[redacted]

De: Rui Castelo [redacted]
Enviado: quarta-feira, 19 de abril de 2017 19:09
Para: Comissão 1ª - CACDLG XIII
Assunto: Envio de Parecer.
Anexos: 40_24_2017.pdf

Importância: Alta

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

N/Ref. 02.02
Proc. n. º 6056/2017
Of. n. 12667 19/04/2017

V. Ref.
Ofício n.º 345/1.ª – CACDLG/2017
NU:572684
05/04/2017

Assunto: Parecer sobre PJL 480/XIII/2.ª (CDS-PP) - Acesso a dados de tráfego, de localização ou outros dados conexos das comunicações por funcionários e agentes dos serviços de informações da República portuguesa.

Em resposta ao pedido de parecer acima identificado, comunico a V. Exa. o Parecer desta CNPD n.º 244/2017, de 18 de abril de 2017, cuja cópia se anexa.

*

Solicita-se a acusação da receção do presente e-mail através da opção recibo de leitura.

Com os melhores cumprimentos.
A Presidente da CNPD,
(Filipa Calvão)

rc

ASSEMBLEIA DA REPÚBLICA
Divisão de Apoio às Comissões
CACDLG
N.º Único 573720
449 20/04/2017

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

PARECER N.º 24/2017

1. Pedido

O Senhor Presidente da Comissão Parlamentar de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República solicitou à Comissão Nacional de Protecção de Dados – CNPD que se pronunciasse sobre o Projeto de Lei n.º 480/XIII-2.ª (CDS-PP) sobre o acesso a dados de tráfego, de localização ou outros dados conexos das comunicações por funcionários e agentes dos serviços de informações da República Portuguesa.

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.

2. Apreciação

O âmbito do presente parecer centra-se na apreciação da matéria relativa ao tratamento de dados pessoais. Como tal só o tratamento de dados reportados a pessoas identificadas ou identificáveis constitui matéria sujeita ao escrutínio da CNPD, posto que apenas esses são considerados "dados pessoais", na aceção do artigo 3.º, alínea *a*), da LPDP.

Visa-se, com o presente projeto de lei, a alteração da Lei n.º 30/84, de 5 de setembro, sucessivamente alterada, em último, pela Lei Orgânica n.º 4/2014, de 13 de agosto (Lei-Quadro do Sistema de Informações da República Portuguesa), bem como a alteração à Lei n.º 62/2013, de 26 de Agosto, retificada pela Declaração de Retificação n.º 42/2013, de 24 de outubro, e alterada pela Lei n.º 40-A/2016, de 22 de dezembro (Lei da Organização do Sistema Judiciário).

- **Notas prévias**

1. Uma vez que as alterações propostas para a Lei n.º 62/2013, de 26 de agosto, são meramente instrumentais e acessórias daquelas propostas para a Lei n.º 30/84, de 5 de setembro, a análise do presente parecer deter-se-á, com maior detalhe, nestas últimas, associando-lhe os comentários pertinentes sobre as primeiras, sempre que se justifique.
2. Quer as alterações propostas, quer os aditamentos avançados no projeto de lei, referentes à Lei n.º 30/84, de 5 de setembro, têm como fito principal permitir aos serviços de informações o acesso a informações bancárias e fiscais, bem com a dados de tráfego, de localização ou outros dados conexos das comunicações por funcionários e agentes dos serviços de informações da República Portuguesa (doravante SIRP). Este propósito consubstancia-se em novas disposições legais cuja motivação se prende com a resposta às objeções levantadas pelo Tribunal Constitucional (doravante TC), no Acórdão n.º 403/2015, de 27 de agosto[1], que se debruçou, a requerimento do Senhor Presidente da República, sobre a constitucionalidade do Decreto n.º 426/XII da Assembleia da República, que «*Aprova o Regime Jurídico do Sistema de Informações da República Portuguesa*», tendo os juízes daquele tribunal concluído pela inconstitucionalidade das alterações então propugnadas.
3. Na altura, o TC delimitou o objeto da fiscalização preventiva da constitucionalidade do seguinte modo: «*Assim, constitui objeto do presente pedido de fiscalização preventiva da constitucionalidade, sobre a qual cumpre emitir pronúncia, a norma, constante do n.º 2 do artigo 78.º do Decreto n.º 426/XII, nos termos da qual, os oficiais de informações do SIS e do SIED podem, para efeitos do disposto na alínea c) do n.º 2 do artigo 4.º, e no seu exclusivo âmbito, aceder a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o*

[1] Disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20150403.html.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

equipamento de telecomunicações ou a sua localização, sempre que sejam necessários, adequados e proporcionais, numa sociedade democrática, para cumprimento das atribuições legais dos serviços de informações, mediante a autorização prévia e obrigatória da Comissão de Controlo Prévio, na sequência de pedido devidamente fundamentado.».

4. Por ora, de forma sumária, dado que teremos hipótese de desenvolver os argumentos do TC no ponto seguinte, dir-se-á apenas que o TC se pronunciou pela inconstitucionalidade da norma citada, inviabilizando o acesso que agora se pretende conceder aos SIRP (ainda que circunscrito aos dados relativos às comunicações), certo sendo que agora se reformulam os preceitos que, na altura, foram alvo de fiscalização.

- **Alteração à Lei n.º 30/84, de 5 de setembro**

São propostas alterações aos art.os 2.º e 5.º, da atual Lei-Quadro do Sistema de Informações da República Portuguesa, as quais se detalham de seguida.

