória de demissão ou suspensão até cinco anos de exercício de funções no SIRP.

Artigo 7.º **Controlo judicial**

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

Artigo 8.º **Iniciativa**

1 - O procedimento obrigatório e vinculado de autorização judicial prévia do acesso dos oficiais de informações do SIS e do SIED a dados de telecomunicações e Internet inicia-se com o pedido elaborado pelos diretores do SIS ou do SIED, ou de quem os substitua em caso de ausência ou impedimento, enviado pela/o Secretária/o-Geral da República à/ao Presidente do Supremo Tribunal de Justiça, com conhecimento ao/à Procurador/a-Geral da República.

2 - O pedido previsto no número anterior é apresentado por escrito, devendo ser fundamentado de modo detalhado e circunstanciado, e conter os seguintes elementos:

a) Indicação da ação operacional concreta a realizar e das medidas pontuais de acesso requeridas;

b) Factos que suportam o pedido, finalidades que o fundamentam e razões que aconselham a adoção das medidas pontuais de acesso requeridas;

c) Identificação da pessoa ou pessoas, caso sejam conhecidas, envolvidas nos factos referidos na alínea anterior e afetadas pelas medidas pontuais de acesso requeridas;

d) Duração das medidas pontuais de acesso requeridas, que não pode exceder o prazo máximo de três meses, renovável por um único período sujeito ao mesmo limite, desde que se verifiquem os respetivos requisitos de admissibilidade.

3 - Para efeitos da presente lei, consideram-se «medidas pontuais de acesso» as providências de recolha de dados, por transferência autorizada e controlada caso a caso, com base numa suspeita concreta e individualizada, que não se prolongam no tempo, sendo a sua duração circunscrita, e que não se estendem à totalidade dos dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, não admitindo a aquisição de informação em larga escala, por transferência integral dos registos existentes, nem a ligação em tempo real às redes de comunicações eletrónicas.

Artigo 9.º **Apreciação judicial**

1 - A apreciação judicial da necessidade, adequação e proporcionalidade do pedido, designadamente no que se refere à justa medida da espécie e da escala de informação obtida, compreende a definição das categorias de dados de telecomunicações e Internet a fornecer pelos operadores, segundo um juízo restritivo, de proibição do excesso, que interdite o acesso indiscriminado a todos os dados de telecomunicações e Internet de um dado cidadão, bem como a definição das condições de proteção do segredo profissional.

2 - O acesso dos oficiais de informações do SIS e do SIED a dados de tráfego só pode ser autorizado no quadro da produção de informações de prevenção da espionagem e do terrorismo.

3 - A decisão judicial de concessão ou de denegação da autorização consta de despacho proferido no prazo máximo de 72 horas, fundamentado com base em informações claras e completas, nomeadamente quanto aos objetivos do processamento.

4 - Em situações de urgência devidamente fundamentadas no pedido, pode ser solicitada a redução para 24 horas do prazo previsto no número anterior.

Artigo 10.º **Acesso aos dados autorizados**

1 - A transmissão diferida dos dados de telecomunicações e Internet obtidos de acordo com o regime consagrado na presente lei processa-se mediante comunicação eletrónica, com conhecimento da formação das secções criminais do Supremo Tribunal de Justiça prevista no artigo 7.º e ao/à Procurador/a-Geral da República, nos termos das condições técnicas e de segurança fixadas em portaria do Primeiro-Ministro e dos membros do governo responsáveis pelas áreas das comunicações e da cibersegurança, que devem observar um grau de codificação e proteção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão,

incluindo métodos de codificação, encriptação ou outros adequados, sem prejuízo da observação dos princípios e do cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados, previstos na Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto, e na Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto, sob fiscalização e controlo da Comissão de Fiscalização de Dados do SIRP nos termos da presente lei.

2 - O acesso do pessoal do SIRP a dados e informações conservados em arquivo nos centros de dados do SIS e do SIED é determinado pelo princípio da necessidade de conhecer e só é concedido mediante autorização superior, tendo em vista o bom exercício das funções que lhe forem cometidas.

3 - O pessoal do SIRP ou quem aceder, tentar aceder, comunicar ou fizer uso dos dados ou informações em violação do disposto no n.º 2, incorre em infração disciplinar grave, punível com sanção que pode ir até à pena de demissão ou outra medida que implique a imediata cessação de funções do infrator, nos termos do disposto no regime de necessidade de acesso aplicável ao pessoal do SIRP.

Artigo 11.º **Garantias**

1 - O controlo judicial pela formação das secções criminais do Supremo Tribunal de Justiça visa garantir o respeito pelos direitos, liberdades e garantias, e pelo princípio da legalidade da recolha, assegurando, nomeadamente, que os dados são:
   a) Recolhidos para finalidades determinadas, explícitas e legítimas;
   b) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos.

2 - Após a comunicação prevista no n.º 1 do artigo anterior, a formação das secções criminais do Supremo Tribunal de Justiça valida o tratamento pelo SIS ou pelo SIED dos dados de telecomunicações e Internet considerados em conformidade com o disposto no número anterior.

3 - Compete à formação das secções criminais do Supremo Tribunal de Justiça determinar a todo o momento o cancelamento de procedimentos em curso de acesso a dados de telecomunicações e Internet, bem como ordenar a destruição imediata de todos os dados obtidos de forma ilegal ou abusiva, ou que violem o âmbito da autorização judicial prévia, bem como os dados que sejam manifestamente estranhos ao processo, nomeadamente quando não tenham relação com o objeto ou finalidades do pedido, ou cujo tratamento possa afetar gravemente direitos, liberdades e garantias.

4 - O/a Procurador/a-Geral da República é notificado das decisões de cancelamento de acesso e de destruição dos dados, para efeitos do exercício das suas competências legais.

5 - A Comissão de Fiscalização de Dados do SIRP é notificada das decisões de cancelamento de acesso e de destruição dos dados, para efeitos do exercício

das suas competências legais em matéria de proteção dos dados pessoais.

Artigo 12.º **Factos indiciários de espionagem e terrorismo**

Os dados obtidos que indiciem a prática de crimes de espionagem e terrorismo são imediatamente comunicados ao/à Procurador/a-Geral da República para os devidos efeitos.

Artigo 13.º **Regime de proteção de dados**

1 - Os dados de telecomunicações e Internet obtidos de acordo com o preceituado na presente lei são processados e conservados nos centros de dados do SIS e do SIED, sendo o diretor de cada centro de dados o responsável pelo seu tratamento nos termos do regime de proteção de dados pessoais.
2 - Cabe ao responsável pelo tratamento assegurar que os dados inseridos no centro de dados do SIS ou do SIED são tratados:
   a) De forma lícita e com respeito pelo princípio da boa-fé;
   b) De forma compatível com as finalidades que determinaram a sua recolha;
   c) De modo a assegurar que sejam apagados ou retificados os dados inexatos ou incompletos, tendo em conta as finalidades da recolha e tratamento;
   d) De modo a que a conservação seja sempre fundamentada e restrita ao período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.
3 - O tratamento dos dados obtidos, nomeadamente a inserção no centro de dados do SIS ou do SIED, bem como a atualidade, fundamento e prazo de conservação, arquivo e eliminação, obedece ao regime especial de proteção de dados pessoais do SIRP, bem como aos critérios e normas classificadas de segurança dos centros de dados do SIS e do SIED.
4 - Aos dados de telecomunicações e Internet constantes dos centros de dados do SIS e do SIED aplicam-se os prazos de conservação, eliminação e destruição definidos em regulamento aprovado pelo Conselho de Ministros, após o parecer obrigatório da Comissão de Fiscalização de Dados do SIRP e a apreciação do Conselho Superior de Informações, nos termos do regime do SIRP aplicável aos centros de dados do SIS e do SIED.
5 - O procedimento de acesso a dados de telecomunicações e Internet da presente lei é coberto pelo regime do segredo de Estado aplicável ao SIRP, sem prejuízo do disposto no regime do pessoal do SIRP relativo à credenciação de segurança.

