COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Exmº Senhor
Presidente da Comissão de Assuntos
Constitucionais, Direitos, Liberdades
e Garantias
Dr. Fernando Negrão

N/Ref.
02.06
Proc. n.º 8837/2015
Of. n.º 18218 2015-06-26

Assunto: Parecer sobre a Proposta de Lei n.º 345/XII/4ª (GOV).

Com referência ao ofício dessa Comissão n.º747/XII/1ª – CACDLG/2015 de 17.06.2015, sobre o assunto em epígrafe remete-se a V. Exª, em anexo, cópia do Parecer n.º51/2015, emitido pela CNPD em 26.06.2015, no âmbito do pedido formulado.

Informa-se, que o referido Parecer irá ser objeto de ratificação na próxima Sessão Plenária da CNPD.

Com os melhores cumprimentos

P.I A Secretária da CNPD

(Isabel Cristina Cruz)

MM

ASSEMBLEIA DA REPÚBLICA
Divisão de Apoio às Comissões
CACDLG
N.º Ofício 528/496
Entrada n.º 847 de 26/06/2015

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
www.cnpd.pt

21 393 00 39
LINHA PRIVACIDADE
Dias úteis das 10 às 13 h
duvidas@cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

PARECER N.º 51/2015

I. Pedido

O Presidente da Comissão dos Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República remeteu à Comissão Nacional de Proteção de Dados (CNPD) a Proposta de Lei n.º 345/XII/4ª (GOV) que aprova o regime do Sistema de Informações da República Portuguesa, para emissão do competente parecer.

O pedido formulado decorre das atribuições conferidas à CNPD pelo n.º 2 do artigo 22.º da Lei n.º 67/98, de 26 de outubro – Lei de Proteção de Dados Pessoais (LPDP), e o parecer é emitido no uso da competência fixada na alínea a) do n.º 1 do artigo 23.º do mesmo diploma legal.

II. Apreciação

A apreciação da CNPD no presente parecer cinge-se às matérias relativas à proteção de dados pessoais, considerando as suas competências legais, reconhecidas pela LPDP e pela Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto ao acesso a dados pessoais.

Assim, a análise dividir-se-á em duas partes: a primeira respeitante ao acesso aos dados pessoais dos cidadãos pelos serviços que compõem o Sistema de Informações da República Portuguesa (SIRP); a segunda referente ao registo de interesses dos membros do Conselho de Fiscalização do SIRP, do Secretário-geral do SIRP e dos membros do gabinete deste órgão, pessoal dirigente e demais pessoal do SIRP.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

1. Acesso a dados pessoais sensíveis

A proposta de lei prevê, no artigo 78.º, n.º 2, que os *oficiais de informações do SIS e do SIED podem, para efeitos da alínea c) do n.º 2 do artigo 4.º, 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, data hora, duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização, sempre que sejam necessários, adequados e proporcionais, numa sociedade democrática, para o cumprimento das atribuições legais dos serviços de informações, mediante a autorização obrigatória da Comissão de Controlo Prévio.*

Importa recordar que as atribuições do SIRP implicam as atividades de recolha, processamento, exploração e difusão 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* (cf. alínea c) do n.º 2 do artigo 4.º).

Note-se que o referido artigo 4.º, n.º 2, alínea c), da Proposta comporta a novidade de estabelecer como atribuição ou finalidade da atividade do SIRP a prevenção da *criminalidade altamente organizada de natureza transnacional.* Em relação a este conceito, cumpre notar que o Código do Processo Penal, na alínea m) do artigo 1.º, define criminalidade altamente organizada como *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.*

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Ora, esta inovação legislativa suscita dúvidas em termos de compatibilização das funções do SIRP com as da Polícia Judiciária – a quem nos termos da lei também cabe a atribuição de prevenção criminal, competindo-lhe para o efeito proceder às diligências adequadas ao esclarecimento das situações e à recolha de elementos probatórios (cf. artigo 2.º e alínea b) do n.º 1 e n.º 2 do artigo 4.º da Lei n.º 37/2008, de 6 de agosto, alterada pela Lei n.º 26/2010, de 30 de agosto.

De facto, não se alcança como se pode conciliar a proibição dirigida ao pessoal do SIRP de exercer poderes, praticar atos ou desenvolver atividades do âmbito ou competência específica dos tribunais, do Ministério Público ou das entidades com funções policiais (cf. n.º 2 do artigo 5.º e n.º 1 do artigo 94.º da Proposta) com a previsão do carácter exclusivo dos órgãos e serviços do SIRP de tais funções e atividades (cf. n.º 2 do artigo 6.º da Proposta).

Repare-se que a questão releva diretamente para a proteção de dados pessoais, porquanto isso poderá significar termos dois organismos públicos com competências sobrepostas cujo exercício se repercute, de forma intrusiva, diretamente na privacidade dos cidadãos. A questão é, pois, a de saber se com a eventual aprovação da Proposta se deve ter por excluída do âmbito das atribuições e competências da Polícia Judiciária a função de prevenção da alta criminalidade organizada de natureza transnacional. A ser assim, sugere-se a revisão dos preceitos acima indicados por forma a tornar clara essa exclusão.