O novo art.º 2.º mantém a epígrafe – Finalidades – e a redação do n.º 1, mas altera o n.º 2. Este preceito repristina o n.º 2 do art.º 4.º, do Decreto n.º 426/XII da Assembleia da República [2] (doravante Decreto), praticamente *ipsis verbis*, com exceção do aditamento da fórmula «*no respeito da Constituição e da lei*», logo no início, bem como do rearranjo da disposição do conteúdo das alíneas b) e c)[3]. Assim, atribui-se aos SIRP

---

[2] Que dispunha que «*O SIRP tem como finalidade assegurar, através dos serviços de informações, 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.*».

[3] No Decreto, o art.º 4., n.º 2, ditava que «*Os serviços de informações desenvolvem atividades de recolha, processamento, exploração e difusão de informações: a)Necessárias à salvaguarda da independência nacional, dos interesses nacionais e da segurança interna e externa do Estado Português; b) Que contribuam para garantir as condições de segurança dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de Direito; e c)Adequadas a prevenir a sabotagem, a espionagem, o*

a competência para «*desenvolver, no respeito da Constituição e da lei, atividades de recolha, processamento, exploração e difusão de informações: a) Necessárias à salvaguarda da independência nacional, dos interesses nacionais e da segurança interna e externa do Estado Português; b) Que contribuam para garantir as condições de segurança dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de Direito e adequadas a prevenir a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido; c) Adequadas a prevenir a sabotagem, a espionagem, o terrorismo e sua proliferação, nos termos da lei de combate ao terrorismo [sublinhado nosso], e a criminalidade altamente organizada de natureza transnacional*». Esta arrumação da alínea c) servirá de fundamento, como veremos na análise ao novo art.º 5.º, à possibilidade de os SIRP terem acesso ao conteúdo das comunicações («*dados de base, de localização e de tráfego*» na catalogação avançada no Acórdão do TC e aqui recuperada), bem como a informação bancária e fiscal, para os efeitos que nela se enunciam.

A atual redação do art.º 5.º dispõe que «*Aos serviços de informações incumbe assegurar, no respeito da Constituição e da lei, a produção de informações necessárias à preservação da segurança interna e externa, bem como à independência e interesses nacionais e à unidade e integridade do Estado*». O que o projeto de lei parece tentar fazer é, por via de uma concretização legal mais detalhada e enquadradora de uma possível ação dos SIRP, no âmbito das suas competências, e com o pano de fundo da lei de combate ao terrorismo, caucionar o acesso à informação bancária, fiscal e das comunicações por parte dos funcionários e agentes destes serviços. Mais adiante veremos se, no entendimento da CNPD, esta tentativa de ultrapassar uma das questões levantadas pelo TC e pela própria Comissão[4] é lograda.

---

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.»

[4] Parecer n.º 51/2015, de 26 de junho, disponível em https://www.cnpd.pt/bin/decisoes/Par/40_51_2015.pdf.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

No proposto e revisto art.º 5.º vem definida a já referida nova via para acesso aos dados das comunicações por parte dos SIRP. Nos termos do n.º 1, «*Os funcionários e agentes, civis ou militares, têm acesso, mediante autorização judicial a conceder nos termos da presente lei, a informação e registos relevantes para a prossecução das suas competências, contidos em ficheiros de entidades públicas, nos termos de protocolo, ouvida a Comissão Nacional de Proteção de Dados no quadro das suas competências próprias.*». Esta redação representa uma profunda revisão do atual paradigma onde o legislador prevê que «*Os funcionários e agentes, civis ou militares, que exercem funções policiais* [sublinhado nosso] *só poderão ter acesso a dados e informações na posse dos serviços de informações desde que autorizados por despacho do competente membro do Governo, sendo proibida a sua utilização com finalidades diferentes da tutela da legalidade democrática ou da prevenção e repressão da criminalidade.*».

O mesmo se diga do que vem disposto no n.º 2 do art.º 5.º revisto pelo projeto de lei sob parecer, onde se determina que «*Os funcionários e agentes dos serviços de informações do SIS e do SIED podem, para efeitos do disposto na alínea c) do n.º 2 do artigo 2.º, e no seu exclusivo âmbito, aceder a informação bancária, a informação fiscal, a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização.*», algo que, até agora, lhes estava vedado.

a. Como nota preliminar, registamos a total falta de correspondência entre o que se permite e a quem se permite, por via de lei, no presente quadro jurídico e o que se visa permitir e a quem se visa permitir de acordo com as alterações propostas no projeto. Repare-se que a atual lei, no art.º 5.º, n.º 1, disciplina o acesso a dados e informações na posse dos serviços de informações, por parte de «*funcionários e agentes, civis ou militares, que exercem funções policiais*», no quadro das finalidades ligadas à tutela da legalidade democrática ou prevenção e repressão da criminalidade. Quer isto dizer, factualmente, que a lei permite àqueles funcionários e agentes que exercem funções policiais, nos limites das suas competências, o acesso à informação gerada e gerida pelos serviços de informações, o que pode só suceder no exercício das referidas

funções. Disciplina-se, então, o acesso de um universo de pessoas que exercem funções policiais às informações dos SIRP e não o contrário, como parece resultar do projeto de lei. Aliás, pela redação proposta, não só se opera a possibilidade de acesso, por parte dos SIRP, às informações e registos contidos em ficheiros de entidades públicas (sejam elas quais forem) que sejam relevantes para a prossecução das suas competências, como se elimina qualquer possibilidade de «*funcionários e agentes, civis ou militares, que exercem funções policiais*» poderem aceder à informação que os SIRP possam produzir no contexto das suas competências.