Artigo 14.º **Comissão de Fiscalização de Dados do Sistema de Informações da República Portuguesa**

1 - A Comissão de Fiscalização de Dados do SIRP é a autoridade pública

competente para a fiscalização do respeito pelos princípios e cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados obtidos de acordo com o presente procedimento obrigatório e vinculado.

2 - Sem prejuízo dos demais poderes de fiscalização previstos no regime geral aplicável aos centros de dados do SIS e do SIED, os dados de telecomunicações e Internet obtidos de acordo com o procedimento previsto na presente lei estão sujeitos à fiscalização oficiosa, por referência nominativa, da Comissão de Fiscalização de Dados do SIRP.

3 - Para os efeitos previstos no número anterior, a formação das secções criminais do Supremo Tribunal de Justiça comunica à Comissão de Fiscalização de Dados do SIRP as autorizações concedidas com referência nominativa.

4 - Os diretores dos centros de dados do SIS e do SIED prestam especial apoio à Comissão de Fiscalização de Dados do SIRP para efeitos do cumprimento do disposto no presente artigo.

5 - Das irregularidades ou violações verificadas deve a Comissão de Fiscalização de Dados do SIRP dar conhecimento, através de relatório, ao Conselho de Fiscalização do SIRP.

6 - O direito de acesso dos cidadãos aos dados processados ou conservados nos Centros de Dados do SIS e do SIED é exercido através da Comissão de Fiscalização de Dados do SIRP segundo o procedimento previsto no regime geral aplicável aos centros de dados do SIS e do SIED quanto à fiscalização mediante participação.

7 - A Comissão de Fiscalização de Dados do SIRP deve ordenar o cancelamento ou retificação dos dados de telecomunicações e Internet recolhidos que envolvam violação dos direitos, liberdades e garantias consignados na Constituição e na lei e, se for caso disso, exercer a correspondente ação penal.

Artigo 15.º **Conselho de Fiscalização do Sistema de Informações da República Portuguesa**

1 - O procedimento de acesso e os dados de telecomunicações e Internet obtidos nos termos do disposto na presente lei estão igualmente sujeitos aos poderes de fiscalização do Conselho de Fiscalização do SIRP.

2 - Compete ao Conselho de Fiscalização do SIRP receber do Secretário-Geral, com regularidade mínima bimensal, uma lista dos pedidos de autorização de acesso a dados de telecomunicações e Internet submetidos à secção judicial de controlo referida no artigo 11.º, podendo solicitar e obter os esclarecimentos e informações complementares que considere necessários e adequados ao exercício das suas funções de fiscalização.

Artigo 16.º **Alteração à Lei da Organização do Sistema Judiciário**

Os artigos 47.º e 54.º da Lei n.º 62/2013, de 26 de agosto, alterada pela Lei n.º 40-A/2016, de 22 de dezembro, passam a ter a seguinte redação:

"Artigo 47.º [...]

1 - [...].
2 - [...].
3 - [...].
4 - No Supremo Tribunal de Justiça uma formação das secções criminais, constituída pelos presidentes das secções criminais do Supremo Tribunal de Justiça e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções, procede ao controlo e autorização prévia da obtenção de dados de telecomunicações e Internet no quadro da atividade de produção de informações em matéria de espionagem e terrorismo do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa.

Artigo 54.º [...]

1 - [...].
2 - [...].
3 - A formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções, procede ao controlo e autorização prévia dos pedidos fundamentados de acesso a dados de telecomunicações e Internet nos termos do procedimento previsto na lei especial que aprova o regime especial de acesso a dados de base e a dados de tráfego de comunicações eletrónicas pelo SIRP."»

3. Tanto o Projeto de Lei n.º 480/XIII como o Projeto de Lei n.º 79/XIII incidem diretamente sobre *matéria relativa ao SIRP*, alterando diretamente o seu regime jurídico, constante da Lei-Quadro do Sistema de Informações da República Portuguesa (Lei n.º 30/84, de 5 de Setembro, alterada pelas Leis n.º 4/95, de 21 de fevereiro, 15/96, de 30 de abril, e 75-A/97, de 22 de julho, e pelas Leis Orgânicas n.º 4/2004, de 6 de novembro e n.º 4/2014, de 13 de agosto, com a Declaração de Retificação n.º 44-A/2014, de 10 de outubro – Lei-Quadro do SIRP), ou introduzindo um "procedimento especial de acesso a dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, sujeito a acompanhamento do Ministério Público e controlo judicial, que se mostrem estritamente necessários para a prossecução da atividade de produção de informações pelo Sistema de Informações da República Portuguesa (SIRP)", tratando, pois, de matéria que também incide sobre o SIRP.

É *competência do CFSIRP*, nos termos do artigo 9.º, n.º 2, alínea *l)*, da Lei-Quadro

do SIRP, "[p]ronunciar-se sobre quaisquer iniciativas legislativas que tenham por objeto o Sistema de Informações da República Portuguesa, bem como sobre modelos de organização e gestão administrativa, financeira e de pessoal dos serviços."

Este Conselho de Fiscalização *irá pronunciar-se* sobre os referidos projeto e proposta de lei. Dada a evidente conexão temática das duas iniciativas legislativas, o CFSIRP pronunciar-se-á *sobre ambas no presente Parecer*, embora fazendo-o *separadamente* quanto a cada uma das iniciativas.

4. Antes de passar à apreciação, no âmbito das competências deste Conselho, das iniciativas legislativas cujo articulado se transcreveu, importa recordar que *não é a primeira vez* que, em tempos recentes, o CFSIRP se tem de pronunciar sobre iniciativas legislativas relativas aos poderes dos Serviços que integram o SIRP para acederem a dados de base e de localização de telecomunicações – iniciativas legislativas a que não será com certeza alheia a evolução do contexto das ameaças que impendem também sobre o nosso País, com destaque, desde logo, para a ameaça terrorista.