Mas mesmo admitindo como legítima a atribuição ao SIRP da função de prevenção da alta criminalidade organizada de natureza transnacional – aspeto que a CNPD aqui não põe em causa, a não ser nos termos acima expostos pela sua eventual repercussão na tutela dos direitos fundamentais dos cidadãos –, os poderes atribuídos ao SIRP no n.º 2

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

do artigo 78.º suscitam as maiores reservas à CNPD quanto à respetiva conformidade com a Constituição da República Portuguesa (CRP), em especial do n.º 2 do artigo 18.º e do n.º 1 e 2 do artigo 26.º, n.º 4 do artigo 34.º e n.º 4 do artigo 35.º, e com o artigo 8.º, n.ºs 1 e 2, da Convenção Europeia dos Direitos do Homem e com os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia.

Na verdade, se se reconhece que as finalidades visadas com a constituição do SIRP implicam a atividade de vigilância secreta, não pode por simples invocação de tais finalidades a lei determinar quaisquer medidas, sem que sejam garantidas soluções adequadas, precisas e efetivas contra o abuso e a arbitrariedade. Isto porque, «onde, como aqui, um poder do executivo é exercido em segredo, os riscos de arbitrariedade são evidentes»; a natural falta de transparência do processo de vigilância implica a sua «não sujeição ao escrutínio pelos indivíduos ou pelo público em geral» e tem, por isso, de ser compensada por uma lei suficientemente tuteladora dos direitos fundamentais (Acórdão do Tribunal Europeu dos Direitos do Homem de 6.06.2006, Caso SEGERSTEDT-WIBERG e outros c. Suécia, pedido n.º 62332/00). Esta é, aliás, a jurisprudência constante do Tribunal Europeu dos Direitos do Homem (TEDH) - veja-se o acórdão de 6.09.1978, caso Klass e outros c. Alemanha, pedido n.º 5029/71, cuja jurisprudência é reiterada no acórdão mais recente de 18.05.2010, caso Kennedy c. Reino Unido, pedido n.º 26839/05.

Precisamente pela impossibilidade, que resulta da natureza das coisas, de o vigiado não poder ter conhecimento de que o está a ser, a recolha e análise de informação pessoal tem de ser o mais enquadrada possível pela lei. Em consequência, «numa área em que o abuso é potencialmente facilitado nos casos individuais e que pode ter consequências tão lesivas para a sociedade democrática no seu todo» (Acórdão do TEDH de 6.09.1978) tem a lei de prever um sistema de controlo efetivo, a ter lugar em três momentos distintos: no momento da decisão de vigiar, durante o procedimento de

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

vigilância e quando o mesmo tiver terminado (neste Sentido, v. a mesma jurisprudência do TEDH). E que as medidas a adotar, porque restringem substancialmente a vida privada, cumpram o princípio da proporcionalidade, nas suas diferentes vertentes.

Vejamos.

a. *A violação do n.º 4 do artigo 34.º da CRP*

Na verdade, determina o n.º 4 do artigo 34.º da CRP a proibição de *toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal.*

Do teor deste preceito constitucional resulta que a inviolabilidade dos meios de comunicação privada, que o mesmo consagra, «inclui a proibição de ingerência nos meios de comunicação, salvo nos casos previstos na lei (reserva de lei) em matéria de processo penal (e não para outros efeitos) e mediante decisão judicial» (Gomes Canotilho/ Vital Moreira, *Constituição da República Portuguesa Anotada*, I, 2007, anot. VII ao artigo 34.º, p. 543). Repare-se, pois, que a ingerência nos meios de comunicação só é admissível se prevista por lei no âmbito de processo penal e mediante decisão judicial.

Uma lei que admita semelhante ingerência em meios de comunicação fora do âmbito de um processo penal está só por si a violar esta proibição constitucional, ou, se se preferir, a restringir direitos, liberdades e garantias em violação do n.º 2 do artigo 18.º da CRP, por ultrapassar o âmbito da autorização constitucional de restrição.

Importa, para o efeito, notar que o n.º 4 do artigo 34.º quando se refere a *toda* a ingerência pretende com isso proibir não apenas o conhecimento do conteúdo das comunicações mas também todas as informações associadas aos meios de

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

comunicação: os chamados dados de tráfego e de localização (neste sentido, Gomes Canotilho/ Vital Moreira, *op. cit.,* anot. VIII ao artigo 34.º, p. 544; Germano Marques da Silva, in Jorge Miranda/ Rui Medeiros, *Constituição Portuguesa Anotada*, anot. IV ao artigo 34.º).

Estes, pela sua natureza, são dados que revelam a todo o momento aspetos da vida privada e familiar dos indivíduos: onde estamos ou estivemos (desde que transportemos connosco o telemóvel, com quem contactamos (chamada por telefone ou telemóvel, envio ou receção de SMS ou de correio eletrónico), com que regularidade contactamos, que sítios da Internet consultamos, etc. A recolha e análise desta informação, inequivocamente pessoal, só pode, pois, ser feita com os limites que o próprio artigo 34.º definiu.