Admite-se que a atual formulação do art.º 5.º, sobretudo se confrontado o teor do n.º 1 e n.º 2, possa dar azo a dúvidas interpretativas quanto aos sujeitos objeto da «*autorização legal*» de acesso à informação, mas se aceitarmos como bons os princípios básicos da interpretação legística, que obrigam à leitura coordenada, encadeada e coerente dos vários preceitos que compõem um artigo, rapidamente chegaremos à conclusão de que o art.º 5.º nunca se dirigiu à possibilidade de os funcionários e agentes dos SIRP poderem aceder, gerar e gerir a informação que aí está em causa. Sem prejuízo de, no n.º 2, se prever uma cominação (pena de prisão até três anos) que, em tese, pode abarcar os funcionários e agentes do SIRP, o certo é que tal hipótese teórica apenas poderia operar na responsabilização desses funcionários e agentes por uma eventual comunicação dos dados em violação do n.º 1. Ora, uma leitura, como se disse, coordenada, encadeada e coerente do art.º 5.º parece não querer admitir sequer tal hipótese, mormente quando no art.º 25.º da Lei n.º 30/84, de 5 de setembro, vem especificamente prevista e disciplinada a matéria do acesso, por parte destes sujeitos, à informação conservada nos arquivos de dados do SIRP; ou quando, no art.º 28.º, n.º 2, se fixam os deveres de sigilo a que esses mesmos funcionários e agentes dos SIRP estão vinculados; ou, ainda, o art.º 33.º, n.º 3, que pune a violação da obrigação a que estão sujeitos os ditos elementos de, em matéria de depoimentos perante autoridades judiciais, não «*revelar factos abrangidos pelo segredo de Estado e, no tocante aos factos sobre os quais possa depor ou prestar declarações, [de] não [...] revelar as fontes de informação nem deve[rem] ser inquirido[s] sobre as mesmas, bem como sobre o resultado de análises ou sobre elementos contidos nos centros de dados ou nos arquivos.*».

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Não obstante todas as cogitações teóricas sobre a aplicação do n.º 2 do art.º 5.º da atual lei aos funcionários e agentes do SIRP, o certo é que, para lá de qualquer dúvida, com a alteração proposta, este artigo passa a aplicar-se apenas aos tratamentos de dados operados pelos SIRP. E passa a permitir, pelo seu novo n.º 2, o acesso a uma série de dados que, até aqui, não estava regulamentado, logo, não permitido, ainda que subjugado à condição de tal acesso se produzir mediante autorização do coletivo de juízes, previsto no aditado 5.º-A, e nos termos das «*atividades de recolha, processamento, exploração e difusão de informações [c)] Adequadas a prevenir a sabotagem, a espionagem, o terrorismo e sua proliferação, nos termos da lei de combate ao terrorismo, e a criminalidade altamente organizada de natureza transnacional*».

b. Diga-se, como elemento originário deste parecer, que os dados cujo tratamento agora se visa permitir aos SIRP[5] enquadram-se no conceito de dados sensíveis, tal como vem previsto no art.º 7.º, n.º 1, da LPDP, dado o seu caráter especialmente intrusivo na privacidade alheia e considerando a própria natureza da informação, relacionada com a vida privada dos titulares dos dados a quem respeitam. Este entendimento já tinha sido sufragado pelo TC, no acórdão referido, quando este cita a posição da CNPD expressa no Parecer n.º 29/98, de 16/4, ainda que naquele apenas por reporte aos dados das comunicações[6]. E, como é sabido, o tratamento deste tipo de dados goza de especial proteção por parte da lei (art.º 7.º, n.º 2, da LPDP), mas também da Constituição (art.º 35.º, n.º 3), vinculando-o a específicos requerimentos de legalidade.

---

[5] De acordo com o n.º 2 do proposto art.º 5.º, permite-se o acesso: «*a informação bancária, a informação fiscal, a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização*».

[6] Ponto 15 do Acórdão n.º 403/2015, de 27 de agosto, do TC.

Na análise ao novo n.º 2 do art.º 5.º, cumpre recuperar os argumentos do TC[7] sobre a possibilidade de os SIRP acederem a este tipo de informação, matéria constitucionalmente problemática e que o presente projeto de lei apenas visa evitar através da introdução de um controlo judicial dos processos internos de produção de informação do SIED (Serviço de Informações Estratégicas de Defesa) e do SIS (Serviço de Informações de Segurança).

Começa-se, pois, por citar as diversas passagens do acórdão onde se dilucida o entendimento unívoco do tribunal quanto à natureza dos dados ligados às comunicações que aqui estão em causa e quanto à proteção constitucional que lhes é reconhecida:

«*De modo que, na jurisprudência constitucional, as comunicações privadas, englobando o conteúdo e circunstancialismos em que as mesmas têm lugar, são reconhecidas como um meio através do qual se manifestam aspetos da vida privada da pessoa e que, por isso, caem no âmbito da proteção constitucional da respetiva reserva.*[8]*(...) Quanto ao âmbito objetivo do direito à reserva sobre a intimidade da vida privada, o Tribunal tem dito – em consonância com a doutrina acima referida – (i) que tal direito inclui, como diferentes manifestações, o direito à solidão, o direito ao anonimato e o direito à autodeterminação informativa; (ii) que o direito ao livre desenvolvimento da personalidade, como liberdade comportamental, de livre conformação e expressão da personalidade, é entre nós tratado distintamente do direito à reserva, no sentido de livre controlo da informação sobre aquilo que, em decorrência dessa liberdade de conduta, cada um faz na sua esfera privada; (iii) que a fórmula "reserva de intimidade da vida privada" não pode ser interpretada restritivamente, de modo a circunscrever a proteção constitucional à vida íntima, pois que tal implicaria deixar de cobrir todas as outras esferas da vida que devem igualmente ser resguardadas do público, como condição de salvaguarda da integridade e dignidade das pessoas; (iv) e que o facto de se recusar a equivalência entre "privacidade" e "intimidade" não impede que se não estabeleçam*

---

[7] Que vão ao encontro, em grande parte, do que a CNPD havia sublinhado no parecer já citado, mormente o que se detalhava no seu ponto 1.