Assim, em julho de 2015 o CFSIRP emitiu o seu *Parecer sobre a Proposta de Lei n.º 345/XII/4.ª – "Aprova o regime do Sistema de Informações da República Portuguesa"*, tendo então dito, no n.º 43:

> «O CFSIRP nota, quanto ao proposto artigo 78.º, n.º 2, que se passa a prever nele, com caráter inovatório, a possibilidade de os oficiais de informações do SIS e do SIED acederem, para recolha de informações adequadas a "prevenir a sabotagem, a proliferação, a espionagem, o terrorismo, 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", 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 fonte, o destino, data hora, duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização.
>
> Isto, prevê-se, desde que tais ações sejam "necessários, adequados e proporcionais, numa sociedade democrática, para o cumprimento das atribuições legais dos serviços de informações" e sempre mediante a autorização obrigatória da Comissão de Controlo Prévio.
>
> O CFSIRP nota que, atualmente, existem já certas entidades administrativas que, para prossecução das suas funções, podem aceder a alguma da informação referida nesta norma (assim, por exemplo, a informações bancárias, quanto às Finanças, ou ao Banco de Portugal).

No que diz respeito, em particular, aos "dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, data hora, duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização", o CFSIRP chama a atenção para as questões de constitucionalidade suscitadas pelo confronto da solução legalmente prevista com os artigos 26.º, n.º 1, e 34.º, n.º 4, da Constituição da República.

O CFSIRP entende que não deve pronunciar-se sobre tais questões. Embora pareça claro ao CFSIRP que a solução legalmente prevista não pode ser liminarmente descartada por grosseira ou claramente inconstitucional – dados os limitados termos em que é admitida, a sua justificação pelas finalidades prosseguidas, e o carácter menos intrusivo do que o acesso ao conteúdo de comunicações –, o CFSIRP recorda que, caso a questão se suscite, em via preventiva ou sucessiva, e a título principal ou incidental, sempre será ao órgão jurisdicional com competência para controlo concentrado da constitucionalidade que cabe dirimi-la na nossa ordem jurídica, e a título definitivo.

Em qualquer caso, o CFSIRP expressa a sua posição de que a solução proposta é, no atual contexto, útil e mesmo necessária para o desempenho das atribuições do SIRP, pelo menos quanto à prevenção do terrorismo. O CFSIRP nota, também, que os serviços de informações portugueses são, presentemente, os únicos que não dispõem de qualquer possibilidade legal de, para desempenho das suas missões (e designadamente de prevenção do terrorismo), recolher informações do tipo das previstas na norma proposta, e que essa limitação se reflete, naturalmente, na sua atividade, quer quanto às possibilidade de colaboração com serviços congéneres no quadro dos compromissos internacionais do Estado (e mesmo da luta internacional contra o terrorismo), quer quanto às possibilidades de deteção de ameaças em território nacional.»

5. Como é sabido, a Proposta de Lei referida no número anterior foi *aprovada* (aliás, por larga maioria) na Assembleia da República, mas o artigo 78.º, n.º 2, do Decreto respetivo, submetido a fiscalização preventiva de constitucionalidade pelo Tribunal Constitucional, veio a ser objeto do Acórdão n.º 403/2015, de 17 de setembro, que se pronunciou no sentido da *inconstitucionalidade da norma do n.º 2 do artigo 78.º* desse Decreto, por violação do n.º 4 do artigo 34.º da Constituição da República.

Por esta razão, *não chegou a ser promulgado* o Decreto a que dera origem a Proposta de Lei n.º 345/XII/4.ª

6. Posteriormente, o CFSIRP teve já ocasião de se *voltar a pronunciar sobre a matéria que dera ao artigo 78.º da referida Proposta de Lei*. Fê-lo no seu *Parecer relativo*

ao ano de 2015, em que recordou que desde o verão de 2015

> "não se verificou qualquer outra iniciativa legislativa, que procurasse prosseguir os mesmos objetivos que este diploma tinha, expurgando-o das inconstitucionalidades declaradas e no pleno respeito dos direitos, liberdades e garantias e dos princípios e regras constitucionais que limitam a atividade dos serviços.
>
> As ameaças que os serviços de informações visam detetar e prevenir não desapareceram nem diminuíram, porém, desde então. Apesar da avaliação globalmente positiva que faz sobre os resultados da atividade do SIRP, no presente quadro legal, e em consequência do contato com a atividade dos serviços (em particular do SIS), e com as suas missões, o CFSIRP entende, porém, que existe grande conveniência em dotar os serviços, em particular o SIS, de meios que, dentro do integral respeito dos direitos, liberdades e garantias e de todos os limites constitucionais e legais à atuação dos serviços, permitam a deteção e prevenção, e a cooperação na deteção e prevenção com serviços congéneres, de ameaças como o terrorismo, em termos semelhantes às melhores práticas de serviços congéneres de países que respeitam as exigências do Estado de direito democrático."

E concluiu pela *recomendação* no sentido da "dotação dos serviços (em particular do SIS) de meios que, dentro do integral respeito dos direitos, liberdades e garantias e de todos os limites constitucionais e legais à atuação dos serviços, permitam a deteção e prevenção, e a cooperação na deteção e prevenção com serviços congéneres, de ameaças como o terrorismo, em termos semelhantes às melhores práticas de serviços congéneres de países que respeitam as exigências do Estado de direito democrático".

No mesmo sentido, no seu *Parecer relativo ao ano de 2016*, o CFSIRP afirmou ser importante dotar os Serviços "dos meios humanos, técnicos e de enquadramento legal adequados", bem como "que o quadro legislativo seja edificado de modo a que o País não seja encarado como território vulnerável para a concretização de ameaças, e que não possa ser considerado como um local de recuo ou base para preparação de ações para terceiros".

7. O CFSIRP mantém o seu entendimento de que *não deve pronunciar-se adrede, e em profundidade, sobre as questões de constitucionalidade* eventualmente suscitadas pelo Projeto de Lei e pela Proposta de Lei sobre que incide este Parecer. Mas mantém também a posição de que as soluções legalmente previstas em qualquer destas iniciativas, e agora, mesmo depois do citado Acórdão n.º 403/2015, de 17 de setembro, *não devem ser liminarmente descartadas por grosseira ou claramente inconstitucionais*.

Em qualquer caso, o CFSIRP recorda que, caso a questão se suscite, em via preventiva ou sucessiva, e a título principal ou incidental, sempre será ao órgão jurisdicional com competência para controlo concentrado da constitucionalidade que caberá de novo dirimi-la na nossa ordem jurídica.

8. Dito isto, analisemos separadamente cada umas das iniciativas legislativas em causa.

Projeto de Lei n.º 480/XIII-2.ª

9. O Projeto de Lei n.º 480/XIII-2.ª, que tem como tema o "acesso a dados de tráfego, de localização ou outros dados conexos das comunicações por funcionários e agentes dos serviços de informações da República portuguesa", visa alterar Lei Quadro do SIRP e a Lei de Organização do Sistrema Judiciário (Lei n.º 62/2013, de 26 de agosto), no sentido de estabelecer a "competência e o procedimento de acesso por funcionários e agentes dos serviços de informações da República Portuguesa, mediante autorização judicial prévia a cargo da secção especial para autorização de acesso a informação e a dados do Supremo Tribunal de Justiça, a dados de tráfego, de localização ou outros dados conexos das comunicações, para cumprimento das atribuições legais desses serviços".