Ora, o n.º 2 do artigo 78.º da Proposta determina a recolha dos dados de tráfego e de localização, dados pessoais – de resto, qualificados como sensíveis pelo n.º 1 do artigo 7.º da LPDP, por revelarem aspetos da vida privada – fora do contexto do processo criminal. Nessa medida, o estatuído no n.º 2 do artigo 78.º viola não apenas o direito à privacidade dos meios de comunicação, como também o direito à reserva da intimidade da vida privada e familiar e o direito à proteção dos dados pessoais, consagrados na CRP (respetivamente, artigos 34.º, 26.º e 35.º) e na Carta dos Direitos Fundamentais da União Europeia (artigos 7.º e 8.º).

Aparentemente, o legislador pretende aqui ultrapassar a inobservância do requisito constitucional, com a institucionalização de um controlo prévio de que se faz depender a recolha e análise de todos os dados sensíveis acima elencados, em que a autorização compete a uma Comissão composta por três juízes (nos termos previstos no artigo 35.º e 36.º da Proposta). Todavia, esta solução de criar condições equiparáveis materialmente àquele requisito do contexto do processo criminal (já que

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

no plano formal, o requisito nunca estará assim cumprido) não assegura a mesma garantia, decorrente da exigência constitucional de um processo penal, que a intervenção judicial confere. O que se pretende é a contextualização da restrição da privacidade num específico processo com todas as garantias que o mesmo implica: intervenção de um poder estadual distinto do poder administrativo, cuja função é a de garantir os direitos fundamentais dos cidadãos.

Ora, não se afigura que um órgão administrativo, como é a Comissão de Controlo Prévio, independentemente da natureza estatutária dos seus membros, se possa equiparar a um órgão judicial, para assim se ter por preenchido o requisito constitucional "em processo penal". A recolha de dados pessoais de tráfego ou de localização feita no contexto de um processo criminal é delimitada, naturalmente, pelo âmbito de investigação processual. Ou seja, apenas se recolhem as informações no contexto daquele específico processo, aberto e instruído para a investigação de um concreto crime (ou conjunto de crimes) em relação a um específico suspeito ou a específicos suspeitos.

Coisa bem distinta é permitir que um órgão administrativo autorize a recolha e análise de informação sem referência a concretos suspeitos. E a verdade é que, apesar do esforço de precisão dos elementos que devem acompanhar o pedido de controlo prévio, logo ressalta, da análise da alínea c) do n.º 2 do artigo 37.º da Proposta, que poderá não haver identificação das pessoas visadas por esse acesso. Por outras palavras, a Proposta de Lei deixa espaço para que o acesso aos dados sensíveis acima elencados se faça de forma massiva de modo a detetar padrões de conduta que permitam reconduzir qualquer cidadão a perfis de potenciais suspeitos de terrorismo, criminalidade altamente organizada, etc. Esta forma de obtenção de informação para efeitos de prevenção de *sabotagem, proliferação, espionagem, terrorismo, criminalidade altamente organizada de natureza transnacional e prática de atos que,*

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

pela sua natureza, possam alterar ou destruir o Estado de Direito Democrático constitucionalmente estabelecido é, em si mesma, altamente discriminatória, comportando além do mais riscos de descontextualização da informação recolhida e de erros de valoração grosseiros dos comportamentos da massa de cidadãos que a esta prática pode ficar exposta.

Demais, o n.º 1 do artigo 36.º apresenta uma redação, no mínimo, muito duvidosa: apenas sujeita a autorização da referida Comissão o acesso aos dados previstos no n.º 2 do artigo 78.º se o acesso for suscetível de contender com a reserva da intimidade da vida privada. Ora, se se admitir que a reserva da intimidade da vida privada tem um âmbito mais restrito do que a vida privada e familiar, dimensão jurídica esta que sempre será afetada com um acesso desta natureza, conclui-se querer o legislador dar "carta branca" aos serviços do SIRP para vasculhar os dados pessoais sensíveis de todos os indivíduos que se encontrem no território nacional, sem dependência de qualquer controlo prévio.

Na verdade, apenas quando em causa esteja a reserva da intimidade da vida privada (cujas fronteiras com a vida privada *lato sensu* são de delimitação difícil) é que tal controlo é obrigatório. Ficando por esclarecer quem determina, *ex ante,* que o acesso é suscetível ou não de contender com a reserva da intimidade da vida privada e, consequentemente, quem determina que o acesso depende de autorização da Comissão de Controlo Prévio. Dir-se-á ser o próprio oficial do SIRP que decide, antecipadamente, se a informação que pretende recolher pode ou não afetar a intimidade da vida privada. É por demais evidente que um controlo deste tipo, em que o controlado decide discricionariamente se há ou não controlo, deixa desprotegidos, com uma extensão e intensidade tal, os direitos à privacidade dos meios de comunicação, à proteção de dados pessoais e à reserva da intimidade da vida privada, com a

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

consequência de aquele não ser suscetível de se equiparar ao controlo que o processo criminal assegura.

