MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA

Vossa referência:
Nossa Referência: Of.º n.º 10655 de 02/06/2017
Proc. n.º 115/2016 – L. 115

ASSUNTO: **Envio de parecer sobre o Projeto de Lei nº 480/XIII/2ª - Proposta de Lei n.º 79/XIII**

Ex.mo Senhor
Presidente da Comissão de Assuntos Constitucionais, Direitos e Liberdades e Garantias
Prof. Dr. Bacelar Vasconcelos

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

Com os melhores cumprimentos,

A Chefe de Gabinete

Helena Gonçalves

ASSEMBLEIA DA REPÚBLICA
Divisão de Apoio às Comissões
CACDLG
S77157
666 S/6617

876944_1
/sv

PARECER

Proposta de Lei nº 79/XIII

Acesso a dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas pelo Sistema de Informações da República

O Governo remeteu à Assembleia da República a Proposta de Lei 79/XIII, pela qual pretende, em lei autónoma, permitir aos serviços de informações aceder a dados de telecomunicações e de internet – *dados de base, de localização e de tráfego* - regulando o âmbito, objetivo e subjetivo, de acesso, as suas finalidades, condições de admissibilidade e o procedimento obrigatório e vinculado de prévia autorização judicial.

A proposta de lei, sem parecer formal da Procuradoria-Geral da República, foi aprovada pelo Conselho de Ministros no dia 11 de maio e, nessa mesma data, enviada à Assembleia da República, onde foi objeto de discussão na generalidade no dia 17 de maio,[1] em conjunto com o projeto de lei 480/XIII, do Grupo Parlamentar do CDS[2], já analisado na PGR.

Em satisfação do solicitado pela Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República, procede-se à análise da Proposta de Lei ora enviada.

---

[1] Aprovada na generalidade com os votos a favor do PSD, PS, CDS-PP, PAN e os votos contra do BE, PCP, PEV. Em 19-5- baixou à comissão especialidade - Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias

[2] Também aprovado, na mesma sessão do Plenário, com os votos a favor do PSD, PS, CDS-PP, a abstenção do PAN e os mesmos votos contra. Baixou também à mesma Comissão de especialidade.

I - Objeto e estrutura do regime proposto

1. Síntese da proposta

Pretende-se, em lei autónoma, regular «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 (SIRP) relacionados com a segurança interna, a defesa, a segurança do Estado e a prevenção da espionagem e do terrorismo*» (nº 1, do art. 1º).

Tratando-se de procedimento especial, e atentas as especificidades do mesmo e a natureza da matéria, **entende-se como adequado que a regulação da matéria em causa não seja objeto da Lei 30/84, de 5/ de setembro, ou da Lei 9/2007, de 19 de fevereiro, mas sim de diploma autónomo que regule integralmente o regime especial de acesso do SIRP aos dados de comunicação**.

Da conjugação do art. 1º, nº 1 da proposta de Lei com o que se dispõe no art. 2º e no art. 3º, resulta que o objeto do acesso do SIRP a dados de telecomunicações que se pretende prever e regular respeita a três categorias de dados – *dados de base, dados de localização e dados de tráfego*.

Em todos os casos o acesso está sujeito a condições/requisitos de admissibilidade vinculados aos *princípios da necessidade, adequação e proporcionalidade*, à proibição de interconexão em tempo real (art. 5º), e a um sistema de autorização prévia e de controlo permanente, interno e externo (designadamente quanto ao cancelamento dos procedimentos de acesso e destruição de dados obtidos ilegalmente, que não respeitem o âmbito da autorização ou que sejam estranhos ao processo), que envolve as seguintes entidades: Supremo Tribunal de Justiça, Procurador-Geral da República, Comissão de Fiscalização de Dados do SIRP e Conselho de Fiscalização do SIRP (arts. 4º a 11º, 14º e 15º).

São definidos, para efeitos da lei que se pretende aprovar, os conceitos de "*dados de telecomunicações e Internet*", "*dados de base*", "*dados de localização de equipamento*", "*dados de tráfego*" e " *autoridades competentes*" (art. 1º, nº 2 e 3).

Distinguem-se as finalidades de acesso aos *dados de base* e de *localização* das finalidades de acesso aos *dados de tráfego*, prevendo-se, quanto aos dois primeiros, um mais amplo leque de finalidades: «*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*» (art. 2º), enquanto o acesso aos *dados de tráfego* apenas pode ter lugar «*para* efeitos de *produção de informações necessárias à prevenção de atos de espionagem e do terrorismo*» (art. 3º).

Define-se o modo de transmissão dos dados e do acesso aos dados e informações conservados em arquivo nos centros de dados do SIS e do SIED (art. 10º).

Define-se, igualmente, o regime de proteção dos dados de telecomunicações e de Internet obtidos pelo SIRP nos termos preceituados na lei que se pretende aprovar, designadamente em sede de prazos de conservação, eliminação e destruição, estabelecendo-se, igualmente, a sujeição do procedimento de acesso ao regime de segredo de Estado aplicável ao SIRP. (art. 12º).

Prevê-se a imediata comunicação ao Procurador-Geral da República dos dados obtidos que indiciem a prática de crimes de espionagem e terrorismo (art. 12º).

Prevê-se a "Agravação" das penas dos crimes p.p. pelos arts. 193º, 194º e 384º do Código Penal, dos crimes p.p. pelos arts. 6º e 7º da Lei 109/2009, de 15/9 e do crime p.p. pelo art. 44º da Lei 67/98, de 26/10 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* nas citadas normas incriminadoras.

Finalmente, adita-se um nº 4 ao art. 47º, e um nº 3 ao art. 54º da Lei 62/2013, de 26/8 (Lei de Organização do Sistema Judiciário), no sentido de prever a estrutura judicial - organizativa e funcional - que, no Supremo Tribunal de Justiça, será competente para proceder ao controlo e autorização prévia de acesso aos dados de telecomunicações e de Internet pelo SIRP, nos termos regulados na lei que se pretende aprovar.

2. Análise genérica face à posição assumida pelo Tribunal Constitucional no Acórdão 403/2015

A proposta de lei retoma a questão da necessidade de acesso dos serviços de segurança a dados de comunicações, face, designadamente, à ameaça terrorista e à premência em dotar aqueles serviços de mecanismos de atuação que possam responder «*aos desafios colocados à segurança nacional e internacional do Estado*» e a posicioná-los a par com os congéneres europeus.

Assim, na convicção de que o nº 4 do art. 34º da CRP deverá ser interpretado de modo integrado com os demais preceitos constitucionais atinentes à salvaguarda dos direitos fundamentais à liberdade e à segurança, bem como das obrigações do Estado na defesa e garantia de tais direitos, a Proposta de Lei prevê a criação de um regime especial e estruturado de acesso àqueles dados.

A conceção do regime, em particular no que se refere às garantias de controlo interno e externo da ingerência nas comunicações pelo SIRP, é feita de modo a corresponder às exigências constitucionais de respeito e salvaguarda dos direitos fundamentais, designadamente do direito à reserva da vida privada que resulta afetado com o acesso aos dados de comunicações, procurando o equilíbrio entre a proteção deste direito e a salvaguarda da liberdade e segurança.

É o que resulta não apenas da Exposição de Motivos como também, em boa medida, do conteúdo da Proposta de Lei.

De tal preocupação é igualmente testemunho a intervenção da Excelentíssima Senhora Ministra da Administração Interna na Assembleia da República aquando da apresentação da Proposta de Lei.

Com efeito, ali foi afirmado que o regime proposto procura ir ao encontro da jurisprudência do Tribunal Constitucional e de uma interpretação atualista da Constituição da República, que deverá ser interpretada como um todo, bem como alcançar a conciliação prática entre os direitos à liberdade e segurança (art. 27º da CRP) e o direito ao sigilo das comunicações (art. 34º), e efetivar a tarefa fundamental do Estado de garantir o direito à segurança individual e coletiva (art. 9º da CRP).

Foi ainda defendido que o regime de acesso que se pretende aprovar tem como objetivo apenas a salvaguarda daqueles valores constitucionais; que o acesso nunca respeita a dados de conteúdo; que a ingerência se dirige a pessoas determinadas e que está sujeito a apertadíssimo controlo de natureza judicial – prévia e obrigatória autorização do STJ e controlo permanente pelo STJ e pela Procuradoria-Geral da República, bem como pela Comissão de Fiscalização de Dados do SIRP e pelo Conselho de Fiscalização do SIRP.