[8] Ponto 12 do Acórdão citado.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

graduações entre diferentes esferas da vida privada, consoante a sua maior ou menor ligação aos atributos constitutivos da personalidade (cfr. entre outros, os Acórdãos n.ºs 306/2003, 368/2002, 355/97, 442/07 e 230/08). (...) O direito ao desenvolvimento da personalidade, na dimensão de liberdade de ação de um sujeito autónomo dotado de autodeterminação decisória, naturalmente que comporta a liberdade de comunicar. Nesta dimensão relacional, do "eu" com o "outro", o objeto de proteção é a comunicação individual, isto é, a comunicação que se destina a um recetor individual ou a um círculo de destinatários previamente determinado. A liberdade de comunicar abrange a faculdade de comunicar com segurança e confiança e o domínio e autocontrole sobre a comunicação, enquanto expressão e exteriorização da própria pessoa. Tal liberdade, enquanto refração do direito ao desenvolvimento da personalidade e da tutela da privacidade, mereceu no texto constitucional um recorte material específico, através da autonomização, no artigo 34.º, do sigilo dos meios de comunicação privada. Servindo para proteger vários bens jurídico-constitucionais, ele é hoje, como refere Gomes Canotilho, «um dos núcleos essenciais do direito à autodeterminação comunicativa, juntamente com a proteção de dados pessoais constantes de ficheiros informatizados ou manuais» (cfr. Privatização e Direitos, Liberdades e Garantias. A propósito do sigilo de correspondência no serviço de telecomunicações, in Estudos de Direitos Fundamentais, 2ª ed. pág. 162).[9] *(...) Pode falar-se assim de um «direito à autodeterminação comunicativa» que serve para defender vários bens jurídico-constitucionais, entre eles: o direito ao desenvolvimento da personalidade e o direito à reserva da intimidade da vida privada. (...) Ora, há um largo consenso na doutrina e na jurisprudência, de resto não se conhece posição contrária, no sentido de se incluir os dados de tráfego no conceito de comunicações constitucionalmente relevante para a proibição de ingerência. Quer dizer: o âmbito de proteção do artigo 34.º, n.º 4 abrange não apenas o conteúdo das telecomunicações, mas também os dados de tráfego.*[10] *(...) Por sua vez, Germano Marques da Silva e Fernando Sá afirmam que «é possível perceber que a intenção da Constituição é oferecer proteção ao tráfego de informação*

[9] Ponto 13 do Acórdão citado.

[10] Ponto 15 do Acórdão citado.

escrita, desenhada ou falada, entre dois ou mais destinatários definidos» e «essa proteção, especialmente nos modernos meios de comunicação, é ainda constitucionalmente garantida às circunstâncias em que se realizam as comunicações. Nesses termos, estão também protegidos os dados relativos aos meios de comunicação usados, à hora da sua utilização, à duração da sua utilização, ao local da sua utilização ou à identidade dos seus utilizadores» (cfr. Anotação ao artigo 34.º, in Jorge Miranda e Rui Medeiros., ob. cit., págs. 772 e 774). (...) Concluímos, pois, respondendo à primeira questão colocada pelo Requerente neste processo, que a proibição de ingerência nas comunicações, constante do artigo 34.º da CRP, abrange os dados de tráfego."».

Do que vimos de citar, adquire-se não só o caráter inquestionável da proteção constitucional conferida às comunicações, mas também o âmbito deste conceito no perímetro dessa proteção, que abrange, sem sombra de dúvida, os dados de tráfego. No quadro dessa mesma proteção constitucional, também o art.º 35.º não pode deixar de ser considerado à luz da definição legal de dados pessoais, inscrita no art.º 3.º, al. a), da LPDP, que abarca, indiscutivelmente, os dados de tráfego, entendimento já acolhido pelo Tribunal de Justiça da União Europeia, no Acórdão de 08/04/2014, Digital Rights Ireland Ltd., processos n.º C-293/12 e C-594/12[11] e no Acórdão de 21/12/2016, Tele 2, processos n.º C-203/15 e C-698/15[12].

c. A problemática em debate, tal como os juízes do TC a encararam, olhando diretamente para a questão da legalidade vigente, consistia no seguinte enunciado: «*Neste quadro legal, a atividade do SIRP está especificamente limitada por alguns princípios inscritos nos n.ºs 1 e 3 do artigo 3.º e n.º 1 do artigo 4.º da LQSIRP: (i) o princípio da constitucionalidade e da legalidade: a atividade dos serviços de informações*

---

[11] Disponível em http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d63d34ffbab785491ab755b34740570fe7.e34KaxiLc3eQc40LaxqMbN4Pax0Qe0?text=&docid=150642&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=48371.