A alteração proposta ao artigo 2.º, n.º 2, da Lei Quadro do SIRP, visa *alargar o quadro de incumbências* dos serviços de informações: enquanto atualmente se diz ali que lhe incumbe "assegurar, no respeito da Constituição e da lei, a produção de informações necessárias à preservação da segurança interna e externa, bem como à independência e interesses nacionais e à unidade e integridade do Estado", passaria a prever-se especificamente a produção de informações que "contribuam para garantir as condições de segurança dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de Direito e adequadas a prevenir a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido" (nova proposta alínea *b)* do n.º 2 do artigo 2.º), e "adequadas a prevenir a sabotagem, a espionagem, o terrorismo e sua proliferação, nos termos da lei de combate ao terrorismo, e a criminalidade altamente organizada de natureza transnacional" (nova proposta alínea *c)* do n.º 2 do artigo 2.º).

Afigura-se ao CFSIRP que, além de evidentemente estas finalidades cuja especificação é agora proposta só poderem ser prosseguidas *com observância do princípio da proporcionalidade* (isto é, e designadamente, das exigências de adequação, necessidade e proibição do excesso da recolha de informações em relação às finalidades visadas), essas finalidades, cuja especificação se propõe, *já decorrem* do que atualmente se preceitua no artigo 2.º, n.º 2, da Lei Quadro do SIRP, devidamente densificado.

A necessidade da nova redação proposta para o artigo 2.º, n.º 2, da Lei Quadro do SIRP é, pois, duvidosa.

10. Na projetada nova redação do artigo 5.º passa a prever-se o acesso, pelos funcionários e agentes, civis ou militares, do SIRP, mediante autorização judicial, a "informação e registos relevantes para a prossecução das suas competências, contidos em ficheiros de entidades públicas, nos termos de protocolo, ouvida a Comissão Nacional de Proteção de Dados no quadro das suas competências próprias" (n.º1).

Além disso, prevê-se que os funcionários e agentes dos serviços de informações do SIS e do SIED podem, para efeitos de obtenção de informações adequadas a prevenir a sabotagem, a espionagem, o terrorismo e sua proliferação, e a criminalidade altamente organizada de natureza transnacional, e no exclusivo âmbito destas finalidades, "aceder a informação bancária, a informação fiscal, a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização" (n.º 2).

A autorização apenas deve ser concedida se não existir outro meio que permita a salvaguarda eficaz e atempada dos bens jurídicos a proteger e houver razões para crer que o acesso aos dados solicitados é indispensável, adequada e proporcional para prevenir a prática dos referidos crimes, sendo que para cada pedido deve ser emitida uma única autorização, que pode combinar várias medidas no âmbito da mesma ação (n.ºs 3 e 4).

Mantém-se a previsão, constante hoje do artigo 5.º, n.º 2, de que o funcionário e agente que comunicar ou fizer uso de informações e de dados em violação do disposto destas regras será punido com pena de prisão até 3 anos, se pena mais grave não lhe for aplicável, independentemente da medida disciplinar que ao caso couber.

O CFSIRP nota, porém, que no Projeto de Lei n.º 480/XIII *se elimina o atual n.º 1 do artigo 5.º da Lei Quadro do SIRP*, segundo o qual os funcionários e agentes, civis ou militares, "que exercem funções policiais só poderão ter acesso a dados e informações na posse dos serviços de informações desde que autorizados por despacho do competente membro do Governo, sendo proibida a sua utilização com finalidades diferentes da tutela da legalidade democrática ou da prevenção e repressão da criminalidade". Afigura-se que esta *previsão é, porém, de manter*, pelo que se afigura que, a não se dever a lapso a eliminação do atual artigo 5.º, n.º 1, da Lei Quadro do SIRP, tal ponto deve ser corrigido.

11. O Projeto de Lei n.º 480/XIII prevê também alterações à Lei de Organização do Sistema Judiciário, para criar uma "secção especial para autorização de acesso a informação e a dados", constituída "por três juízes da secção penal do Supremo Tribunal de Justiça, anual e sucessivamente designados, cabendo a um juiz as funções de relator e aos outros juízes as funções de adjuntos" (projetados novos n.ºs 2 e 3 do artigo 47.º), devendo o Procurador-Geral da República designar "anualmente um procurador-geral-adjunto junto da secção especial para autorização de acesso a informação e a dados" (projetado novo n.º 3 do artigo 66.º).

A competência para a concessão de autorização, o procedimento do pedido de autorização e a transmissão, tratamento, manutenção e destruição das informações e dados são regulados em 3 novos artigos (5.º-A, 5.º-B e 5.º-C) que o Projeto de Lei n.º 480/XIII se propõe aditar à Lei Quadro do SIRP.

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

O CFSIRP nota que a concessão de competência para concessão de autorização a uma *secção especial do Supremo Tribunal de Justiça permitirá aparentemente ultrapassar a objeção de constitucionalidade*, posta no citado Acórdão n.º 430/2015, resultante do facto de a autorização prevista no diploma então apreciado não ser uma *autorização judicial*.

Quanto ao *procedimento* do pedido de autorização, prevê-se, no projetado artigo 5.º-B (aliás, apenas para o pedido de acesso às informações e aos dados a que alude o n.º 2, do artigo 5.º, enquanto aparentemente a competência prevista no artigo anterior é para toda a autorização previstas no artigo 5.º, portanto incluindo o n.º 1 deste, devendo este aspeto ser clarificado), que o pedido é apresentado por escrito pelos Diretores do SIS ou do SIED ao procurador-geral adjunto junto da secção especial para autorização de acesso a informação e a dados do Supremo Tribunal de Justiça, contendo indicação concreta da ação operacional a realizar e das medidas requeridas, factos que suportam o pedido, finalidades que o fundamentam e razões que aconselham a adoção das medidas requeridas, identificação da pessoa ou pessoas, caso sejam conhecidas, envolvidas nos factos referidos na alínea anterior e afetadas pelas medidas e indicação do local onde as mesmas devam ser realizadas, e a duração das medidas requeridas, que não pode exceder o prazo máximo de três meses, prorrogáveis mediante autorização expressa. A secção especial referida deve decidir no sentido da concessão ou denegação da autorização por despacho fundamentado, proferido no prazo máximo de 48 horas, podendo, em caso de urgência, devidamente fundamentado no pedido dos serviços de informações, ser solicitada a redução para 24 horas deste prazo. Este procedimento é coberto pelo regime do segredo de Estado.

O CFSIRP *nada tem a opor* a este procedimento, parecendo possível que o pedido seja efetuado *diretamente pelos Diretores do SIS e do SIED* ao Procurador-Geral Adjunto, que deva conter os elementos mencionados, incluindo a duração das medidas requeridas, que não pode exceder o prazo máximo de três meses. O pedido de *prorrogação* deste prazo *deve igualmente ser objeto de fundamentação*, o que parece resultar do articulado projetado – embora não expressamente.

O CFSIRP nota que se prevê também a destruição imediata de todos os dados e informação recolhidos, mediante a autorização prevista, sempre que não tenham relação com o objeto ou finalidades da mesma (n.º 7 do projetado artigo 5.º-B), o que se afigura importante para observância do princípio da necessidade – embora seja de ponderar se essa *destruição deve poder ter lugar apenas por decisão do Secretário-Geral do SIRP*, ou exigirá *pelo menos comunicação prévia ao Procurador-Geral Adjunto* afeto à referida secção especial do Supremo Tribunal de Justiça.