Foi ainda salientado, no sentido da defesa da compatibilização constitucional do regime proposto, que o acesso apenas poderá ter lugar se a informação não puder ser obtida por outra via, e que se prevê a proibição de interconexão em tempo real.

2.1. Efetivamente, a Proposta de Lei, ciente das questões de desconformidade constitucional do Decreto da Assembleia da República nº 426/XII[3] apontadas pelo Acórdão nº 403/2015 do Tribunal Constitucional[4], vem, claramente, reforçar o regime de controlo, interno e externo, da atividade do SIRP, no segmento da ingerência nas

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

[4] Que igualmente foram reafirmadas pela Declaração de Voto da Conselheira Maria Lúcia Amaral como fundamento do seu voto no juízo de inconstitucionalidade, como resulta da posição assumida, uma vez que assume posição no sentido da admissibilidade constitucional de acesso do SIRP aos dados de comunicações, designadamente aos dados de tráfego, como adiante se referirá.

comunicações, bem como restringe o âmbito das finalidades desse acesso, pelo menos no que se refere aos dados de tráfego.

Vetores que poderão configurar-se como essenciais na apreciação da conformidade constitucional daquela ingerência, ultrapassada que possa ser a questão da interpretação do nº 4 do art. 34º da CRP.

De facto, referido Decreto da Assembleia da República foi objeto de pedido de fiscalização preventiva da constitucionalidade no segmento normativo do nº 2 do art. 78º daquele diploma, visando a apreciação da sua conformidade constitucional com o disposto no nº 4 do artigo 34º da Constituição da República.

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

- Os dados relativos às telecomunicações a que se refere o nº 2 do art. 78º do Decreto da AR consubstanciam dados de tráfego, e, como tal, estão a coberto da proteção da norma constitucional do nº 4 do art. 34º da CRP;

- A restrição dos direitos fundamentais objeto da proteção constitucional do nº 4 do art. 34º da CRP apenas é admitida em sede de processo penal;

- As atribuições do SIRP para efeitos de acesso àqueles dados - recolha, processamento, exploração e difusão de informações -, porque preventivas, não se inserem no âmbito da investigação criminal, constituindo-se as suas *ações de prevenção* como *procedimentos administrativos que, devendo respeitar os direitos, liberdades e garantias, não obedecem aos princípios jurídico-constitucionais conformadores do processo penal, proclamados no art. 32º da CRP*;

• A ingerência nos dados de comunicação não tem, no presente contexto, lugar num procedimento que dê garantias e faculdades de proteção de alcance assimilável àquelas que conformam constitucionalmente o processo criminal;

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

2.2. Antes de se proceder à análise concreta do regime proposto, cremos que se justificará dar nota de algumas passagens do Acórdão do Tribunal Constitucional e das Declarações de Voto dos Ex.mos Conselheiros Maria Lúcia Amaral e Teles Pereira, no sentido de ilustrar, por um lado, as dificuldades que poderão decorrer da questão nuclear da limitação que resulta da formulação do nº 4 do art. 34º da CRP, e, por outro lado, o positivo contributo, no sentido da conciliação do sistema com as exigências constitucionais, do previsto regime procedimental e de controlo de acesso aos dados de comunicações pelo SIRP.
Isto sem prejuízo do que adiante se afirmará quanto a alguns pontos concretos do regime constante da proposta de lei.

Assim, importa considerar, como resulta do já exposto, que o referido aresto não fundou o juízo de inconstitucionalidade apenas na consideração da natureza administrativa da Comissão de Controlo Prévio prevista no Decreto 426/XIII da Assembleia da República, e na não equivalência dos poderes daquele órgão *a uma intervenção em processo penal.*

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

Com efeito, o referido aresto concluiu que «*a proibição de ingerência nas comunicações, constante do artigo 34º da CRP, abrange os dados de tráfego*» e que «*Na verdade os fins e*

interesses que a lei incumbe ao SIRP de prosseguir, os poderes funcionais que confere ao seu pessoal e os procedimentos de atuação e controlo que estabelece, colocam o acesso aos dados de tráfego fora do âmbito da investigação criminal».

Acrescentando, por referência às atribuições do SIRP e às finalidades do acesso pretendido, que «[Ora*], a caracterização dessa concreta actividade como recolha de "informações" para efeitos de "prevenção" dissocia-a, de forma clara e precisa, da atividade própria da investigação criminal*. (...)».

Concluindo o Acórdão, depois de analisar a relação entre "informações" e "investigação criminal" que «*o legislador teve a preocupação de distinguir, em sentido material e orgânico, as duas atividades*» *distinção radical* « [que*] impede os oficiais de informação de intervirem no processo penal. As informações [...] visam a obtenção de um conhecimento específico necessário à tomada de decisões e não a recolha de prova conducente ao exercício da ação penal. Ainda que a recolha e a análise de informações possa ser utilizada na investigação criminal e com vista a medidas de prevenção policiais, não deixa de ser uma atividade autónoma e prévia à investigação criminal*».

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

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

Conclusão que assume maior impacto quando relacionada com a consideração de que a atribuição ao SIRP da possibilidade de acesso aos dados das comunicações (dados de tráfego, no que ora releva quanto ao acesso pretendido), não se insere nos limites constitucionalmente admitidos pelo nº 4 do art. 34º da CRP de restrição aos direitos fundamentais, pois, «*Ao definir o campo de incidência da lei restritiva do direito à inviolabilidade das comunicações peça "matéria de processo criminal" a Constituição ponderou e tomou posição (em parte) sobre o conflito entre os bens jurídicos protegidos por aquele direito fundamental e os valores comunitários, especialmente os da segurança, a cuja realização se dirige o processo penal. Não obstante as restrições legais ao direito à inviolabilidade das comunicações que o legislador está autorizado a estabelecer deverem obedecer à ponderação do princípio da proporcionalidade, a preferência abstrata pelo valor da segurança em prejuízo da privacidade das comunicações só pode valer em matéria de processo penal*».

Após se pronunciar quanto à eventual *existência de matérias em que o valor da segurança sobreleva os valores próprios do direito à inviolabilidade da comunicações cuja não inclusão no âmbito da restrição a estes direitos pudessem contrariar o plano ordenador do sistema jurídico-constitucional,* e de afirmar que o legislador constitucional ao longo das revisões constitucionais «*deixou inalterados os termos da norma permissiva de ingerência nas telecomunicações, estabelecida na 2ª parte do nº 4 do art. 34, e o seu alcance restrito a "matéria de processo criminal"*», o Tribunal Constitucional conclui que «Nada *autoriza, pois, a admitir uma eventual extensão do âmbito da ressalva final do nº 4 do art. 34º - para a qual, aliás, o intérprete, neste contexto concreto, não dispõe de instrumentos metodológicos adequados*».

2.3. A posição assumida pelo Tribunal Constitucional parece limitar a margem de atuação do legislador ordinário em sede de atribuição ao SIRP da possibilidade de acesso aos dados de comunicações, mesmo quando essa possibilidade seja, como é, nos termos da Proposta de Lei ora em análise, dirigida, no caso dos *dados de base* e de *localização*, a prevenir *atos de sabotagem, espionagem, terrorismo, proliferação de armas*

de destruição maciça e criminalidade altamente organizada, ou, *no caso dos dados de tráfego, a prevenir atos de espionagem e do terrorismo.*

De qualquer modo, a questão não parece ser unânime no seio do Tribunal Constitucional como resulta das posições assumidas nas duas Declarações de Voto constantes daquele Acórdão, e, que, ainda que em graus diferenciados, direcionam a interpretação do nº 4 do art. 34º da CRP no sentido de permitir a inclusão no seu âmbito normativo da atividade de prevenção do SIRP, no contexto dirigido aos fenómenos criminais que agora se contêm nos arts. 2º e 3º da Proposta de Lei.

Na verdade, afigura-se relevante a posição assumida naquelas Declarações no sentido de que uma interpretação integrada daquele normativo constitucional com outros normativos constitucionais, relativos à liberdade e à segurança e ao dever de o Estado garantir tais direitos, admite que o SIRP, para o exercício das suas funções no âmbito da prevenção de tais fenómenos, aceda a dados das comunicações.

É igualmente relevante do ponto de vista jurídico-constitucional, a abordagem feita numa dessas Declarações de Voto quanto às garantias de controlo e fiscalização da intervenção do SIRP nas comunicações.