Nestes termos, a CNPD entende que a institucionalização de um controlo prévio nos termos descritos na Proposta não é suficiente para ultrapassar o incumprimento do requisito previsto na parte final do n.º 4 do artigo 34.º da CRP, concluindo, assim, pela inconstitucionalidade do disposto no n.º 2 do artigo 78.º da CRP (por violação do n.º 4 do artigo 34.º e do n.º 2 do artigo 18.º da CRP).

Até porque não está aqui institucionalizado um sistema de controlo efetivo *ex post*, como o que vale para a investigação policial – em que é possível, no âmbito de inspeções, verificar com rigor quem, quando, a quê e em que condições se acedeu aos dados pessoais sensíveis, para além da possibilidade de defesa, com arguição de nulidades quanto à recolha da prova de utilização e de meios de obtenção de prova, e com possibilidade de recurso de despachos judiciais. Os poderes de controlo reconhecidos ao Conselho de Fiscalização do SIRP e ao Conselho de Fiscalização Comissão de Fiscalização de Dados estão longe de ter esta extensão e precisão.

Com o mesmo fundamento, por não estar assegurado o controlo efetivo desta ingerência nos direitos à vida privada e familiar e à correspondência, que o TEDH tem entendido ser necessário para se ter por suficientemente delimitada e justificada a mesma ingerência (cf. acórdãos acima citados), parece poder concluir-se pela violação do n.º 1 do artigo 8.º da Convenção Europeia dos Direitos Do Homem.

b. *A desproporcionalidade do acesso aos dados de tráfego e aos dados de localização*

Além do mais, importa atender ao facto de os dados de localização e os dados de tráfego relativos às consultas na Internet só constarem da base de dados das

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

comunicações eletrónicas que as operadoras têm o dever de manter nos termos da Lei n.º 32/2008, de 17 de julho, que transpôs para a ordem jurídica portuguesa a Diretiva n.º 2006/24/CE, do Parlamento e do Conselho, de 15 de março (Diretiva da Retenção de Dados). Em rigor, os restantes dados de tráfego também se encontram conservados nesta base de dados, embora sejam igualmente tratados noutras bases de dados das operadoras, no âmbito da faturação, por períodos de tempo inferiores.

A tais dados, dispõe essa lei, só podem aceder as autoridades judiciárias e as autoridades de polícia criminal elencadas na alínea f) do n.º 1 do artigo 2.º deste diploma legal e para a finalidade de investigação, deteção, repressão de crimes graves por parte destas autoridades, mediante despacho fundamentado do juiz, sendo que os dados só podem dizer respeito a suspeito ou arguido, a pessoa que sirva de intermediário e a vítima de crime.

Não obstante as precisões feitas nesta lei a delimitar o acesso, e que, repare-se, não têm correspondência, na Proposta de Lei agora analisada, a Diretiva da Retenção de Dados (Diretiva n.º 2006/24/CE) foi declarada inválida pelo Tribunal de Justiça da União Europeia – TJUE (Acórdão de 8 de abril de 2014, Proc. C-293/12 e C-594/12), sem que a validade da Lei n.º 32/2008, ao abrigo da qual as operadoras são obrigadas a conservar pelo período de um ano e transmitir dados de localização e de tráfego, tenha ainda sido apreciada na nossa ordem jurídica – base de dados a que os serviços do SIRP irão aceder parte da informação que pretendem, elencada no n.º 2 do artigo 78.º.

Em suma, o SIRP vai aceder a uma base de dados cuja legitimidade não está ainda determinada na nossa ordem jurídica.

Independentemente do juízo que venha ser formulado quanto à validade da Lei n.º 32/2008, importa atentar nos argumentos expendidos pelo TJUE e que calham aqui

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

como uma luva. O TJUE considera que a conservação das bases de dados e o acesso à mesma pelas autoridades nacionais competentes constitui uma ingerência de grande amplitude e gravidade nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia.

Desenvolvendo, *a luta contra a criminalidade grave, designadamente a criminalidade organizada e o terrorismo, por mais fundamental que seja, não pode, por si só, justificar que uma medida de conservação como a que foi instituída pela Diretiva 2006/24 seja considerada necessária para efeitos da referida luta* (cf. § 51). Esta afirmação do TJUE vale também para esta sede, se, para demonstrar a inconstitucionalidade e a violação dos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, houvesse ainda necessidade de demonstrar a violação do princípio da proporcionalidade de tal solução.

É que os termos em que se prevê, no n.º 2 do artigo 78.º da Proposta de Lei, a possibilidade de acesso aos dados de tráfego e de localização abrangem, como se demonstrou atrás, *de forma generalizada todas as pessoas, todos os meios de comunicação eletrónica e todos os dados relativos ao tráfego, não sendo efetuada uma diferenciação, limitação ou exceção em função do objetivo de luta contra as infrações graves.* (§ 57 do referido acórdão). Isto é tanto mais relevante, quanto há sempre o risco de utilização abusiva desta informação, sem possibilidade efetiva do controlo.