Além disso, prevê-se que pode ser determinado o cancelamento de quaisquer procedimentos de acesso a informação e a dados, bem como participados à Comissão de Fiscalização de Dados do SIRP os elementos conducentes à destruição imediata dos respetivos dados ou informações, tudo isto por decisão do coletivo de juízes. Afigura-se igualmente positiva estas medida, sendo de ponderar a *possível conveniência da intervenção do Procurador-Geral Adjunto também no pedido de cancelamento* desses procedimentos de acesso, e a audição do Secretário Geral do SIRP a esse respeito.

12. Quanto à transmissão, tratamento, manutenção e destruição das informações e dados, prevista no projetado novo artigo 5.º-C, o CFSIRP concorda que a transmissão seja feita por comunicação eletrónica, de acordo com o disposto em diplomas especiais, que estabelecem os termos das *condições técnicas e de segurança* em que se processa a comunicação eletrónica para efeitos da transmissão de dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado. O CFSIRP também nada tem a observar à exigência de que a transmissão dos dados respeite 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, nem à ressalva de que as novas regras não prejudicam o cumprimento das regras aplicáveis previstos nas Leis n.ºs 67/98, de 26 de outubro e 41/2004, de 18 de agosto.

Apesar de tal se não encontrar expressamente previsto (pois só se ressalva o acompanhamento permanente da Comissão de Fiscalização de Dados do SIRP), o CFSIRP entende que resulta do Projeto de Lei n.º 480/XIII que as *suas competências de fiscalização do SIRP, incluindo no respeitante aos pedidos de autorização para acesso a informações e dados, e sua execução, não são também prejudicadas* pelo articulado proposto.

13. O CFSIRP nota ainda, como fez já no Parecer que emitiu em 2015 sobre a Proposta de Lei n.º 345/XII/4.ª – "Aprova o regime do Sistema de Informações da República Portuguesa" –, que, atualmente, existem já certas entidades administrativas que, para prossecução das suas funções, podem aceder a alguma da informação referida nesta norma (assim, por exemplo, a informações bancárias, quanto às Finanças, ou ao Banco de Portugal).

E, no que diz respeito, em particular, aos "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", o CFSIRP chama a atenção para as *questões de constitucionalidade* eventualmente suscitadas pelo confronto da solução legalmente prevista com os artigos 26.º, n.º 1, e 34.º, n.º 4, da Constituição da República, cuja apreciação e decisão competirá ao Tribunal Constitucional, se e quando vier a ser suscitada a sua intervenção.

Em todo o caso, o CFSIRP considera *positiva* a apresentação de iniciativas legislativas que visem responder à necessidade de dotar o SIRP de instrumentos legais que permitam responder às *necessidades* – designadamente, de prevenção da ameaça terrorista – que determinaram, já em 2015, a aprovação por larga maioria, na Assembleia da República, da referida Proposta de Lei n.º 345/XII/4.ª. Isto, a fim de que os serviços de informações nacionais deixem de ser os *únicos serviços de informações* que, no contexto europeu, estão *impedidos* de aceder, com autorização judicial e outras garantias destinadas a proteger os direitos fundamentais, a dados de tráfego, de localização ou

outros dados conexos das comunicações, com a finalidade de prevenir a *ameaça de terrorismo*.

Proposta de Lei n.º 79/XIII/2.ª

14. A Proposta de Lei n.º 79/XIII/2.ª insere-se no *mesmo objetivo* que o Projeto de Lei n.º 480/XIII, de dotar os serviços de informações nacionais dos referidos mecanismos legais. No entanto, não se propõe uma *alteração* (pelo menos expressa) à Lei Quadro do SIRP, antes introduz, em *lei especial*, um *procedimento especial de acesso a dados* "previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, sujeito a acompanhamento do Ministério Público e controlo judicial, que se mostrem estritamente necessários para a prossecução da atividade de produção de informações pelo Sistema de Informações da República Portuguesa (SIRP) relacionadas com a segurança interna, a defesa, a segurança do Estado e a prevenção da espionagem e do terrorismo".

A Proposta de Lei n.º 79/XIII define o que se entende, para efeitos desse diploma, por *"dados de telecomunicações"* ("registos ou informação constantes de bancos de dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas relativos à prestação de serviços telefónicos acessíveis ao público e à rede de suporte à transferência, entre pontos terminais da rede, de comunicações vocais, serviços de mensagens e multimédia e de outras formas de comunicação") e *"dados de Internet"* ("registos ou informação constantes de bancos de dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, relativos a sistemas de transmissão e a equipamentos de comutação ou encaminhamento que permitem o envio de sinais ou dados, quando não deem suporte a uma concreta comunicação"). Importante (pois o seu regime é diferenciado) é também a distinção, dentro daquelas categorias, entre *"dados de base"* (dados para acesso à rede pelos utilizadores, compreendendo a identificação e morada destes, e o contrato de ligação à rede"), *"dados de localização de equipamento"* ("dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de telecomunicações que indiquem a posição geográfica do equipamento terminal de um serviço de telecomunicações acessível ao público, quando não deem suporte a uma concreta comunicação"), por um lado, e *"dados de tráfego"* (dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou no âmbito de um serviço de telecomunicações, ou para efeitos da faturação da mesma"), por outro lado.

Com efeito, a Proposta de Lei n.º 79/XIII prevê (artigo 2.º) que o acesso a dados de base e de localização de equipamento, por parte de oficiais de informações do SIS e do SIED, é possível "para efeitos de produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada, e no seu exclusivo âmbito", enquanto o acesso a *dados de tráfego* (artigo 3.º) apenas é permitido para efeitos de produção de informações necessárias à

prevenção de atos de espionagem e do terrorismo.

A Proposta de Lei n.º 79/XIII prevê não só uma *vinculação estrita* da conservação e transmissão pelos prestadores de serviços de comunicações eletrónicas dos dados referidos *a estas finalidades*, como que a transmissão dos dados pelos prestadores de serviços de comunicações eletrónicas às autoridades competentes do SIS e do SIED (definidos como os seus dirigentes superiores e intermédios), só pode ser autorizada e ordenada por *despacho judicial fundamentado* de acordo com o procedimento estatuído nesse diploma.

Antes de entrar na análise do procedimento de autorização, o CFSIRP nota que se faz, assim, distinção entre *dados de tráfego*, por um lado, e *dados de base e de localização*, por outro, podendo o acesso aos primeiros ser autorizado apenas para produção de informações necessárias à prevenção de *atos de espionagem e do terrorismo*, enquanto as finalidades que legitimam a autorização de acesso aos segundos são *mais amplas* (incluindo também a produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada).

O CFSIRP considera que essa distinção corresponde a uma *concretização mais perfeita do princípio da proporcionalidade* (na vertente da necessidade de acesso), na medida em que a necessidade que realmente mais se faz notar no presente contexto, quanto ao acesso a dados de tráfego (que ainda assim não envolvem o acesso ao conteúdo da comunicação, como acontece numa escuta), diz respeito à prevenção do *terrorismo* (e, também, da espionagem).