Na verdade, não se poderá olvidar que o próprio Acórdão do Tribunal Constitucional apenas se pronunciou negativamente quanto a esta questão porque o sistema procedimental de controlo previsto no diploma da Assembleia da República tinha natureza administrativa e não garantia as exigências decorrentes da Constituição nesta matéria.

Segmento da questão que a Proposta de Lei não descurou ao prever um sistema de controlo externo - prévio e permanente, e de natureza judicial e judiciária -, e um sistema de controlo interno pela Comissão de Fiscalização de Dados e pelo Conselho de Fiscalização do SIRP. Sistema que poderá responder cabalmente às exigências constitucionais de efetiva garantia dos *princípios da necessidade, adequação,*

proporcionalidade ou proibição do excesso, de que a ingerência é dirigida a "alvos determinados" e delimitada por finalidades, também elas objeto de proteção constitucional, mensuráveis e passíveis de avaliação externa, e de que os dados não serão utilizados para outras finalidades.

2.4. Como referido, *a Declaração de Voto da Conselheira Maria Lúcia Amaral* coloca a desconformidade constitucional da norma que foi objeto de apreciação pelo Tribunal Constitucional nas questões relativas à inexistência de *um sistema de controlo interno quanto ao cumprimento dos limites legais das interceções de comunicações que fosse, ele também, protector da ameaça da liberdade que aquela interceção representa*. Sistema que, em seu entender, não cumpria as exigências decorrentes do nº 2 do art. 18º da CRP [5].

Sem prejuízo da questão base colocada pelo Tribunal Constitucional relativa delimitação do âmbito de aplicação do nº 4 do art. 34º, será igualmente relevante dar nota do que se afirma naquele aresto quanto à matéria concernente ao controlo da ingerência nas comunicações prevista na norma sobre que recaiu a apreciação de inconstitucionalidade.

Na verdade, após analisar a natureza e características da então proposta Comissão de Controlo Prévio para efeitos de aferição da suscetibilidade da sua adequação constitucional, afirma-se no citado acórdão 403/2015 «(...) *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*

[5] A norma não definia com a precisão necessária os limites da intervenção administrativa na liberdade individual, *pois ao se dizer que a intervenção seria legítima quando implicasse a adoção de meios «necessário, adequados e proporcionais, numa sociedade democrática, para o cumprimento das atribuições legais dos serviços de informação», equivale praticamente a dizer que toda a ponderação quanto à proporcionalidade da intervenção seria por inteiro devolvida à administração; (...) por outro lado, dizer-se que tal intervenção só seria possível para efeitos do disposto no nº 2 do art. 4º significava, pela amplitude e indeterminação da habilitação que era conferida à administração, que a intervenção desta última seria legítima numa tão vasta plêiade de circunstâncias que se tornaria praticamente impossível delimitar os fatores da sua não admissibilidade.* Por ultimo, e na ausência de tais limites, a intervenção prévia da *Comissão de Controlo Prévio não preencheria por si só a necessidade de controlo e fiscalização interna da intervenção administrativa, não constituindo um procedimento eficiente de controlo que prevenisse ou evitasse intromissões abusivas nas liberdades individuais.*

a atuação de acesso aos dados de comunicações privadas por parte dos oficiais dos serviços de informação como integrando um "processo criminal". (...)».

E, mais adiante, referindo-se às garantias relativas ao tratamento e conservação dos dados afirma-se que «(...) *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.*"

Acrescentando, relativamente aos termos da concreta intervenção daquela Comissão que, «(...) *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.»

Assim, e sem prejuízo da questão relativa ao âmbito do nº 4 do art. 34º e à distinção feita entre a atividade do SIRP e a investigação criminal, cremos que se poderá considerar que aquele Acórdão não rejeita alguma aproximação à admissibilidade de acesso dos serviços de informação a dados de comunicações, desde que o regime legal se conforme no sentido de garantir um controlo efetivo dessa atividade por entidade de natureza judicial que salvaguarde os direitos afetados, não apenas em sede de autorização mas, igualmente, no domínio de todo o tratamento, manutenção e eliminação da informação acedida.

Ora, sem prejuízo do que adiante se assinalará relativamente a alguns aspetos do regime legal constante da Proposta de Lei, como já referido, **afigura-se que o sistema de controlo ora proposto, quer quanto à exigência de autorização judicial quer quanto à manutenção dessa intervenção em momentos posteriores do processamento dos dados, poderá conformar-se às exigências constitucionais nesta matéria**.

Não sendo, igualmente, de desconsiderar, neste aspeto, as demais instâncias de controlo previstas na Proposta de Lei, as quais reforçarão as garantias de que a atividade desenvolvida pelos serviços de informação no âmbito do acesso aos dados de comunicação será desenvolvida e se manterá nos estritos limites das finalidades para as quais a autorização de acesso foi concedida.

2.5. Se assim se pode entender quanto à questão do controlo de acesso aos dados de comunicações, importa, no entanto, considerar a questão relativa à avaliação da natureza e finalidades da atividade dos serviços de informação.

Como se referiu, o Acórdão do Tribunal Constitucional assumiu a posição de que o âmbito de aplicação do nº 4 do art. 34º está limitado à investigação criminal, o que exclui, na sua leitura jurídica, a atividade de prevenção dos serviços de informação.

A Conselheira Maria Lúcia Amaral, na sua Declaração de Voto, aceita, porém, que *havendo afinidade valorativa ou teleológica entre as finalidades prosseguidas pelos serviços de informação e as normas penais incriminadoras (...) poder-se-ia concluir (...) que a autorização constitucional para restringir a inviolabilidade das telecomunicações em «matérias de processo criminal» se estenderia, por maioria de razão, ao SIRP.*

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

Por sua vez, a Declaração de Voto do Conselheiro Teles Pereira aprofunda a análise das diferentes vertentes da questão do acesso a dados de comunicação pelos serviços de informação, referindo existir uma relação de complementaridade entre a atividade dos Serviços de Informações e o processo penal.

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

Na verdade, se o SIRP tem como finalidade assegurar, através dos dois Serviços de informações que o integram, no estreito respeito da Constituição e da lei, a produção de informações necessárias à salvaguarda da segurança interna e externa, da independência e interesses nacionais e da unidade e integridade do Estado (artigo 2º do Decreto n.º 426/XII) e se desenvolve atividades de recolha, processamento, exploração e difusão de informações necessárias à salvaguarda da independência nacional, dos interesses nacionais e da segurança interna e externa do Estado Português, informações que contribuam para garantir as condições de segurança dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade, informações adequadas a prevenir a sabotagem, a espionagem, o terrorismo, e sua proliferação, a criminalidade altamente organizada de natureza transnacional e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido (artigo 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."

Aprofundando a análise no domínio dos *princípios da proporcionalidade e da proibição do excesso* afirma o Senhor Conselheiro que «*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.»

Assim, e em seu entender, as questões de constitucionalidade suscitadas no pedido de fiscalização preventiva deveria ser respondidas 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.»

Ora, da conjugação dos elementos referenciados, **afigura-se que a posição defendida em ambas as Declarações de Voto quanto à admissibilidade constitucional de acesso pelos serviços de informação aos dados das comunicações não poderá deixar de ser levada em conta como referencial jurisprudencial de uma visão interpretativa conforme à Constituição.**

Entendimento que deverá ser ponderado face aos valores em confronto, em qualquer dos casos constitucionalmente protegidos e sem natureza absoluta.

Devendo ainda relevar-se a circunstância de que o regime proposto de acesso aos dados de telecomunicações e Internet pelo SIRP se restringe à sua atividade de prevenção de atos potencialmente conformadores de ilícitos criminais, que poderão, com forte probabilidade, determinar a intervenção estadual em sede de repressão para defesa da segurança coletiva e do Estado de Direito.

Não descurando a tese vencedora do Acórdão do Tribunal Constitucional, **cremos que se poderá afirmar que num espaço como o da hermenêutica jurídico-constitucional o elemento literal não poderá ser erigido como única fonte interpretativa, desde logo quando está em causa o equilíbrio entre direitos fundamentais de natureza não absoluta, quando a ingerência se insere num âmbito de proximidade finalística com o que resulta do elemento literal da norma, e quando os procedimentos reguladores garantem a *necessidade, adequação e proporcionalidade* da ingerência e o controlo da atividade desenvolvida, e consequentemente, a salvaguarda dos direitos afetados.**

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

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

Sendo certo que as finalidades da atividade do *Centro Nacional de Inteligencia*, embora genericamente coincidentes com as finalidades do SIRP, são elencadas na lei com menor especificação no que tange à prevenção de atividades criminosas[6].