[12] Disponível em http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=48416.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

está sujeita ao escrupuloso respeito pela Constituição e pela lei, designadamente em matéria de proteção dos direitos fundamentais das pessoas, especialmente frente à utilização de dados informatizados; (ii) o princípio da exclusividade: a atividade dos serviços está rigorosamente limitada às suas atribuições, não podendo desenvolver uma atividade de produção de informações em domínio que não lhe tenha sido concedido; (iii) o princípio da especialidade: a atividade dos serviços de informações reduz-se ao seu estrito âmbito, não podendo a sua atividade confundir-se com a atividade própria de outros organismos, como no domínio da atividade dos tribunais ou da atividade policial (cfr. Jorge Bacelar Gouveia, Os Serviços de Informações de Portugal: organização e fiscalização, in Estudos de Direito e Segurança, Almedina, 2007, pág. 181-182).»[13]. É especialmente relevante esta passagem do acórdão, dada a circunscrição teórico-prática que é delineada para a amplitude de ação dos SIRP. Donde, os princípios da constitucionalidade e da legalidade surgem como limitadores de uma atuação que ultrapasse a Constituição e a lei; o princípio da exclusividade impede os SIRP de extravasarem as suas atribuições, ainda no caso de se encontrarem a desempenhar as suas funções de produtores de informação; finalmente, o princípio da especialidade manda que os SIRP se não imiscuam «[n]*a atividade própria de outros organismos, como no domínio da atividade dos tribunais ou da atividade policial*». Esta separação resultava não apenas de uma artificial estanquicidade *ope legis*, mas antes, «[e para] *além de fatores históricos, de princípios e valores eminentes da nossa ordem jurídica.*»

Esta tripla limitação foi entendida pelo TC como sendo violada pelo Decreto então sob o seu escrutínio, pois 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 de controlo que estabelece, colocam o acesso aos dados de tráfego fora do* [seu] *âmbito*»[14] porque pertencentes ao da investigação criminal. Ao habilitar os SIRP com a possibilidade legal de acesso àquelas comunicações (dados pessoais, relembre-se), o legislador desrespeitava as barreiras constitucionais que balizavam a restrição

[13] Ponto 7 do Acórdão citado.

[14] Ponto 19 do Acórdão do TC citado.

dos direitos fundamentais dos visados, tal como previstas no n.º 4 do art.º 34.º da CRP, que só permite a ingerência nas comunicações «[n]*os casos previstos na lei em matéria de processo criminal*».

De forma eloquente, o TC foi perentório na delimitação dessas barreiras, esclarecendo que «*Ao definir o campo de incidência da lei restritiva do direito à inviolabilidade das comunicações pela "matéria de processo criminal" a Constituição ponderou e tomou posição (em parte) sobre o conflito entre os bens jurídicos protegidos por aquele direito fundamental e os valores comunitários, especialmente os da segurança, a cuja realização se dirige o processo penal. Não obstante as restrições legais ao direito à inviolabilidade das comunicações que o legislador está autorizado a estabelecer deverem obedecer à ponderação do princípio da proporcionalidade, a preferência abstrata pelo valor da segurança em prejuízo da privacidade das comunicações só pode valer em matéria de processo penal. É que a não inclusão de outras matérias do âmbito da restrição do direito à inviolabilidade das comunicações, não é contrária ao plano ordenador do sistema jurídico-constitucional. Ainda que se pudesse considerar, em abstrato, que há outras matérias em que o valor da segurança sobreleva os valores próprios do direito à inviolabilidade das comunicações, a falta de cobertura normativa da restrição em matérias extraprocessuais não frustra as intenções ordenadoras do atual sistema, porque há razões político-jurídicas que estão na base da abstenção do legislador constitucional*"»[15]. E diz mais: «*Nada autoriza, pois, a admitir uma eventual extensão do âmbito da ressalva final do n.º 4 do artigo 34.º - para a qual, aliás, o intérprete, neste contexto concreto, não dispõe de instrumentos metodológicos adequados*», como que clarificando a perenidade de uma alteração constitucional, embora não o prescrevendo, como meio único de promoção de uma alteração de paradigma.

O legislador, através deste projeto de lei, limita-se a tentar, por via de um rearranjo do inconstitucional Decreto n.º 426/XII da Assembleia da República, uma resposta paliativa aos obstáculos estruturais que o TC identificou.

---

[15] Ponto 17 do Acórdão do TC citado.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Vejamos, ao recuperar o teor do art.º 4.º do referido Decreto (agora art.º 2.º, ainda que com alterações de pormenor já citadas), o legislador nada mais faz do que insistir numa formulação que a CNPD já tinha criticado por «*não se alcança*[r] *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 1 do artigo 4.º da atual lei] com a previsão do carácter exclusivo dos órgãos e serviços do SIRP de tais funções e atividades [cf. artigo 6.º da Proposta]*».

Depois, o novo art.º 5.º em nada modifica a questão constitucional dos limites de acesso à informação por parte destes serviços, já que o art.º 34.º, n.º 4, da CRP, mantém-se inalterado, como inalterada se mantém a prescrição de que a ingerência nas comunicações apenas se admite «[n]*os casos previstos na lei em matéria de processo criminal*». Se assim é, e se se mantém, ainda, a natureza dos SIRP e as suas atribuições, como pode admitir-se que estes passem a ter acesso a dados para os quais a própria Constituição determina uma condição que os exclui automaticamente dessa possibilidade?

d. Note-se que o projeto de lei não mexe, e adequadamente, julgamos, na natureza dos SIRP, não ultrapassando barreiras de competências e atribuições perfeitamente definidas e estabilizadas na ordem jurídica nacional. O que faz, para obviar à restrição constitucional, é, porém, mais preocupante.