De igual modo, o CFSIRP considera que é de *aplaudir a vinculação estrita* da conservação e transmissão dos dados referidos a essas finalidades, e a *necessidade de autorização judicial*, por despacho fundamentado, para transmissão dos dados pelos prestadores de serviços de comunicações eletrónicas às autoridades competentes do SIS e do SIED.

15. A Proposta de Lei n.º 79/XIII prevê expressamente que o acesso dos oficiais de informações do SIS e do SIED a dados de telecomunicações e Internet no âmbito da atividade de pesquisa depende de uma *autorização judicial prévia e obrigatória*, por uma *formação das secções criminais do Supremo Tribunal de Justiça*, que garante a ponderação da relevância dos fundamentos do pedido e a salvaguarda dos direitos, liberdades e garantias constitucionalmente previstos, sendo o processo de autorização de acesso aos dados sempre comunicado ao/à Procurador/a-Geral da República (artigo 4.º).

No artigo 7.º da Proposta de Lei n.º 79/XIII, sobre "controlo judicial", prevê-se que esse controlo e a autorização prévia do acesso dos oficiais de informações do SIS e do SIED a dados de telecomunicações e Internet são efetuados por uma formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções.

Assim, a Proposta de Lei n.º 79/XIII prevê também uma alteração à Lei da

Organização do Sistema Judiciário: cria no Supremo Tribunal de Justiça uma formação das secções criminais, constituída pelos presidentes das secções criminais do Supremo Tribunal de Justiça e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções, para proceder ao controlo e autorização prévia dos pedidos fundamentados de acesso a dados de telecomunicações e Internet nos termos do procedimento previsto na lei especial (Proposta de Lei n.º 79/XIII) que aprovará o regime especial de acesso a dados de base e a dados de tráfego de comunicações eletrónicas pelo SIRP.

O CFSIRP nota, também aqui, que a concessão de competência para concessão de autorização a uma secção especial do Supremo Tribunal de Justiça permitirá, também quanto a esta iniciativa legislativa, *aparentemente ultrapassar a objeção de constitucionalidade, posta no citado Acórdão n.º 430/2015, resultante do facto de a autorização prevista no diploma então apreciado não ser uma autorização judicial.* O CFSIRP considera também relevante que o processo de autorização de acesso aos dados seja sempre comunicado ao/à Procurador/a-Geral da República.

16. No tocante às *condições do pedido de acesso*, prevê-se expressamente (artigo 5.º) que o pedido só pode ser autorizado quando houver razões para crer que a diligência é necessária, adequada e proporcional, para a obtenção de informação sobre um alvo ou um intermediário determinado, ou para a obtenção de informação que seria muito difícil ou impossível de obter de outra forma ou em tempo útil para responder a situação de urgência. Trata-se de exigências que decorrem do *princípio da proporcionalidade*, uma vez que estão em causa *limitações a direitos fundamentais*, pelo que deve estar numa relação de adequação, necessidade e proporcionalidade em sentido estrito com as finalidades prosseguidas.

A Proposta de Lei n.º 79/XIII *proíbe* ainda expressamente a *interconexão em tempo real* com as bases de dados dos operadores de telecomunicações e Internet para o acesso direto em linha aos dados requeridos.

O CFSIRP *nada mais tem a observar* quanto a estes aspetos do proposto novo regime jurídico.

17. Quanto ao *procedimento*, ele é obrigatório e vinculado, incluindo a autorização judicial prévia do acesso dos oficiais de informações do SIS e do SIED a dados de telecomunicações e Internet.

A iniciativa consiste em pedido elaborado pelos diretores do SIS ou do SIED, ou de quem os substitua em caso de ausência ou impedimento, devendo ser enviado pelo Secretário-Geral do SIRP[1] ao Presidente do Supremo Tribunal de Justiça, com conhecimento ao/à Procurador/a-Geral da República, sendo apresentado por escrito, e fundamentado de modo detalhado e circunstanciado, e tendo de conter os seguintes

[1] Aqui o articulado desta Proposta de Lei contém uma *gralha*, referindo-se ao pedido "enviado pela/o Secretária/o-Geral da República". Afigura-se, porém, que se quer referir o *Secretário-Geral do SIRP*.

elementos: indicação da ação operacional concreta a realizar e das medidas pontuais de acesso requeridas; factos que suportam o pedido, finalidades que o fundamentam e razões que aconselham a adoção das medidas pontuais de acesso requeridas; identificação da pessoa ou pessoas, caso sejam conhecidas, envolvidas nos factos referidos na alínea anterior e afetadas pelas medidas pontuais de acesso requeridas; duração das medidas pontuais de acesso requeridas, que não pode exceder o prazo máximo de três meses, renovável por um único período sujeito ao mesmo limite, desde que se verifiquem os respetivos requisitos de admissibilidade (proposto artigo 8.º, n.ºs 1 e 2).

O pedido apenas pode, pois, dizer respeito, não a um acesso indiscriminado e indeterminado no tempo, mas a "medidas pontuais de acesso", isto é, como se define na Proposta de Lei, a "providências de recolha de dados, por transferência autorizada e controlada caso a caso, com base numa suspeita concreta e individualizada, que não se prolongam no tempo, sendo a sua duração circunscrita, e que não se estendem à totalidade dos dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, não admitindo a aquisição de informação em larga escala, por transferência integral dos registos existentes, nem a ligação em tempo real às redes de comunicações eletrónicas" (artigo 8.º, n.º 3).

Afigura-se ao CFSIRP que *nada há a opor*, nem à iniciativa, nem aos termos prescritos do pedido nem ao âmbito possível das medidas, determinadas como apenas podendo ser *"medidas pontuais"*.

A apreciação judicial incide sobre a necessidade, adequação e proporcionalidade do pedido, designadamente no que se refere à "justa medida da espécie e da escala de informação obtida", e deve compreender a definição das categorias de dados de telecomunicações e Internet a fornecer pelos operadores, segundo um juízo restritivo, de proibição do excesso, que interdite o acesso indiscriminado a todos os dados de telecomunicações e Internet de um dado cidadão, bem como a definição das condições de proteção do segredo profissional. De novo se salienta aqui, no artigo 9.º (tal como resultava já do artigo 3.º), que o acesso a dados de tráfego por oficiais de informações do SIS e do SIED "só pode ser autorizado no quadro da produção de informações de prevenção da espionagem e do terrorismo". A decisão judicial de concessão ou de denegação da autorização consta de despacho proferido no prazo máximo de 72 horas, fundamentado com base em informações claras e completas, nomeadamente quanto aos objetivos do processamento, podendo, porém, em situações de urgência devidamente fundamentadas no pedido, ser solicitada a redução para 24 horas do prazo previsto no número anterior.

O CFSIRP *nada tem a opor* a estas soluções, notando que as finalidades de *prevenção do terrorismo poderão em certos casos exigir a adoção das referidas medidas pontuais de acesso com urgência*, pelo que se compreende o prazo curto para a decisão, e a possibilidade de sua redução para 24 horas.