Não se olvida que a norma Constitucional espanhola poderá permitir uma interpretação mais abrangente que o nº 4 do art. 34º da Constituição portuguesa, pois ali se determina que «*Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*»[7]

Estipulando o nº 2 do art. 55º da Constituição Espanhola que «*Una ley orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas*

[6]Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia – Art. 1º «El Centro Nacional de Inteligencia es el Organismo público responsable de facilitar al Presidente del Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones».
[7] Art. 18º nº 3.

determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas».

II – Apreciação específica

1. Artigos 1.º e 2º - Objeto e definições

1.1. O n.º 1 do artigo 1.º estabelece que "*A presente lei regula um procedimento especial de acesso a dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas (...).*

A menção a "*dados previamente armazenados*" quererá esclarecer- e bem, em nosso entender – que esta lei não visa criar qualquer nova obrigação de *conservação de dados* (expressão utilizada pela Lei 32/2008 e que nos parece mais adequada que a expressão "*armazenados*") por parte dos prestadores de serviços de comunicações, mas apenas permitir o respetivo acesso por parte do SIRP, como exceção ao regime de tratamento de dados pessoais e proteção da privacidade no setor das comunicações eletrónicas.

Estas exceções à privacidade dos dados de telecomunicações encontram-se previstas no n.º 4 do artigo 1.º da Lei 41/2004, de 18 de agosto, segundo o qual "*as exceções à aplicação da presente lei que se mostrem estritamente necessárias para a proteção de atividades relacionadas com a segurança pública, a defesa, a segurança do Estado e a prevenção, investigação e repressão de infrações penais são definidas em legislação especial*".

A não criação de uma nova obrigação de *conservação de dados* apenas para os serviços de segurança é relevante, não só para os prestadores de serviços, como por não se justificar, tendo até em conta o enquadramento constitucional acima analisado, que o SIRP tivesse acesso a dados a que as autoridades judiciárias não poderiam aceder no âmbito da investigação criminal, e que são, no essencial, os dados conservados nos

termos da Lei 41/2004 e, sobretudo, o âmbito alargado de dados conservados previstos na Lei 32/2008, precisamente destinados ao combate a crimes graves.

A alteração que adiante sugerimos para o n.º 1 do artigo 1.º visa precisamente clarificar que o SIRP pode aceder a todos os dados conservados pelos prestadores de serviços de comunicações eletrónicas, independentemente da finalidade legal que fundamentou essa conservação.

Veja-se que o n.º 1 do artigo 3.º da lei 32/2008 estabelece que *"A conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes"*. Com base nesta norma os prestadores de serviço – e de forma justificada - recusam transmitir, mesmo às autoridades judiciárias no âmbito de investigações criminais, dados que detêm quando não estão em causa crimes graves (pressupondo a legalidade deste regime de conservação de dados apesar da jurisprudência sobre esta matéria do TJCE, que não cumpre analisar nesta sede).

1.2. Por outro lado, constata-se uma **incoerência normativa entre as finalidades do acesso previstas no nº 1 do art. 1º e as finalidades previstas no art. 2º.**

a. De acordo com o nº 1 do art. 1º os dados de comunicações a que o SIRP poderá aceder são os *que se mostrem estritamente necessários para a prossecução da* sua atividade *de produção de informações relacionadas com a segurança interna, a defesa, a segurança do Estado e a* ***prevenção da espionagem e do terrorismo***.

Prevendo-se no art. 2º e no art. 3º, respetivamente, o acesso a *dados de base* e de *localização de equipamentos* e o acesso a *dados de tráfego*.

Como já referido, é diferente o âmbito das finalidades de um e de outro acesso.

Assim:

O art. 3º restringe acesso a *dados de tráfego* às finalidades de *produção de informações necessárias à prevenção de atos de espionagem e do terrorismo* – previsão que coincide com as finalidades de acesso previstas no nº 1 do art. 1º.

Já, contudo, o art. 2º prevê que o acesso aos *dados de base* e de *localização do equipamento* tem como finalidade 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.***

Previsão que não encontra, pois, total cobertura no nº 1 do art. 1º, uma vez que alarga o acesso também às finalidades de *prevenção de atos de sabotagem, proliferação de armas de destruição maciça e criminalidade altamente organizada.*

Ora, não se vislumbra qualquer justificação para que o nº 1 do art. 1º não traduza, na sua totalidade, o efetivo objeto da lei e do procedimento especial que esta visa regular.

Com efeito, o procedimento especial regulado na lei é aplicável ao acesso às três categorias de dados, apenas divergindo o âmbito das finalidades - mais restrito no caso de acesso aos *dados de tráfego*. Diferença que, contudo, não justifica que não se insiram na norma do nº 1 do art. 1º, atento o seu carácter enquadrador, as finalidades, mais alargadas, de acesso aos *dados de base* e de *localização*.

Sendo certo que a omissão de referência, naquele preceito, a tais finalidades, que constituem o fundamento substantivo jurídico-constitucional de admissibilidade desse acesso, poderá suscitar dúvidas interpretativas que importará acautelar em matéria de natureza tão sensível como a que é objeto do diploma que se pretende aprovar.

b. Por outro lado, cremos que se mostrará justificado e aconselhável que o diploma se apresente coerente também do ponto de vista concetual e do objeto quando estejam em causa realidades idênticas e os objetivos que se pretendem sejam os mesmos.

É o caso dos conceitos de *segurança interna*, *defesa* e *segurança do Estado* (nº 1 do art. 1º) e de *defesa nacional* e *segurança interna* (art. 2º), em ambos os casos enquanto finalidades do acesso aos dados e, no fundo, enquanto condição prévia desse acesso.

Assim, sem prejuízo de poder existir coincidência concetual material entre uns e outros daqueles conceitos, não se vislumbra, no entanto, e até por isso mesmo, razão para que no artigo 2º não sejam utilizados os exatos conceitos do nº 1 do art. 1º.

Nessa medida, **sugere-se:**

(i) que se pondere **a alteração do nº 1 do art. 1º no sentido de no mesmo passarem a constar as finalidades de prevenção de *atos de sabotagem, proliferação de armas de destruição maciça e criminalidade altamente organizada.***

(ii) que se pondere **a alteração do artigo 2º no sentido de no mesmo serem utilizados os conceitos de *segurança interna, defesa e segurança do Estado* que são objeto da previsão do nº 1 do art. 1º.**

c. Sem prejuízo do referido e sugerido nos pontos anteriores, suscita-se a eventual ponderação da previsão relativa à *criminalidade altamente organizada* para efeitos de acesso a dados de comunicação pelo SIRP no âmbito da sua atividade de prevenção nesse âmbito.

Com efeito, o conceito processual penal de *criminalidade altamente organizada* previsto na al. m) do art. 1º do Código de Processo Penal[8], abarca um alargado e diferenciado leque de crimes, nos quais se incluem ilícitos criminais que integram o habitualmente designado fenómeno de criminalidade económico-financeira, como é o caso dos crimes de *corrupção, tráfico de influência, participação económica em negócio ou branqueamento*.

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

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

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

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

1.3. Ainda no artigo 1.º, uma vez que, como vimos, o presente diploma não visa criar um novo regime de *conservação de dados*, entendemos que o **n.º 4 não deve incluir a menção "conservação", mas apenas referir-se a "transmissão"**, uma vez que a conservação dos dados visa, não só as finalidades do diploma agora em análise, como as finalidades previstas noutros diplomas legais.

De referir que, em nosso entender, **esta norma poderia ser eliminada por falta de conteúdo normativo autónomo**, uma vez que a *conservação de dados* está prevista noutros diplomas e os termos da transmissão constam das restantes normas da proposta de lei.

Pelo acima exposto, **sugere-se a seguinte redação para o nº 1 do art. 1º e para o artigo 2º:**

Artigo 1º

Objeto e definições

1 - ***A presente lei regula o acesso pelo Sistema de Informações da República Portuguesa (SIRP) aos dados previamente conservados pelos prestadores de serviços de comunicações eletrónicas, mediante autorização judicial e controlo do Ministério Público, quando se mostre estritamente necessário para a prossecução da atividade de produção de informações relacionadas com a segurança interna, a defesa, a segurança do Estado e a prevenção da espionagem e do terrorismo e de atos de sabotagem, proliferação de armas de destruição maciça e criminalidade altamente organizada.***

2 (...)