Com efeito, e aproveitando as palavras proferidas pelo Tribunal a propósito da Diretiva, a Proposta de lei *abrange, em geral, todas as pessoas que utilizam serviços de comunicações eletrónicas, sem que, no entanto, as pessoas cujos dados são conservados se encontrem, mesmo indiretamente, numa situação suscetível de dar lugar a ações penais. Assim, aplica-se mesmo a pessoas para as quais não existe nenhum indício suscetível de fazer crer que o seu comportamento possa ter uma qualquer relação, mesmo indireta ou longínqua, com infrações graves. Além disso, não prevê nenhuma exceção, pelo que é aplicável mesmo a pessoas cujas comunicações, segundo as regras do direito nacional, estão sujeitas ao segredo profissional* (§ 58 do

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

referido acórdão) – pense-se, por exemplo, na profissão de jornalista ou de advogado, em que a simples informação de com quem se contacta e a ocasião, a duração e a regularidade dos contactos pode invadir com grande intensidade o sigilo profissional.

A esta ausência geral de limites acresce que [não se] estabelece um critério objetivo que permita delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior para prevenir, detetar ou agir penalmente contra infrações suscetíveis de ser consideradas, à luz da amplitude e da gravidade da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, suficientemente graves para justificar tal ingerência. (§60 do mesmo acórdão).

Conclui-se, pois, que o acesso aos dados de tráfego e de localização, constantes das bases de dados criadas ao abrigo da Lei n.º 32/2008, nos termos abertos em que vem formulado na Proposta de Lei (cf. n.º 2 do artigo 78.º, n.º 1 do artigo 36.º e n.º 2 do artigo 37.º), representa uma restrição aos direitos à privacidade dos meios de comunicação, à reserva da intimidade da vida privada e familiar e à proteção dos dados pessoais – e à liberdade, pelo condicionamento a esta que tal devassa sempre implicará –, cuja necessidade e proporcionalidade em sentido estrito não está demonstrada, nem se verifica, em clara violação do n.º 2 (*in fine*) do artigo 18.º da CRP.

c. *A desproporcionalidade do acesso a dados pessoais bancários e fiscais*

Mas a este ponto não se restringe a reserva da CNPD quanto à conformidade constitucional da previsão do n.º 2 do artigo 78.º da Proposta. É que a norma prevê ainda o acesso a *informação bancária* e a *informação fiscal*.

Em causa estão dados pessoais sujeitos ao regime especial de sigilo, porque reveladores da vida privada e familiar. Com efeito, este tipo de dados revela informação sobre onde fomos e onde estamos (cada vez que realizamos uma operação bancária, ou adquirimos um bem ou serviço com a indicação do NIF), que património temos, que

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

rendimentos auferimos e qual a fonte desses rendimentos, em que gastamos o nosso dinheiro, onde e quanto gastamos, qual o nosso agregado familiar, se no mesmo se integram deficientes e com que grau de deficiência, etc. O acesso a estes dados pessoais sensíveis (cf. n.º 1 do artigo 7.º da LPDP) sempre configura uma restrição dos direitos à reserva da intimidade da vida privada e familiar e à proteção dos dados pessoais, consagrados na CRP (respetivamente, 26.º e 35.º) e na Carta Europeia dos Direitos Fundamentais (artigos 7.º e 8.º).

Nos termos da lei, tais dados são suscetíveis de acesso por autoridades públicas no estrito âmbito de investigação criminal, portanto, no contexto estrito de um processo criminal, devidamente tutelado pelas autoridades judiciárias que velam pela legalidade dos atos praticados.

Ora, em relação a estes dados sensíveis (sigilosos), importa verificar se a restrição operada pelo disposto no n.º 2 do artigo 78.º da Proposta, cumpre todas as exigências constitucionais, aqui especialmente relevando a proporcionalidade da restrição legal dos direitos, liberdades e garantias, nos termos do n.º 2 do artigo 18.º da CRP. Sendo certo que a avaliação aqui em vista abrange um juízo sobre a adequação, a necessidade e a proibição do excesso. Como ensinam Gomes Canotilho e Vital Moreira, «[p]ara que a restrição seja constitucionalmente legítima, torna-se necessária a verificação *cumulativa* das seguintes condições: [...] que a restrição vise salvaguardar outro direito ou interesse constitucionalmente protegido (n.º 2, *in fine*); que a restrição seja exigida por essa salvaguarda, seja apta para o efeito e se limite à medida necessária para alcançar esse objetivo (n.º 2, 2.ª parte); [...]».

Não pondo em causa a legitimidade da finalidade visada, que é evidentemente de interesse nacional, logo surgem as dúvidas quanto à idoneidade ou adequação do acesso a esta informação para tal finalidade – por não se afigurar evidente que um

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

terrorista ou membro de uma associação criminosa transnacional deixe rastro das transações comerciais que realiza nas bases de dados bancárias ou fiscais, ou declare os seus rendimentos e as respetivas fontes à Autoridade Tributária.

Mas, independentemente de tal juízo sobre a adequação, a qual não está *prima facie* demonstrada, não se alcança a imprescindibilidade desse acesso. Com efeito, a ordem jurídica portuguesa prevê já mecanismos aparentemente ágeis para assegurar a obtenção de informação pelo SIRP. É o que sucede, por exemplo, com o mecanismo de interação criado pela Lei da Segurança Interna (Lei n.º 53/2008, de 29 de agosto) no âmbito do Conselho Superior de Segurança Interna, ou com o acesso a ficheiros de entidades públicas, previsto no n.º 1 do artigo 78.º, e que se concretiza nos termos a definir em protocolos, ouvida a CNPD.