Embora tal não se encontre expressamente previsto, o CFSIRP nada tem igualmente a opor a que se preveja a *intervenção do Procurador-Geral da República*, diretamente ou através de Procurador-Geral Adjunto que o represente junto do Supremo Tribunal de Justiça, emitindo *parecer sobre os pedidos de acesso, anteriormente à sua*

decisão, desde que tal *não seja incompatível com os prazos curtos de decisão*, e ficando sempre salvaguardada a *vinculação ao segredo de Estado* dos intervenientes.

18. No que toca ao *acesso*, prevê-se no proposto artigo 10.º, n.º 1, que a transmissão, sempre diferida, dos dados de telecomunicações e Internet obtidos de acordo com o regime previsto, se processa mediante comunicação eletrónica, com conhecimento da formação das secções criminais do Supremo Tribunal de Justiça prevista para a decisão sobre a autorização e e ao/à Procurador/a-Geral da República, "nos termos das condições técnicas e de segurança fixadas em portaria do Primeiro-Ministro e dos membros do governo responsáveis pelas áreas das comunicações e da cibersegurança, que devem observar um grau de codificação e proteção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados, sem prejuízo da observação dos princípios e do cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados, previstos na Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto, e na Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto, sob fiscalização e controlo da Comissão de Fiscalização de Dados do SIRP nos termos da presente lei".

O CFSIRP *nada tem a observar* sobre esta solução, notando que houve preocupação em dar a conhecer não só o *pedido* como a *concretização do acesso* à formação judicial que a autoriza, bem como ao/à Procurador(a)-Geral da República, bem como em impor a observância de um *nível de codificação que seja o mais elevado possível de acordo com o estado da técnica*.

Também a propósito da *concretização do acesso* se repete que o acesso do pessoal do SIRP a dados e informações que estejam conservados em arquivo nos centros de dados do SIS e do SIED é "determinado pelo princípio da necessidade de conhecer e só é concedido mediante autorização superior, tendo em vista o bom exercício das funções que lhe forem cometidas". Trata-se de solução que se entende já hoje vigorar, e que corresponde à prática quanto à determinação pelo princípio da necessidade de acesso e da necessidade de autorização.

Prevê-se que o pessoal do SIRP ou quem aceder, tentar aceder, comunicar ou fizer uso dos dados ou informações em violação do disposto sobre o princípio da necessidade de conhecer e a necessidade de autorização superior, incorre em infração disciplinar grave, punível com sanção que pode ir até à pena de demissão ou outra medida que implique a imediata cessação de funções do infrator, nos termos do disposto no regime de necessidade de acesso aplicável ao pessoal do SIRP.

O CFSIRP *nada tem a opor ou a observar* sobre estas soluções.

19. O controlo judicial proposto visa "garantir o respeito pelos direitos, liberdades e garantias, e pelo princípio da legalidade da recolha, assegurando, nomeadamente, que os dados" são recolhidos "para finalidades determinadas, explícitas e legítimas", e que são "adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos". Trata-se, também aqui, do *controlo da vinculação estrita às finalidades*

legalmente previstas, da sua determinação, explicitação, e do princípio da proporcionalidade em sentido estrito (nas vertentes da adequação, necessidade e proibição do excesso).

Prevê-se também (proposto artigo 11.º, n.º 2) que, após a comunicação do acesso, "a formação das secções criminais do Supremo Tribunal de Justiça valida o tratamento pelo SIS ou pelo SIED dos dados de telecomunicações e Internet considerados" em conformidade com as exigências legais referidas. O controlo judicial estende-se, além da autorização, também à *concretização do acesso* e a uma sua *validação* a posteriori.

Além disso, compete também à formação das secções criminais do Supremo Tribunal de Justiça "determinar a todo o momento o cancelamento de procedimentos em curso de acesso a dados de telecomunicações e Internet, bem como ordenar a destruição imediata de todos os dados obtidos de forma ilegal ou abusiva, ou que violem o âmbito da autorização judicial prévia, bem como os dados que sejam manifestamente estranhos ao processo, nomeadamente quando não tenham relação com o objeto ou finalidades do pedido, ou cujo tratamento possa afetar gravemente direitos, liberdades e garantias", devendo o/a Procurador/a-Geral da República ser "notificado das decisões de cancelamento de acesso e de destruição dos dados, para efeitos do exercício das suas competências legais", também sendo notificada, para efeitos do exercício das suas competências legais em matéria de proteção dos dados pessoais, a Comissão de Fiscalização de Dados do SIRP.

O CFSIRP *nada tem a opor* à solução de atribuição à formação das secções criminais do Supremo Tribunal de Justiça competente para a decisão sobre a autorização da *competência para ordenar o cancelamento* de procedimentos.

A notificação *a posteriori* tanto ao/à Procurador(a) Geral da República como à Comissão de Fiscalização de Dados, embora quanto a esta apenas para o exercício das suas competências, afigura-se uma duplicação cuja *necessidade é duvidosa*, tendo em conta que essa Comissão é constituída por *três magistrados do Ministério Público, e tem sede na Procuradoria-Geral da República* (artigo 26.º, n.ºs 2 e 3, da Lei Quadro do SIRP).

A previsão legal de notificação à Comissão de Fiscalização de Dados *em nada contende com as competências de fiscalização do CFSIRP*, e com a exigência de comunicação dos pedidos de autorização, sua fundamentação, execução e resultados ao CFSIRP, para exercício das competências de fiscalização do CFSIRP – ponto a que se voltará mais à frente.

20. O artigo 13.º da Proposta de Lei n.º 79/XIII prevê o regime de *proteção dos dados recolhidos*.

Assim, os dados de telecomunicações e Internet obtidos "processados e conservados nos centros de dados do SIS e do SIED, sendo o diretor de cada centro de dados o responsável pelo seu tratamento nos termos do regime de proteção de dados pessoais", e devendo assegurar que os dados inseridos no centro de dados do SIS ou do SIED são tratados: de forma lícita e com respeito pelo princípio da boa-fé, de forma compatível com as finalidades que determinaram a sua recolha; de modo a assegurar que sejam apagados ou retificados os dados inexatos ou incompletos, tendo em conta as

finalidades da recolha e tratamento; e de modo a que a conservação seja sempre fundamentada e restrita ao período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.

Prevê-se também que o tratamento dos dados obtidos, nomeadamente a inserção no centro de dados do SIS ou do SIED, bem como a sua atualidade, fundamento e prazo de conservação, arquivo e eliminação, obedece ao regime especial de proteção de dados pessoais do SIRP, bem como aos critérios e normas classificadas de segurança dos centros de dados do SIS e do SIED.

Quanto aos prazos de conservação, eliminação e destruição dos dados de telecomunicações e Internet constantes dos centros de dados do SIS e do SIED, prevê-se a aplicação dos prazos definidos em regulamento aprovado pelo Conselho de Ministros, após o parecer obrigatório da Comissão de Fiscalização de Dados do SIRP e a apreciação do Conselho Superior de Informações, nos termos do regime do SIRP aplicável aos centros de dados do SIS e do SIED.

E prevê-se que o procedimento de acesso a dados de telecomunicações e Internet da presente lei fica coberto pelo regime do segredo de Estado aplicável ao SIRP, sem prejuízo do disposto no regime do pessoal do SIRP relativo à credenciação de segurança.