Com efeito, o art.º 5.º, n.º 1, lido conjuntamente com o novo art.º 5.º-A, parece condicionar o acesso «*a informação e registos relevantes para a prossecução das suas competências, contidos em ficheiros de entidades públicas*» a um controlo judicial de alto nível, já que se exige autorização do «*coletivo de juízes da secção especial para autorização de acesso a informação e a dados do Supremo Tribunal de Justiça,* [que intervém] *a requerimento do procurador-geral-adjunto junto da mesma secção*[16]», todos provindos da secção em matéria penal do STJ. Contudo, não se compreende como

[16] Esta secção é criada pelo art.º 6.º do projeto, por via da alteração do art.º 47.º da Lei n.º 62/2013, de 26 de agosto.

pode tal controlo ser operado quando a regulamentação do procedimento para o mesmo inexiste.

Está previsto, de facto, no art.º 5.º-B, também aditado pelo projeto, um procedimento delineado com algum detalhe, mas que apenas serve para o acesso à informação contida no n.º 2 do art.º 5.º do projeto, ou seja, somente para os dados das comunicações, informação bancária e fiscal.

Sem prejuízo da intervenção da CNPD, em momento prévio ao do estabelecimento dos protocolos que permitirão esse acesso, a inexistência de um procedimento claro e tipificado, numa matéria que tem grave e longo alcance nos direitos fundamentais dos cidadãos, descurando-se o estabelecimento de questões básicas, como o prazo de conservação da informação, constitui um óbice muito considerável à legalidade e constitucionalidade da solução gizada. E não se diga, sequer, que o n.º 3 do art.º 5.º pode servir como atenuante, já que aí se prevê que a autorização do n.º 1 só deverá ser concedida «*quando não exista outro meio que permita a salvaguarda eficaz e atempada dos bens jurídicos a proteger e houver razões para crer que o acesso aos dados solicitados é indispensável, adequada*[o] *e proporcional para prevenir a prática dos crimes previstos na alínea c) do n.º 2 do artigo 5.º* [esta referência deverá ter-se por mero lapso, já que é claramente o art.º 2.º que aqui está em causa]». O conteúdo deste inciso não responde aos critérios fundamentais de certeza e segurança jurídica a que, por exemplo, o TJUE já se referiu em matéria de «*condições materiais e processuais*»[17] indispensáveis.

No que concerne ao n.º 2 do art.º 5.º do projeto de lei, permite-se aos agentes do SIS e do SIED, «*para efeitos do disposto na alínea c) do n.º 2 do artigo 2.º, e no seu exclusivo âmbito, aceder a informação bancária, a informação fiscal, a dados* [de comunicações]». Aqui se demonstra que a alínea c) do n.º 2 do art.º 2.º, do projeto, passa a servir como "fundamento de legitimidade" de acesso a estes dados por parte do SIRP. Não se vislumbra, porém, como pode tal acesso processar-se de acordo com a lei e a

---

[17] Parágrafo 60 e 61 do Acórdão de 08/04/2014, Digital Rights Ireland Ltd., processos n.º C-293/12 e C-594/12.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Constituição, mesmo admitindo que o projeto de lei viesse a ser aprovado, tal como está. Como já se referiu, torna-se impraticável «*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*» com estas novas prerrogativas de atuação. É que, mantendo-se essa "incompatibilidade" e correspondendo uma tal atuação dos SIRP, ainda que no quadro legal veiculado pelo projeto, a funções matricialmente policiais [18] (como se verá seguidamente) facilmente se conclui pela manutenção da impossibilidade de aqueles serviços as poderem levar a cabo.

Observe-se que a alínea c) do n.º 2 do art.º 2.º, remete, desde logo, para um quadro legal (lei de combate ao terrorismo[19] e a criminalidade altamente organizada[20]) que conflitua com competências próprias de autoridades policiais e volta a colocar em xeque a compatibilização das atribuições dos SIRP com as suas suprarreferidas "incompatibilidades".

Ainda que o projeto de lei pudesse ter como fito afastar o regime de acesso a estas informações do âmbito de uma atuação geneticamente policial, esse desígnio, apesar de eventualmente salvaguardar o acesso dos SIRP àquela informação, logo acabaria por perecer atenta a limitação constitucional que só cauciona a ingerência nas comunicações no âmbito de um processo criminal. É, então, evidente, a contradição nos termos gerados por esta solução. Ademais, por muito que aceitássemos uma distinção evidente entre prevenção criminal e processo criminal, por forma a admitir a ingerência nas comunicações por parte dos SIRP, no âmbito da sua atividade operacional (sempre ligada à primeira), tal diferenciação apenas serviria para confirmar a inadmissibilidade da dita ingerência, porque aquela é, reafirma-se, estranha ao processo criminal, este sim, espaço único e restrito da limitação legítima do direito fundamental previsto no art.º 34.º da CRP.

---

[18] Veja-se, a este título, o que decorre do entendimento do TC, no ponto 19 do acórdão citado.

[19] Lei n.º 52/2003, de 22 de Agosto, sucessivamente alterada, em último pela Lei n.º 60/2015, de 24 de junho.

[20] Alínea m) do artigo 1.º do Código do Processo Penal.