3 (...)

4. *(sugere-se a eliminação ou, em alternativa a seguinte redação)* ***A 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 ***segurança interna, defesa e segurança do Estado*** *e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada, e no seu exclusivo âmbito.*

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

a. Epígrafe

Considerando a sistemática do preceito e o diferente nível de intervenção funcional das entidades no mesmo previstas, *e sem prejuízo do que adiante se referirá quanto à intervenção do/a Procurador/a-Geral da República*, cremos que se justificará que a epígrafe seja alterada na ordem de indicação do objeto da norma, sugerindo-se a seguinte formulação: «*Autorização judicial e comunicação ao Ministério Público*».

b. *Formação das secções criminais do Supremo Tribunal de Justiça* - Nº 1 do art. 4º, arts. 7º,10º, 11º e 16º, este por referência ao aditamento de um nº *4 ao art. 47º* e de um *nº 3 ao art. 54º da Lei 62/2013, de 26 de agosto*]

Prevê-se, em consonância com a formulação proposta para o nº 4 do art. 47º e para o nº 3 do art. 54º da Lei 62/2013, de 26 de agosto, que a autorização judicial obrigatória e prévia para acesso aos dados de comunicações pelo SIRP é da competência de *uma formação das secções criminais do Supremo Tribunal de Justiça*.

O mesmo tipo de designação é utilizado no art. 7º, nº 1 do art. 10º e no art. 11º, bem como no nº 4 do art. 47º e nº 3 do art. 54º, Lei de Organização do Sistema Judiciário, que o art. 16º da proposta de lei pretende aditar.

Não questionando a solução adotada para apreciação do pedido formulado pelo SIRP e para a concessão de autorização e controlo de acesso, cremos, contudo, que a designação *"formação das secções criminais do Supremo Tribunal de Justiça"* não tem correspondência com os conceitos que, no âmbito da organização judiciária, designam legal e funcionalmente, o conjunto de juízes com competência para a prática de atos processuais ou procedimentais.

Cremos, pois, que se justificará a ponderação da designação adotada pela Proposta de Lei, fazendo apelo a conceitos e designações organizativas que traduzam identidade com o nosso sistema judicial.

Assim, e tendo em consideração a estrutura organizativa da designada "*formação*", está em causa um *coletivo* de juízes do Supremo Tribunal de Justiça constituído pelos presidentes das secções criminais e por um juiz designado pelo Conselho Superior da magistratura de entre os mais antigos dessas secções.

Nessa medida, **sugere-se** seja ponderada a alteração de designação "*formação das secções criminais do Supremo Tribunal de Justiça*" pela designação "***coletivo de juízes das secções criminais do Supremo Tribunal de Justiça***".

Em conformidade sugere-se a seguinte redação para o nº 1 do artigo 4º e para o art. 7º:

Artigo 4º

«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 de ***um coletivo de juízes 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».*

Artigo 7º

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 ***um coletivo de juízes das secções criminais do Supremo Tribunal de Justiça****, constituído pelos* ***respetivos*** *presidentes e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos* ***daquelas*** *secções.*

Propõe-se, igualmente, que, **adotando-se a formulação sugerida, sejam efetuadas as correspondentes alterações de designação no nº 1 do art. 10º e no art. 11º.**

c. Artigos 47º e 54º da Lei 62/2013 - Pese embora, na sistemática de análise adotada (por sequência de normas), as anotações a efetuar a estes preceitos se justificassem em momento posterior, uma vez que se irá propor a alteração da designação *"formação das secções criminais do Supremo Tribunal de Justiça"* e as correspondentes adequações de redação, optou-se por proceder, agora, à análise da totalidade das questões que julgamos dever suscitar relativamente a estas normas.

Assim:

(i) No nº 4 do art. 47º da Lei 62/2013, preceito que regula a organização do STJ, para além da alteração da designação *"formação das secções criminais do Supremo Tribunal de Justiça"* para ***coletivo de juízes das secções criminais do Supremo Tribunal de Justiça***, **sugere-se ainda a eliminação da descrição, neste preceito, das suas competências materiais**. Isto porque está em causa normativo relativo à organização, e também porque aquelas competências se encontram já previstas no nº 3 que se pretende aditar ao art. 54º, (ainda que essas competências se encontrem formuladas de modo diverso em cada um dos preceitos, como seguidamente se anotará).

(ii) De qualquer modo, se a opção recair sobre a manutenção, neste preceito, da descrição daquelas competências materiais, cremos que importará salvaguardar divergências relativas ao seu conteúdo, situação que parece ocorrer na redação de cada um dos preceitos.

Na verdade, no nº 4 do art. 47º, prevê-se que a *"formação de secções criminais"* do STJ *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.*

Por seu turno, o nº 3 do art. 54º prescreve que aquela *"formação" 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.*

Ora, se o que se pretende com o regime especial a criar é sujeitar todos os casos de acesso do SIRP a dados de comunicações a controlo e autorização judicial obrigatória e prévia, como parece ser o objetivo da Proposta de Lei, afigura-se que a formulação do nº 4 do art. 47º - ao apenas se referir à atividade do SIRP em matéria de espionagem e terrorismo - parece restringir essa autorização judicial ao acesso a *dados de tráfego* (que apenas podem ser acedidos para aqueles efeitos) com a consequente restrição da competência da *"formação de secções criminais"* do STJ.

No entanto, haverá que considerar, para além do mais, o que se dispõe no art. 2º da Proposta de Lei, bem como o facto de o nº 3 do art. 54º, que ora se pretende aditar à Lei 62/2013, não restringir àquela categoria de dados a competência para autorização, na medida em que prevê expressamente não só os *dados de tráfego* como também os *dados de base*.

Ao que acresce que o art. 7º da Proposta não limita o controlo judicial a uma concreta categoria de dados de comunicações, antes prevendo esse controlo de forma ampla por referência genérica a *"dados de telecomunicações e Internet"*.

Por outro lado, a previsão do nº 2 do art. 9º (relativo à *apreciação judicial* do pedido de acesso) não tem como objetivo limitar a autorização judicial àquela categoria de dados (de tráfego) mas sim reafirmar, agora do ponto de vista da decisão de autorização, o que resulta já de outras normas da Proposta, designadamente do art. 3º, ou seja, que o acesso aos dados de tráfego é concedido apenas para efeitos de prevenção da *espionagem* e do *terrorismo*.

De onde decorre, salvo melhor opinião, que o nº 4 do art. 47º fica aquém do que é, efetivamente, o escopo do procedimento especial previsto na Lei que se pretende aprovar e do que são as efetivas competências da *"formação de secções criminais do*

Supremo Tribunal de Justiça", pelo que, a manter-se a sua redação, o diploma padecerá de incoerências normativas que não deixarão de suscitar dúvidas interpretativas.

Não pode, ainda, deixar de se anotar que o nº 3 do art. 54º omite a referência aos *dados de localização do equipamento* - dados que a Proposta de Lei define autonomamente na al. b) do nº 3 do art. 1º, e que delimita, quanto às finalidades de acesso, no art. 2º.

Assim, ainda que na conceção dominante os *dados de localização* sejam integrados no conceito de *dados de tráfego*, o que se verifica é que a Proposta autonomiza esses dados, quer em sede de definições quer em sede de finalidades de acesso (segmento em que os equipara a dados de base). Nessa medida, cremos que, mais uma vez, a Proposta cria incoerências internas ao nível normativo-concetual, situação que, pela sua relevância prática e interpretativa, deverá ser salvaguardada.

Justificando-se assim que a menção aos *dados de localização* seja incluída na redação do nº 3 que se pretende aditar ao art. 54º da Lei 62/2013, ou, em alternativa, se reformule a redação desse preceito, de modo a, num conceito amplo de dados de telecomunicações e Internet, a abranger todas as categorias de dados objeto do diploma e do procedimento especial que visa regular.

Assim, **sugerem -se as seguintes formulações para o nº 4 do art. 47 e para o nº 3 do art. 54º da Lei 62/2013:**

«Artigo 47.º

Organização

[...]

1 - [...].

2 - [...].

3 - [...].

4 -No Supremo Tribunal de Justiça funciona ainda ***um coletivo de juízes das secções criminais, constituído pelos respetivos presidentes*** *e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções,* ***para efeitos do procedimento especial previsto na lei que aprova o regime especial de acesso a dados de telecomunicações e de Internet pelo SIRP.***

Artigo 54º

(...)