Mas ainda que se pudesse entender ser necessária tal informação, persiste a conclusão da desproporcionalidade deste acesso. A falta de precisão ou densidade normativa do n.º 2 do artigo 78.º, ao prever o acesso a informação bancária e fiscal, sem mais delimitações, associada à abertura assumida no plano dos fundamentos e do universo de indivíduos a abranger com tais medidas – que, em rigor, pode corresponder à totalidade das pessoas que se encontra no território nacional (n.º 2 do artigo 37.º da Proposta) –, permite concluir que a elevadíssima quantidade e a especial qualidade (sensibilidade) dos dados suscetíveis de acesso implica uma restrição não admissível, por insuportável, dos direitos à privacidade dos meios de comunicação, à reserva da intimidade da vida privada e familiar e à proteção dos dados pessoais, e à liberdade, consagrados na CRP, na Convenção Europeia dos Direitos do Homem e na Carta dos Direitos Fundamentais. Além de corporizar igualmente um perigo evidente de utilizações abusivas e porventura para outros fins.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Se a tais dados somarmos os dados de tráfego e de localização (permanente), potencialmente relativos, reitera-se, a todos as pessoas que se encontram no território nacional, impõe-se a conclusão de que as vantagens que possam de tal acesso decorrer não compensam, não são suficientes para justificar a restrição grosseira daqueles direitos fundamentais.

Impõe-se, pois, nesta matéria a proibição do excesso como limite último à atividade estadual de vigilância, sob pena de se negar o Estado de Direito que a mesma atividade pretende promover.

d. *Outros aspetos de regime*

Acresce que, como se disse atrás, pela natureza da atividade desenvolvida pelos serviços do SIRP, a recolha e análise de informação pessoal é evidentemente feita sem conhecimento dos titulares dos dados pessoais. Por essa razão, o tratamento de dados pessoais realizado tem de estar particularmente delimitado por lei e com garantias de um efetivo controlo.

Ora, a delimitação temporal da recolha dos dados pessoais, que nos termos da alínea d) do n.º 2 do artigo 37.º da Proposta, pode estender-se por três meses, sucessivamente renováveis, sem limite, parece violar o princípio da proporcionalidade.

Também a ausência de fixação de um prazo da conservação dos dados pessoais põe em causa os princípios básicos de tratamentos de dados pessoais. Apenas se prevê, no n.º 7 do artigo 37.º, o poder-dever do Secretário-Geral do SIRP para determinar a destruição dos dados pessoais que não tenham relação com o objeto ou finalidades da autorização. O que significa, desde logo, que em relação a toda a informação pessoal relativa à vida privada recolhida sem passar pelo crivo do controlo prévio (cf. o que se disse supra, sobre o n.º 1 do artigo 36.º da Proposta), não está consagrado este dever.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Portanto, nestes casos e quando a informação relativa à intimidade da vida privada tenha conexão com a finalidade da autorização, a informação pode ou deve(?) ser conservada *ad eternum* nas bases de dados do SIRP. É, por demais, evidente a desproporcionalidade da conservação sem limite deste tipo de dados pessoais, entendendo a CNPD que a presente Proposta de lei deveria integrar uma norma que impusesse especificamente como objeto de verificação por parte da Comissão de Fiscalização de Dados a avaliação da necessidade de conservação dos dados pessoais sensíveis obtidos por esta via – os termos genéricos da previsão constante do n.º 3 do artigo 30.º da Proposta não se afiguram ser suficiente.

Em relação ao n.º 1 do artigo 78.º, importa ainda notar que a inovação introduzida de ouvir a CNPD antes da celebração dos protocolos de acesso aos ficheiros das entidades públicas, não afasta o disposto na LPDP em relação ao desvio de finalidade do tratamento de dados pessoais realizado pelas entidades públicas, em especial a necessária autorização da CNPD nos termos da alínea c) do n.º 1 do artigo 23.º da LPDP para que a entidade pública transmita ou disponibilize os dados pessoais para finalidade distinta da que determinou a recolha.

e. *Conclusão*

Em síntese, a opção legal de previsão de forma aberta, pouco precisa, da possibilidade de acesso (sem controlo prévio ou com um reduzido controlo) a uma massa imensa de dados pessoais sensíveis relativos a quaisquer pessoas (porventura, todos os cidadãos portugueses ou todos os que se encontrem em território nacional), sem que exista qualquer tipo de indício de prática ou ligação às atividades criminosas e atentatórias da segurança nacional que se visa prevenir, com o risco evidente de uso abusivo dos dados, viola o disposto no n.º 2 do artigo 18.º e no n.º 1 e n.º 2 do artigo 26.º, n.º 1 do artigo 27.º, n.º 4 do artigo 34.º e n.º 4 do artigo 35.º da CRP, e no artigo 8.º, n.ºs 1 e 2,

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

da Convenção Europeia dos Direitos do Homem e nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia.