Ora, a intervenção provocada de um coletivo de juízes e de um procurador-geral-adjunto, no seio de «*uma secção especial para autorização de acesso a informação e a dados*» (como inscrito no proposto art.º 47.º, n.º 2, da Lei n.º 62/2013, de 26 de agosto[21]) vem criar ainda maior confusão naquilo que se pretende vir a ser o novo enquadramento legal de acesso a estes dados por parte dos SIRP. Compreende-se que o projeto tente, com esta novidade, criar um novo espaço de legalidade formal no controlo do acesso a estes dados. Contudo, a intermediação de um tribunal, ainda que superior, coloca dois desafios de difícil compatibilização. Por um lado, judicializando o controlo do acesso aos dados confere-se ao procedimento uma natureza judicial até aqui desconhecida, o que claramente pretende responder a uma das objeções do TC, ligada não só ao controlo do acesso à informação, mas também ao exercício dos direitos dos sujeitos/arguidos envolvidos. Se essa judicialização pode traduzir uma preocupação louvável de controlo independente e qualificado dos acessos pretendidos, ela torna ainda mais patente, por outro lado, a insuficiência procedimental regulamentada no projeto. Isto porque é umbilical a ligação entre as garantias constitucionais do arguido e a existência de um processo criminal onde ele possa exercer os seus direitos fundamentais, mormente no contexto do acesso a dados de comunicações. Garantias e direitos esses que são completamente obliterados pelo procedimento inscrito no art.º 5.º, n.º 2. Ao contrário do processo penal, que tem natureza pública[22], este procedimento, previsto pelo projeto, está coberto pelo regime do segredo de Estado (art.º 5.º-B, n.º 6). Em nenhum momento se prevê a possibilidade de os titulares dos dados, suspeitos ou arguidos, poderem exercer qualquer direito de defesa, acesso ou apagamento dos dados tratados pelos SIRP, ao arrepio do art.º 32.º e 35.º, n.º 1, da CRP. E não é, seguramente, por se introduzir a intermediação de um coletivo de juízes que se estabelece a natureza

---

[21] Note-se que a redação proposta para este novo n.º 2 do art. 47.º que prevê que, *Dentro da secção em matéria penal, funciona uma secção especial para a autorização de acesso a informação e a dados*, não é adequada, pois, ao não delimitar o tipo de informação ou o tipo de acesso que tem em vista, parece abarcar todo e qualquer acesso a informação e a dados por qualquer terceiro – o que afastaria as competências de entidades administrativas como a Comissão de Acesso aos Documentos Administrativos ou a própria CNPD.

[22] Art.º 86.º, n.º 1, do CPP.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

criminal do processo. Mas ainda que fosse, um tal processo não poderia dispensar as mais elementares garantias de defesa dos arguidos, nem se admitiria que por ele se concedesse a qualquer organismo, serviço ou entidade, competências despidas da necessária cobertura legal.

Em suma, o que este projeto de lei parece tentar lograr é conferir natureza criminal ao processo de acesso à informação bancária, fiscal e dados de comunicações, para que esse acesso se constitua como constitucionalmente aceitável e, ao mesmo tempo, retirar essa natureza criminal para que se mantenham prerrogativas de atuação compreensíveis, dentro das fronteiras de atribuições dos SIRP e sujeitas à sua reconhecida especificidade, como é disso exemplo o recurso ao segredo de Estado, mas que sincronizadamente se constituem como inadmissíveis no quadro do acesso e utilização dos dados de comunicações dos visados, a quem não pode deixar de se reconhecer um conjunto de garantias e direitos constitucionalmente previstos.

Esta natureza híbrida do processo acaba por negar esses mesmos direitos constitucionalmente consagrados aos visados pela produção de informações/investigação dos SIRP, bem como conferir atribuições ilegais a estes serviços, o que, em qualquer dos casos, se torna inadmissível.

- **Desproteção do direito fundamental à proteção de dados pessoais em particular**

a. Mantêm-se, com particular acuidade, as questões suscitadas pela CNPD, no parecer já citado e que respeitam à desproporcionalidade do acesso aos dados de tráfego e aos dados de localização, mas também aos restantes dados sensíveis como a informação bancária e fiscal, pelo que se têm por reproduzidas as reservas constantes das alíneas b) e c) do ponto 1.

b. Numa análise centrada nos art.º 5.º e 5.º-A, dir-se-á que, em comum, nenhum dos preceitos define critérios precisos e objetivos que permitam conexionar indícios com suspeitos concretos da prática de uma infração criminal, tal como o TJUE já reclamou

repetidamente[23] e a CNPD sublinhou no seu parecer de 2015. Igualmente ignorados são os direitos de acesso dos titulares dos dados à informação, sendo que apenas se admite que por via da decisão do coletivo de juízes se cancelem quaisquer procedimentos em curso, sem que se perceba como podem esses juízes inteirar-se da existência de procedimentos anómalos ou ilegais para lá do momento da concessão da autorização prevista no art.º 5.º (e 5.º-B). Ainda neste âmbito, é sintomático que apenas o Secretário-Geral dos SIRP possa ordenar a destruição das informações recolhidas, ainda que «*mediante a autorização prevista no presente artigo,* [e unicamente quando] *não tenham relação com o objeto ou finalidades da mesma*».

c. Apesar de se reconhecer a relevância das preocupações tecnológicas inscritas no art.º 5.º-C, não se compreende porque é que estas se limitam a abarcar os dados previstos no art.º 5.º, n.º 2, já que a informação recolhida nos termos do n.º 1 desse artigo pode revestir a mesma sensibilidade dos primeiros. Neste artigo, no seu n.º 4, insiste-se na alocação do controlo permanente «*da transmissão, o tratamento, a manutenção e a destruição das informações e dados*» previstos na lei à Comissão de Fiscalização de Dados do SIRP, ainda que se remeta para legislação especial outras regras que influam nessas operações que são, todas elas, quando envolvam dados pessoais, tratamentos de dados, na aceção do art.º 3.º, al. b), da LPDP.

d. Finalmente, cabe ainda relembrar a especial acuidade do Acórdão de 21/12/2016, Tele 2, processos n.º C-203/15 e C-698/15, no que tange à Lei n.º 32/2008, de 17 de julho (que transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março) que é, no fundo, a lei «*que regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes*».