3. O coletivo de juízes das secções criminais constituído nos termos do nº 4 do art. 47º, *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,* ***a dados de localização*** *e a dados de tráfego de comunicações eletrónicas pelo SIRP.»*

Ou, em alternativa,

3 - O coletivo de juízes das secções criminais constituído nos termos do nº 4 do art. 47º *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 telecomunicações e Internet pelo SIRP.»***.

d. O nº 2 do art. 4º prevê que *o processo de autorização de acesso aos dados é sempre comunicado ao/à Procurador/a-Geral da República.*

Por seu turno, o nº 1 do art. 8º prevê que o pedido de acesso a dados de telecomunicações e Internet é enviado, pelo Secretário-Geral do SIRP[9] ao Presidente do Supremo Tribunal de Justiça, com conhecimento ao/à Procurador/a-Geral da República.

[9] Anota-se que na redação do preceito se verifica omissão de designação, apenas se referindo "Secretária/o-Geral da República".

É também dado conhecimento ao/à Procurador/a Geral da República da transmissão dos dados ao SIRP (nº 1 do art. 10º), e, para efeitos do exercício das suas competências legais, são-lhe comunicadas as decisões de cancelamento de acesso e de destruição dos dados, (nº 4 do art. 11º).

Finalmente, são-*lhe imediatamente comunicados os dados obtidos que indiciem a suspeita de crimes de espionagem e terrorismo* (art. 12º).

Quanto a esta última comunicação, tomar-se-á posição aquando da análise do art. 12º uma vez que a sugestão a fazer difere um pouco do que ora se procurará dar nota e sugerir.

Assim, salvo no caso do art. 12º e, de algum modo, do nº 4 do art. 11º - quando faz apelo genérico ao *exercício das suas competências legais*[10] -, da leitura da proposta resulta que a intervenção do Procurador/a da República se encontra delineada numa perspetiva de controlo formal, uma vez que, pese embora as comunicações previstas, nada se prevê quanto à possibilidade de intervenção para efeitos de apreciação da legalidade do pedido.

Na verdade, caso o pedido formulado não conforme os requisitos – formais e substantivos – previstos na lei, o/a Procurador/a-Geral da República não tem, com base na lei que se pretende aprovar, e no domínio do concreto procedimento especial de autorização de acesso, qualquer efetiva competência de intervenção. O que se traduz, na prática, na impossibilidade de exercer qualquer efetivo controlo, designadamente em matéria de legalidade.

Tanto assim que a possibilidade de intervir no procedimento através dos magistrados que representam o/a Procurador/a-Geral da República no Supremo Tribunal de Justiça se mostra totalmente arredada na versão da Proposta de Lei na medida em que não lhe é também conferida competência de intervenção no procedimento especial - o qual

[10] E que se ligarão a competências externas ao procedimento especial. Trata-se sem dúvida, tal como no artigo 12º, de competências no âmbito do processo penal, uma vez que poderão estar em causa decisões de destruição de dados obtidos de forma ilegal ou abusiva, ou violadores do âmbito de autorização judicial prévia.

não conforma, como claramente resulta da lei, qualquer tipo de procedimento em que a competência de intervenção concreta do Ministério Público resulte de outros dispositivos legais.

A efetiva intervenção do/da Procurador/a-Geral da República desde o início do procedimento, nos termos que adiante se sugerem, não expõe o procedimento e a atividade de acesso a dados a qualquer interpretação espúria sobre a sua natureza, nem interfere com princípios estruturantes do sistema, designadamente em sede de separação funcional da atividade do SIRP da atividade de investigação criminal, na medida em que a intervenção pretendida se cinge *à defesa da legalidade* – vertente funcional constitucionalmente atribuída ao Ministério Público (art. 219º da CRP), e que apenas pode ser exercida no âmbito de atribuições concretas, de conteúdo formal e material devidamente densificado na lei.

Por outro lado, o acesso aos dados de comunicações e Internet pelo SIRP respeita ao exercício das competências dos serviços de informação em matéria de prevenção de fenómenos ou atos que, pondo em causa valores estruturantes do estado de direito, são criminalmente puníveis.

Devendo, igualmente salientar-se que o acesso a dados mais intrusivos, como sejam os dados de tráfego, se cinge à prevenção de *atos de espionagem e terrorismo.* O que ocorre, de igual modo, com o acesso às demais categorias de dados de comunicação.

Ao que acresce que a deteção de indícios da prática daqueles crimes obriga aqueles serviços à comunicação imediata ao/à Procurador/a-Geral da República.

Ou seja, será relevante a relação de interconexão que se estabelece entre as finalidades daquela atividade preventiva e a atividade de investigação criminal que lhe poderá suceder.

Finalmente, não poderá deixar de se salientar também que a efetiva intervenção do/a Procurador/a-Geral da República é indissociável da intervenção judicial, no Supremo Tribunal de Justiça, prevista na Proposta de Lei. Não se podendo conceber um sistema em que, face ao objeto e às finalidades do pedido e do procedimento, aquela *intervenção* fique cingida ao mero conhecimento da existência do pedido e das decisões ao mesmo atinentes, sem que possa intervir em qualquer das fases do procedimento.

Ora, a Proposta de Lei é totalmente omissa quanto ao que efetivamente poderá o/a Procurador/a-Geral da República fazer na posse das comunicações de formulação do pedido, da autorização dada e das decisões de cancelamento e destruição de dados que a Proposta de Lei prevê que lhe sejam feitas no âmbito do procedimento especial de autorização e controlo do acesso aos dados pelo SIRP.

O mero conhecimento do procedimento e do pedido, sem que se densifique uma concreta competência de intervenção, não se afigura suficiente para que se possa entender estar em causa um efetivo controlo por parte do/da Procurador/a-Geral da República enfraquecendo, deste modo, o controlo das entidades judiciárias e o correspondente juízo sobre a constitucionalidade do sistema proposto.

A especial sensibilidade da matéria imporá, pois, que o/a Procurador/a-Geral da República possa intervir no procedimento especial a que se refere a Proposta de Lei, não se compreendendo, assim, que apenas se prevejam meras comunicações, procedimentos, que não poderão deixar de consubstanciar em mero controlo formal.

Nessa medida, cremos que se poderá conceber um sistema de intervenção que, sem colocar em causa ou desvirtuar a natureza do procedimento, garanta o exercício, pelo/a Procurador/a-Geral da República, de um efetivo controlo do acesso do SIRP aos dados de telecomunicações e Internet para efeitos das finalidades que o justificam.

Assim, cremos que se exigirá a atribuição de concretas competências ao/à Procurador/a-Geral da República no âmbito do procedimento especial, desde o

seu início, e não apenas o conhecimento da sua existência e da decisão no mesmo proferida.

Nessa conformidade, para que ocorra uma efetiva fiscalização/controlo do acesso, e mantendo-se, como é evidente, a iniciativa do SIRP tal como prevista no art. 8º, considera-se que o pedido de acesso deverá ser remetido ao/à Procuradora-Geral da República, que emitirá pronúncia sobre o mesmo em matéria de legalidade (apreciação e pronúncia sobre a verificação dos requisitos formais e substanciais do pedido, de acordo com o previsto na lei especial de acesso e com a Constituição da República).

Dever-lhe-á, igualmente, ser atribuída competência de pronúncia relativamente ao cancelamento de procedimentos e à destruição dos dados a que se refere o atual nº 3 do art. 11º.

Tudo conforme redação que, nos respetivos artigos 8º e 11º, se irá sugerir.

Quanto ao art. 4º, e tendo apenas por referencial o sistema que ora se propõe, **cremos que a epígrafe do art. 4º e a redação do seu nº 2, merece alteração nos seguintes termos:**

Artigo 4.º

Autorização judicial e intervenção do Ministério Público

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 Ministério Público intervém no processo de autorização de acesso aos dados por intermédio do/da Procurador/a-Geral da República, nos termos definidos na presente lei.

3. Artigo 5º - Admissibilidade

O nº 1 do art. 5º fixa as condições de admissibilidade do pedido de acesso aos dados – Da conjugação do preceituado no nº 1, e também com o disposto na al. c) do nº 2 do art. 8º, parece resultar que o acesso pode ser autorizado quando não exista um *alvo* ou *intermediário determinado*.