A simples menção de que o acesso e análise dos dados será feita segundo o princípio da proporcionalidade é insuficiente, por não ser acompanhada da previsão de garantias efetivas para a sua concretização.

A extensão e intensidade do tratamento de dados pessoais realizado, de dados que revelam diversos aspetos da vida privada, quando não mesmo, porque analisados no seu conjunto, toda a nossa vida privada, implica o reconhecimento pela Proposta de lei em apreço da possibilidade de uma agressão tal aos direitos à privacidade, à proteção de dados e à liberdade, que não se pode senão falar de uma devassa, no sentido jurídico do termo, aparentemente legitimada pela lei mas que viola os pilares do Estado de Direito e de uma sociedade democrática.

2. Registo de interesses

Para garantia da necessária independência para o exercício de funções no SIRP, prevê a Proposta de lei a apresentação de um registo de interesses dos candidatos ao Conselho de Fiscalização do SIRP, do indigitado para o cargo de Secretário-Geral do SIRP e ainda de todos os membros do gabinete do Secretário-Geral, dirigentes e demais pessoal do SIRP, nos termos dos artigos 22.º, 41.º e 88.º da Proposta.

Na verdade estas disposições não são novas, tendo sido introduzidas em 2014, com a Lei Orgânica n.º 4/2014, de 13 de agosto, que alterou a Lei n.º 30/84, de 5 de setembro. Simplesmente, como o projeto dessa lei orgânica não foi submetido à consulta da CNPD, a Comissão pronuncia-se agora sobre o teor dessas normas,

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

considerando o impacto que as mesmas têm na privacidade das pessoas abrangidas por tal obrigação.

A informação exigida no referido registo de interesses pretende, pois, prevenir conflitos de interesses no exercício das funções a assumir no âmbito do SIRP, aqui particularmente importante dada a reduzida transparência da atividade a desenvolver, por força da natureza das funções.

Em especial, merecem nota os dados pessoais exigidos nas alíneas c) e g) do n.º 2 do artigo 22.º (para o qual remete o n.º 2 do artigo 44.º) e nas alíneas c) e g) do n.º 2 do artigo 88.º. No primeiro caso, pela abrangência da expressão "em quaisquer entidades de natureza associativa", que abarca informação reveladora de aspetos da vida privada; no segundo caso, por implicar a comunicação de informação pessoal relativa a terceiros, (cônjuge, unido de facto ou filhos), ainda que esta informação não se revista de especial sensibilidade – em causa está a participação de terceiros próximos do titular dos dados no capital de sociedades.

Sendo certo que a informação exigida é bastante extensa e, como se disse, respeita até a terceiros, admite-se que na ponderação subjacente a esta opção legislativa tenha sido levado em linha de conta a relevância da atividade a desenvolver pelos titulares de dados e, sobretudo, a dificuldade de escrutínio dessa atividade, para efeitos de controlo de um efetivo desempenho independente de funções tão impactantes na sociedade. Por essa razão, se terá reforçado o controlo *ex ante* dos conflitos de interesses.

Isto não significa que os dados pessoais dos candidatos ou indigitados para aqueles órgãos e os dirigentes e demais pessoal do SIRP devam ficar, sem mais, expostos à consulta pública.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Importa aqui analisar os diferentes planos da proteção destes dados pessoais: primeiro, a recolha da informação para ser objeto de apreciação por quem tem, nos termos da lei, especificamente competência para o efeito (*v.g.,* Deputados à Assembleia da República); segundo, a consulta por qualquer interessado da informação, que deva ser tida como pública, no contexto de um Estado democrático; terceiro, a disponibilização de informação, que a lei pode quer que seja pública, na Internet.

Se quanto ao primeiro plano, a solução legal não suscita especiais dúvidas à CNPD, já os outros dois planos merecem uma análise mais detida.

Na medida em que os candidatos ao Conselho de Fiscalização do SIRP e o indigitado para o cargo de Secretário-Geral do SIRP são, no âmbito do procedimento da sua designação, sujeitos a audição em comissões parlamentares, compreende-se que esta informação constante dos registos de interesses seja relevante para o público em geral, para efeito do pretendido escrutínio democrático. Simplesmente, importa aqui distinguir aquela informação pessoal que pode, e deve, estar disponível para consulta na Assembleia da República, da sua divulgação na Internet.

Na verdade, o artigo 103.º, n.º 2, do Regimento da Assembleia da República prevê que *todos os documentos em análise, ou já analisados, pelas comissões parlamentares, que não contenham matéria reservada, devem ser disponibilizados no portal da Assembleia na* Internet. Na medida em que os candidatos ao Conselho de Fiscalização do SIRP e o indigitado para o cargo de Secretário-Geral do SIRP são ouvidos nas comissões parlamentares, tal norma implicaria a publicitação dos respetivos registos de interesses. Esse resultado tem de estar claramente afastado nesta Proposta de Lei.