---

[23] Acórdão de 08/04/2014, Digital Rights Ireland Ltd., processos n.º C-293/12 e C-594/12 e no Acórdão de 21/12/16, Tele 2, processos n.º C-203/15 e C-698/15.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Tendo sido chamado a interpretar legislação nacional de Estados-Membros da UE (Suécia e Reino Unido) que transpunha a Diretiva 2006/24/CE, implicando a recolha massiva, indiscriminada de dados das comunicações e obrigando à sua conservação por um período compreendido entre 6 meses e dois anos (tal como previsto no seu art.º 5.º e 6.º), o TJUE veio concluir que «*Uma regulamentação deste tipo não exige nenhuma relação entre os dados cuja conservação se encontra prevista e uma ameaça para a segurança pública. Nomeadamente, não está limitada a uma conservação que tenha por objeto dados relativos a um período temporal e/ou uma zona geográfica e/ou a um círculo de pessoas que possam estar envolvidas de uma maneira ou de outra numa infração grave, nem a pessoas que, por outros motivos, mediante a conservação dos seus dados, podiam contribuir para a luta contra a criminalidade...*»[24].

Pela completa desproporcionalidade da recolha e retenção de dados em tais termos, esclareceu que «*O artigo 15.°, n.° 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e de todos os dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica*».

Donde, para efeitos de legislação nacional, «*O artigo 15.°, n.° 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz dos artigos 7.°, 8.° e 11.° bem como do artigo 52.°, n.° 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da*

[24] Parágrafo 106 do Acórdão de 21/12/16, Tele 2, processos n.º C-203/15 e C-698/15.

luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União.»

Se dúvidas se mantivessem, à luz das conclusões do acórdão, que acabámos de transcrever, sobre a "invalidade" da legislação nacional que procedeu à transposição da Diretiva 2006/24/CE, sublinhe-se o que o TJUE veio considerar como intolerável, especificamente tratando da derrogação permitida pelo art.º 15.º, n.º 1, da Diretiva 2002/58/CE, na redação que lhe foi dada pela diretiva relativa à retenção de dados: «*tal disposição não pode justificar que a exceção a essa obrigação de princípio* [de garantir a confidencialidade das comunicações e dos correspondentes dados de tráfego] *e, em especial, a proibição de armazenar esses dados, prevista no artigo 5.º desta diretiva, se converta na regra*».

E é isto que a Lei n.º 32/2008, de 17 de julho, justamente permite, através do seu art.º 4.º, obrigando, como regra, à recolha indiscriminada de dados das comunicações, com o pretexto dos fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes. É patente a desproporcionalidade desta medida, o que, como já tinha sido sinalizado pela CNPD, no seu parecer de 2015, faz perigar não só a "validade" da lei que transpõe a diretiva, mas também, e por arrasto, compromete a própria constitucionalidade da mesma, já 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.*». E, portanto, só pode concluir-se que a Lei n.º 32/3008 viola 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).

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Nesta senda, prevê-se, a curto prazo, e tendo em conta os acórdãos que vão sendo conhecidos sobre esta matéria[25], a inevitável pronúncia por parte do TC sobre a constitucionalidade desta lei, que nos parece claramente comprometida e, portanto, insuficiente para legitimar a recolha de dados nos termos em que tal operação nela vem prevista.

3. Conclusão

Com os fundamentos acima expostos, a CNPD entende que o projeto de lei em análise não vem obviar aos obstáculos constitucionais assinalados pelo Tribunal Constitucional, no Acórdão n.º 403/2015, de 27 de agosto. E conclui desta forma, uma vez que as soluções propostas visam, por um lado, conferir aos SIRP atribuições quase-policiais, manifestamente incompatíveis com o art.º 4.º, nº 1, da Lei n.º 30/84, de 5 de setembro, e, por outro, judicializar o processo de aquisição e acesso de informações, enquadrando-o num procedimento de autorização na dependência da secção penal do Supremo Tribunal de Justiça, pretendendo, com isso, insinuar uma natureza criminal (ou garantística) comparável à do processo penal, para, assim, legitimar o acesso a dados relativos às comunicações, o que se revela manifestamente insuficiente quando comparado com as garantias que o processo penal atribui ao arguido, num todo coerente, materialmente robusto e procedimentalmente tipificado, estranho ao regime ora proposto.

Mantêm-se, por inteiro, as reservas elencadas no Parecer da CNPD n.º 51/2015, de 26 de junho, acrescentando-se a firme convicção de que, em face da jurisprudência do Tribunal de Justiça da União Europeia a Lei n.º 32/2008, de 17 de julho, ao transpor a Diretiva 2006/24/CE, já invalidada por aquele tribunal, e ao permitir uma recolha indiferenciada, permanente e persistente de todos os dados previstos no seu art.º 4.º, de todas as pessoas, indiscriminadamente e por um período de tempo, também ele, despojado de qualquer consideração fáctica relacionada com o caso concreto, viola a

[25] Ac. Tribunal da Relação de Évora de 19-05-2015; Ac. Tribunal da Relação de Lisboa de 03-05-2016 e Ac. Tribunal da Relação de Lisboa de 22-06-2016.

Constituição da República Portuguesa a Convenção Europeia dos Direitos do Homem e a Carta dos Direitos Fundamentais da União Europeia.

Este é o parecer da CNPD.

Lisboa, 18 de abril de 2017

Filipa Calvão (Presidente)