Na verdade, e de acordo com o nº 1, o acesso pode reportar-se à obtenção de *informação sobre um alvo ou um intermediário determinado* **ou** à *obtenção de informação que seria muito difícil ou impossível de obter de outra forma ou em tempo útil para responder a situação de urgência.*

A conjunção alternativa ***"ou"*, bem como a ressalva da al. c) do nº 2 do art. 8º quanto à identificação da pessoa ou pessoas envolvidas nos factos - *"caso sejam conhecidas"*** - sugere, pois, que o pedido de acesso a dados pode ser formulado e autorizado sem que esteja determinado um concreto *alvo* ou *intermediário*.

O que, a ser assim, poderá suscitar dúvidas sobre a admissibilidade de acesso nos casos a que se refere a al. b) do nº 1 do art. 5º da Proposta de Lei.

Por outro lado, deixa igualmente a dúvida sobre se o acesso nos termos da al. a) não depende da impossibilidade ou dificuldade de obtenção, por outra forma, ou em tempo útil, em caso de urgência, das informações que se pretendem obter. Ou seja, se, no caso de *alvos* ou *intermediários determinados*, o SIRP poderá recorrer ao acesso aos dados de comunicação como meio normal de produção de informações, não dependendo esse acesso da impossibilidade ou dificuldade de obter as informações pretendidas através de outros meios.

Nessa medida, e porque, salvo melhor opinião, esta questão se revela nuclear no regime especial que se pretende criar, tendo em consideração os limites constitucionais à ingerência nas telecomunicações e outros dados de comunicação, **importará clarificar qual a concreta relação entre as condições de admissibilidade previstas no nº 1 do art. 5º. Em especial, clarificar se na al. a) não se exige que o acesso seja, no momento, a única via de produção das informações necessárias às finalidades de prevenção para aquele caso concreto, e se a condição da al. b) não demanda a existência de um *alvo determinado*.**

4. Artigo 6º - Agravação

A proposta de lei prevê que «*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*»

Corresponde, pois, à agravação das penas aplicáveis aos referidos crimes, se em concreto se verificarem as circunstâncias agravantes de *violação da proibição de ingerência* previstas na norma.

Estão em causa os crimes de *Devassa por meio de informática* (art. 193º do CP), de *Violação de correspondência ou de telecomunicações* (art. 194º do CP), *Violação de segredo de correspondência ou de telecomunicações* (art. 384º do CP), *Acesso ilegítimo e Interceção ilegítima* (arts. 6º e 7º da Lei 109/2009) e de *Acesso indevido* (art. 44.º da Lei n.º 67/98).

Não pondo em causa a bondade da agravação das penas nem a circunstância agravante prevista, afigura-se, porém, que, do ponto de vista da técnica legislativa, a norma não apresenta clareza suficiente, o que importará garantir, desde logo porque estão em causa de condutas penalmente puníveis.

Assim, se o que se pretende, como parece resultar, desde logo, da epígrafe do preceito, é a agravação das penas dos crimes especificamente elencados na norma, afigura-se que a mesma deveria ser redigida de modo mais claro e direto.

Nessa medida, e seguindo a técnica legislativa utilizada neste domínio, designadamente no Código Penal, permitimo-nos **sugerir que seja ponderada a alteração da redação da norma, eventualmente nos seguintes termos**:

Artigo 6º

Agravação

«***Quando os crimes 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, forem cometidos com violação da proibição de ingerência do pessoal do SIRP na correspondência, nas telecomunicações e nos demais meios de comunicação, o agente é punido com a pena aplicável ao crime respetivo agravada de um terço nos seus limites mínimo e máximo.***»

5. Art. 8º - Iniciativa

a. O art. 8º, sob a epígrafe "*Iniciativa*", identifica quem, no âmbito do SIRP, pode dar início ao procedimento de autorização judicial prévia de acesso aos dados (nº 1), e define a forma e o conteúdo desse pedido (nº 2).

Afigura-se que a epígrafe não reflete o efetivo objeto da norma, **sugerindo-se a eventual alteração para "*Pedido de acesso*"**.

b. Na sequência do que acima se sugeriu **quanto às competências a atribuir ao/à Procurador/a-Geral da República** sobre o pedido de acesso pelo SIRP a dados de telecomunicações e Internet, **sugere-se que a seguinte redação para o nº 1 do artigo 8º:**

Art. 8º

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.

2. O pedido é enviado pela/o Secretária/o-Geral do Sistema de Informações da República Portuguesa (SIRP) à/ao Procurador/a-Geral da República que, após emitir pronúncia em matéria de legalidade, o apresenta ao Presidente do Supremo Tribunal de Justiça para os efeitos previstos na presente lei em matéria de controlo judicial e autorização prévia pelo coletivo de juízes das secções criminais daquele Tribunal.

3. Atual número 2 (com o aditamento de uma alínea e) abaixo sugerida).

4. Atual nº 3 (caso não seja aceite a sugestão abaixo formulada de transferência deste normativo para o artigo 1º).

c. Periodicidade da transmissão dos dados

Nos termos do n.º 2 do artigo 5.º *"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"*, proibição que é repetida na parte final do n.º 3 do artigo 8.º *("nem a ligação em tempo real às redes de comunicações eletrónicas")*.

No mesmo sentido, o n.º 1º do artigo 10.º estabelece que a transmissão dos dados tem de ser "diferida".

Ora, compreendendo que a lei proíba o *acesso direto em linha* – exigindo assim um ato de transmissão de dados do prestador de serviços para o SIRP para um maior controlo do acesso aos dados - pensamos que em certos casos mais urgentes – que competirá ao Tribunal validar – se pode justificar que o SIRP tenha conhecimento imediato e

permanente dos *dados de tráfego* ou de *localização* do visado (veja-se o caso de uma visita a Portugal, de curta duração, de uma pessoa suspeita de intensa catividade terroristas).

E na verdade, afirmar o carácter diferido da transmissão não esclarece se o diferimento terá de ser de semanas, dias, horas ou minutos.

Uma vez que a lei permite que o SIRP pretenda aceder a dados futuros – pois só assim se compreende que exista uma "*duração das medidas pontuais de acesso*" – torna-se essencial que o tribunal mencione, no despacho, a periodicidade de transmissão dos dados (diariamente, semanalmente ou mesmo assim que ocorra qualquer registo, com um efeito similar a ligação em tempo real mas sem acesso direito).

Pelo exposto, **sugere-se que se acrescente no n.º 2 do artigo 8.º uma alínea e) com o seguinte teor:**

«e) A periodicidade de transmissão dos dados futuros podendo, em casos excecionais e especialmente fundamentados, ser determinada a transmissão imediata dos dados após o seu registo».

d. No nº 3 o preceito insere a definição do conceito de «*medidas pontuais de acesso*», a que se reportará o pedido, conforme, aliás, previsto nas diversas alíneas do seu nº 2.

Estando em causa a definição de um conceito para efeitos da lei a aprovar, e tendo o legislador optado por inserir, no nº 2 do art. 1º, um elenco de definições para aqueles mesmos efeitos, **afigura-se que, por uma questão de coerência sistemática, se poderia ponderar a inclusão da definição de «*medidas pontuais de acesso*» neste normativo (nº 2 do art. 1º).**

Aliás, estando em causa o acesso aos *dados de telecomunicações* e de *Internet* cujos conceitos estão definidos naquele preceito, cremos que melhor se adequaria que ali se

congregassem todos os conceitos que, para efeitos daquela lei, se considerou deverem merecer particular definição.

6. Artigo 11.º - Garantias

O artigo 11º regula o controlo judicial do acesso aos dados por parte do SIRP, após a autorização prevista no artigo 9.º, norma que reputamos essencial para a conformidade constitucional do respetivo acesso a dados de telecomunicações.

Para além de, tendo em conta o conteúdo normativo do artigo, se **sugerir a alteração da epígrafe para "Fiscalização judicial"**, cumpre salientar que os dados de comunicações podem, como vimos, implicar a recolha de dados futuros, durante o período de manutenção da medida.

Esta medida exige um controlo jurisdicional regular durante a sua efetivação, para que o tribunal avalie regularmente a sua *proporcionalidade, adequação e necessidade*.

Para o efeito, deverá tomar-se como referência o procedimento de fiscalização judicial do acesso a dados de telecomunicações previsto do Código de Processo Penal, cuja formulação atual decorreu de uma larga jurisprudência constitucional que tem sedimentado as regras necessárias para que se possa considerar efetiva aquela fiscalização.