Não faz sentido que informação pessoal, com o detalhe com que é apresentada no registo de interesses, seja disponibilizada para todo o sempre em rede aberta,

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

acessível em qualquer ponto do mundo para qualquer um. Até por razões de segurança do Estado e de proteção da vida e integridade física dos titulares dos dados em causa.

Por esta razão, a CNPD entende dever ser acrescentada no artigo 22.º uma disposição a proibir a sua divulgação na Internet ou a classificar expressamente tal informação como reservada.

No plano intermédio, subsiste a questão da consulta por terceiros desta informação pessoal. Na perspetiva da CNPD, pode justificar-se a classificação de parte desta informação como reservada e portanto merecedora de uma proibição de acesso, por via de consulta, por qualquer interessado, sempre que ela configure uma intromissão na vida privada, excessiva em relação ao objetivo que com a consulta se pretende alcançar.

Quanto ao pessoal dirigente e ao restante pessoal do SIRP, é evidente que este registo de interesses não pode ser público, porque não pode ser do conhecimento público a identidade do seus titulares (ou, pelo menos, da maioria dos seus titulares).

Nestes termos, deve o legislador salvaguardar esta particular situação no artigo 88.º da Proposta.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

III. CONCLUSÕES

Com os fundamentos acima expostos, a CNPD entende que:

1. O n.º 2 do artigo 78.º da Proposta de Lei, que prevê o acesso e análise dos dados pessoais bancários e fiscais, dos dados pessoais de tráfego e de localização no âmbito das comunicações, de 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, lido em conjugação com o n.º 1 do artigo 36.º e o n.º 2 do artigo 37.º da Proposta, ~~v~~iola a Constituição da República Portuguesa (o disposto no n.º 2 do artigo 18.º, no n.º 1 e n.º 2 do artigo 26.º, n.º 1 do artigo 27.º, n.º 4 do artigo 34.º e n.º 4 do artigo 35.º), a Convenção Europeia dos Direitos do Homem (o artigo 8.º, n.ºs 1 e 2) e a Carta dos Direitos Fundamentais da União Europeia (os artigos 7.º e 8.º), porque:
   a. Prevê o acesso aos dados pessoais de tráfego e de localização fora do âmbito de um processo penal, em violação clara do n.º 4 do artigo 34.º da CRP;
   b. A submissão do acesso aos dados de tráfego e de localização a um controlo a realizar pela Comissão de Controlo Prévio, composta por juízes, não é suficientemente garantística para efeito de contornar a exigência constitucional de integração do acesso em processo criminal (por só ocorrer se antecipadamente for possível perceber que tal acesso

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

vai atingir a reserva da intimidade da vida privada, avaliação que é feita, discricionariamente, pelos próprios serviços do SIRP);

c. Possibilita o acesso a dados pessoais de localização e dados pessoais de tráfego das comunicações conservados em bases dados das operadoras por imposição de uma lei que transpõe uma Diretiva (relativa à retenção de dados) , declarada inválida pelo Tribunal de Justiça da União Europeia;

d. Permite o acesso, massivo, a uma quantidade imensa de dados pessoais sensíveis (para além dos dados de tráfego e de localização, ainda os dados bancários e os dados fiscais) relativa a quaisquer pessoas (porventura, todos os cidadãos portugueses ou todos os que se encontrem em território nacional) sem que exista qualquer tipo de indício de prática ou ligação às atividades criminosas e atentatórias da segurança nacional que se visa prevenir;

e. Em face do reduzido controlo, prévio e sucessivo, dos tratamentos dos dados pessoais sensíveis, há um evidente risco de utilização abusiva desta informação;

f. Ao deixar abertura para o tratamento de dados pessoais, com esta extensão e intensidade e com reduzidíssimo controlo, permite o conhecimento de muitos aspetos da vida privada de cada um de nós, quando não mesmo, porque analisados no seu conjunto, toda a nossa vida privada, numa agressão grosseira aos direitos à privacidade e à proteção de dados pessoais e, em consequência, ao direito à liberdade;

g. Legitima uma devassa, no sentido jurídico do termo, violadora dos valores estruturantes do Estado de Direito democrático.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

2. Em relação ao registo de interesses dos candidatos ao Conselho de Fiscalização do SIRP, do indigitado para o cargo de Secretário-Geral do SIRP e dos membros do gabinete do Secretário-Geral, dirigentes e demais pessoal do SIRP, que devem ser introduzidas alterações nos artigos 22.º e 88.º da Proposta de Lei, nos seguintes termos:
   a. No artigo 22.º, proibir a divulgação da informação pessoal constante do registo de interesses na *Internet*, ou classificá-la expressamente como reservada; e definir com precisão quais os dados pessoais que podem ser disponibilizados para consulta pública, atendendo aqui ao imperativo de proibir a sua disponibilização sempre que ela configure uma intromissão na vida privada excessiva em relação ao objetivo que com a consulta se pretende alcançar;
   b. No artigo 88.º, salvaguardar os dados pessoais do pessoal dirigente e ao restante pessoal do SIRP, sobretudo quanto àqueles cuja identidade não pode ser do conhecimento público.

Este é o nosso parecer.

Lisboa, 26 de junho de 2015

Carlos de Campos Lobo (Relator)