O CFSIRP nota que seria *conveniente prever um regulamento específico para a conservação, eliminação e destruição dos dados de telecomunicações e Internet*, ou alterar o Regulamento dos Centros de Dados do SIS e do SIED de modo *a prever disposições próprias para esses dados*, tendo em conta a sua especificidade.

Quanto às restantes soluções relativa à proteção de dados, o CFSIRP *nada tem a opor-lhes*, tendo em conta o *regime especial* a que devem estar sujeitos os dados recolhidos no âmbito do SIRP, para prossecução das finalidades específicas a que estão vinculados, e o controlo judicial, prévio e posterior, legalmente previsto.

21. A Proposta de Lei n.º 79/XIII prevê ainda a agravação de penas, em um terço nos seus limites mínimo e máximo (agravação correspondente à prevista já no artigo 30.º da Lei Quadro do SIRP), para quem, violando a proibição de ingerência do pessoal do SIRP na correspondência, nas telecomunicações e nos demais meios de comunicação, for condenado por qualquer dos crimes especialmente previstos nos artigos 193.º, 194.º e 384.º do Código Penal, nos artigos 6.º e 7.º da Lei n.º 109/2009, de 15 de setembro, e no artigo 44.º da Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto, é punido com a pena aplicável ao crime respetivo agravada de um terço nos seus limites mínimo e máximo.

Também em correspondência com o previsto no citado artigo 30.º, prevê-se a possibilidade de o tribunal aplicar ao membro do Gabinete da/o Secretária/o-Geral, ao pessoal dirigente e ao demais pessoal do SIRP, que seja condenado por prática com dolo dos tipos de crime referidos, uma pena acessória de demissão ou suspensão até cinco anos de exercício de funções no SIRP.

O CFSIRP *nada tem a opor* a estas soluções, cujo *paralelismo com o previsto já no artigo 30.º da Lei Quadro do SIRP* se afigura claro.

22. Por fim, no que diz respeito à *fiscalização do regime especial de acesso a dados* de telecomunicações e Internet, a Proposta de Lei n.º 79/XIII contém duas normas, os artigos 14.º e 15.º, relativos respetivamente à Comissão de Fiscalização de Dados do Sistema de Informações da República Portuguesa e ao CFSIRP.

Assim, prevê-se que *a Comissão de Fiscalização de Dados* é a autoridade pública competente para a fiscalização do respeito pelos princípios e cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados obtidos de acordo com o procedimento obrigatório e vinculado, estando esses dados de telecomunicações e Internet sujeitos a fiscalização oficiosa, por referência nominativa.

Prevê-se também a comunicação, pela formação das secções criminais do Supremo Tribunal de Justiça, à Comissão de Fiscalização de Dados do SIRP, das autorizações concedidas com referência nominativa, prestando os diretores dos centros de dados do SIS e do SIED "especial apoio à Comissão de Fiscalização de Dados do SIRP para efeitos do cumprimento" das suas funções de fiscalização.

As irregularidades ou violações verificadas devem ser *comunicadas, pela Comissão de Fiscalização de Dados do SIRP, através de relatório, ao CFSIRP* (proposto artigo14.º, n.º 5).

Além disso, prevê-se que o direito de acesso dos cidadãos aos dados processados ou conservados (*"habeas data"*) nos Centros de Dados do SIS e do SIED é exercido através da Comissão de Fiscalização de Dados do SIRP, segundo o procedimento previsto no regime geral aplicável aos centros de dados do SIS e do SIED quanto à fiscalização mediante participação. E, ainda, que a Comissão de Fiscalização de Dados do SIRP deve ordenar o cancelamento ou retificação dos dados de telecomunicações e Internet recolhidos que envolvam violação dos direitos, liberdades e garantias consignados na Constituição e na lei e, se for caso disso, exercer a correspondente ação penal.

O CFSIRP entende que a atribuição à Comissão de Fiscalização de Dados de competência de fiscalização dos dados de telecomunicações e Internet recolhidos é *coerente com as competências dessa Comissão*, previstas no artigo 26.º da Lei Quadro do SIRP.

Como resulta dos propostos artigo 14.º, n.º 5, e 15.º, essa competência *não prejudica, porém, os poderes de fiscalização do CFSIRP*, também sobre o procedimento de acesso e os dados de telecomunicações e Internet obtidos nos termos do processo previsto no diploma proposto.

A este último propósito afigura-se que a comunicação dos pedidos de autorização de acesso a dados de telecomunicações e Internet ao CFSIRP, por parte do Secretário-Geral do SIRP, deveria ter uma *regularidade mensal*, e *não apenas bimensal*, em correspondência com a prática seguida quanto ao envio ao CFSIRP quer de relatórios mensais por parte do SIS, do SIED e do Secretário-Geral, sobre a sua atividade, quer da lista integral de processos em curso nos serviços de informações. Assim, onde se propõe, no artigo 15.º, n.º 2, que "Compete ao Conselho de Fiscalização do SIRP receber do Secretário-Geral, com regularidade mínima bimensal, uma lista dos pedidos de autorização de acesso a dados de telecomunicações e Internet submetidos à secção judicial de controlo referida no artigo 11.º, podendo solicitar e obter os esclarecimentos e

informações complementares que considere necessários e adequados ao exercício das suas funções de fiscalização", deveria passar a prever-se que compete ao CFSIRP receber do Secretário-Geral receber essa lista *com regularidade mínima mensal.*

23. Por fim o CFSIRP chama de novo, também quanto à Proposta de Lei n.º79/XIII, a atenção para as *questões de constitucionalidade* eventualmente suscitadas pelo confronto da solução legalmente prevista com os artigos 26.º, n.º 1, e 34.º, n.º 4, da Constituição da República, cuja apreciação e decisão competirá ao Tribunal Constitucional, se e quando vier a ser suscitada a sua intervenção.

Em todo o caso, afigura-se ao CFSIRP que essas soluções *não estão, pelo menos, manifestamente feridas de inconstitucionalidade*, mesmo tendo em conta fundamentação do já citado Acórdão n.º 430/2015, do Tribunal Constitucional.

E, também a propósito da Proposta de Lei n.º 79/XIII, o CFSIRP sublinha que é *positiva a existência de iniciativas legislativas que visem responder à necessidade de dotar o SIRP de instrumentos legais* que permitam responder às necessidades – designadamente, de *prevenção da ameaça terrorista* – que determinaram, já em 2015, a aprovação por larga maioria, na Assembleia da República, da referida Proposta de Lei n.º 345/XII/4.ª. Isto, para que, como já se disse, os serviços de informações nacionais *deixem de ser os únicos* que, no contexto europeu, não podem aceder, com autorização judicial e outras garantias destinadas a proteger os direitos fundamentais, a dados de tráfego, de localização ou outros dados conexos das comunicações, com a finalidade de *prevenir a ameaça terrorista.*

Lisboa, 14 de junho de 2017

O Conselho de Fiscalização do Sistema de Informações da República Portuguesa:

Paulo Mota Pinto (Presidente)

Filipe Neto Brandão

António Rodrigues