Assim, se no que se refere aos dados de base ou de períodos anteriores ao pedido, a mera comunicação dos mesmos ao Tribunal permite que este exerça a sua função de fiscalização, no que se refere aos dados de comunicações futuros a recolher durante um certo período de tempo, a principal lacuna do projeto reside na ausência de acompanhamento periódico dos dados recolhidos.

Embora o regime previsto no artigo 188.º do CPP se aplique aos *dados de conteúdo*, sendo a obtenção e junção aos autos de *dados de localização* ou de *tráfego* regulados pelo n.º 2 do artigo 189º do mesmo diploma, entendemos que existem dois elementos

que **devem estar presentes no caso em análise para uma efetiva fiscalização judicial do acesso aos dados de comunicações:**

a) A fiscalização periódica dos dados obtidos;

b) A competência judicial para ordenar a destruição dos dados alheios às finalidades visadas e, se for o caso, para determinar a cessação imediata da medida.

Se o segundo se encontra previsto na proposta, o mesmo não acontece com o primeiro.

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

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

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

No mesmo sentido, a elaboração de um relatório pela entidade que recebe os dados de comunicações é essencial para que a decisão judicial possa ser esclarecida. Veja-se que

os *dados de tráfego* ou *localização* obtidos podem ser apenas listagens de números e de comunicações, as quais, sem um esclarecimento pelos serviços, podem ser ininteligíveis, frustrando o controlo jurisdicional.

Por fim, e como já acima referido, entendemos que o/a Procurador/a-Geral da República não deverá ter uma mera intervenção formal, devendo assumir integralmente a sua função de controlo da legalidade, pronunciando-se sobre qualquer pedido de acesso a dados, nos termos já sugeridos, bem como sobre a destruição de dados ou a cessação do respetivo acesso.

Assim, **sugerimos que se adicione entre os números 2 e 3 do atual artigo 11.º da proposta de lei, dois números com o seguinte teor**:

«3 – No que se refere aos dados de tráfego ou de localização os serviços que procedem à análise dos dados e informações transmitidas lavram o correspondente auto e elaboram relatório no qual descrevem de modo sucinto o respetivo conteúdo e, fundamentadamente, explicam o seu alcance para as finalidades que determinaram o respetivo acesso».

«4 – Os autos e relatórios previstos no número anterior são remetidos de 15 em 15 dias a partir do início da primeira receção de dados e informações ao coletivo de juízes das secções criminais ao/à Procurador/a-Geral da República, que emite pronúncia para os efeitos previstos no número seguinte.»

(...) atual nº 3

(...) atual nº 4

7. Art. 12º - *Factos indiciários de espionagem e terrorismo*

a. Prevê-se neste artigo que «*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.*».

Compreende-se a preocupação do legislador na inserção de uma tal previsão na lei que regula o procedimento especial de acesso aos dados de telecomunicações e de Internet, desde logo porque esse acesso apenas pode ter como finalidade, nos termos do artigo 1º, *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.***[11]

No entanto, cumpre referir que esta última finalidade - a *prevenção da espionagem e do terrorismo* – não é a única que se relaciona com a prevenção de atos de natureza criminal, como decorre do art. 2º, no qual se prevê que o acesso a *dados de base* e de *localização* tem como finalidade a *produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna e a* ***prevenção de atos de sabotagem***[12]***, espionagem, terrorismo, proliferação de armas de destruição maciça***[13] ***e criminalidade altamente organizada***[14]*, e no seu exclusivo âmbito.*

Assim, podendo os dados obtidos com o acesso indiciar a prática de outros crimes inseridos no âmbito da atividade do SIRP em sede de prevenção, e sendo também essa atividade que justifica a autorização de acesso, não parece haver justificação para que a comunicação a que se refere o art. 12º da Proposta seja limitada apenas aos crimes de *espionagem* e *terrorismo.*

---

[11] Negrito nosso.
[12] Crimes de sabotagem contra a defesa nacional (art. 315º) e de sabotagem (art. 329º).
[13] Poder-se-á ter em consideração a punição, pelo art. 275º do Código Penal, dos atos preparatórios para execução dos atos integradores dos crimes dos artigos 272º e 273º do CP, ou mesmo o art. 86º, nº 1, al. a) e b) da Lei 5/2006, de 23/2.
[14] Os crimes que integram o conceito de '*Criminalidade altamente organizada*' previsto na alínea m) do art. 1º do Código de Processo Penal: *as condutas que integrarem crimes de associação criminosa, tráfico de pessoas, tráfico de armas, tráfico de estupefacientes ou de substâncias psicotrópicas, corrupção, tráfico de influência, participação económica em negócio ou branqueamento.*

Tanto mais que os demais atos objeto da atividade de prevenção do SIRP assumem, igualmente, gravidade bastante para a imediata comunicação ao Ministério Público dos indícios da prática do crime que esses atos são passíveis de integrar.

Pelo que se sugere que o referido preceito seja reponderado no sentido de alargar o objeto da comunicação aos dados obtidos que indiciem a prática de todos os crimes que se insiram na atividade de prevenção do SIRP, de acordo com o âmbito definido no art. 1º e no art. 2º.

b. A norma do art. 12º prevê que a comunicação seja feita ao Procurador- Geral da República *para os devidos efeitos*.

Está em causa a prática de crimes de elevada gravidade e danosidade, que poderá exigir a intervenção célere do Ministério Público e dos órgãos de polícia criminal que o coadjuvam, designadamente para a adoção e concretização das medidas cautelares que o caso justificar, de modo a garantir a celeridade e eficácia da investigação e a possível sustação da atividade criminosa.

Nessa medida, **cremos que se justificará a ponderação de que a comunicação a que se refere o art. 12º seja efetuada a uma concreta estrutura do Ministério Público com competência de investigação, com conhecimento ao Procurador-Geral da República.**

Considerando o tipo de crimes em causa e a natureza e competência do Departamento Central de Investigação e Ação Penal (DCIAP), conforme disposto no nº 1 do art. 46º e nos nºs 1 e 2 (quanto à coordenação da direção da investigação) e nº 3 (quanto à direção da investigação e exercício da ação penal) do art. 47º, ambos do Estatuto do Ministério Público, afigura-se ser este Departamento que reunirá as características e competências legais para receber a comunicação e, nos termos do Código de Processo Penal, dar imediato início à investigação, e, se for caso disso, praticar os demais atos eventualmente necessários a transmitir o inquérito para o departamento competente, nos termos do nº 1 do art. 266º do Código de Processo Penal, ou a solicitar ao

Procurador-Geral da República o deferimento de competência nos termos da al. b) do art. 47º do Estatuto do Ministério Público.

c. Por fim, no sentido de esclarecer que os dados comunicados podem, não só dar início a um inquérito criminal, mas serem nessa sede utilizados como meio de prova, eliminando dúvidas que, a serem suscitadas em juízo, colocariam em causa irremediavelmente o combate à criminalidade grave e organizada, sugere-se que se adicione a este normativo um novo número com o seguinte teor: "***Os dados comunicados nos termos do número anterior podem ser utilizados em processo penal***".

Atente-se que será muito provável que os dados obtidos nesta sede se mostrem cruciais para suportar e validar eventual intervenção imediata das autoridades judiciárias e órgãos de polícia criminal no âmbito do inquérito que seja instaurado, designadamente para efeitos de realização de diligências urgentes de obtenção de prova, detenções ou promoção de medidas intrusivas.

Tendo em consideração o exposto, **sugere-se a seguinte redação para o art. 12º:**

Artigo 12º

Factos indiciários de crimes

Para os devidos efeitos, são de imediato comunicados ao Departamento Central de Investigação e Ação Penal, com conhecimento ao/a Procurador/a Geral da República, os dados obtidos que indiciem a prática:

a. De crimes de sabotagem, espionagem e terrorismo;

b. De crimes que integrem o conceito de "criminalidade altamente organizada" previsto na al. m) do artigo 1º do Código de Processo Penal;

c. De atos preparatórios puníveis nos termos do artigo 275º do Código Penal destinados à execução dos crimes previstos nos artigos 272º e 273º do Código Penal ou da prática destes crimes;

d. De crimes previstos nas alíneas a) e b) do nº 1 do artigo 86º da Lei 5/2003, de 23 de fevereiro, na redação da Lei n.º 50/2013, de 24/07.»

2. Os dados comunicados nos termos do número anterior podem ser utilizados em processo penal.

Lisboa, 2 de junho de 2017