COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

# PARECER N.º 38/2017

## I. Pedido

O Senhor Presidente da Comissão dos Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República solicitou à Comissão Nacional de Proteção de Dados (CNPD) parecer sobre a Proposta de Lei n.º 79/XIII/2.ª (GOV) *que aprova o regime especial de acesso a dados de base e a dados de tráfego de comunicações eletrónicas pelo Sistema 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, alterada pela Lei n.º 103/2015, de 24 de agosto – 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

O presente parecer cinge-se às matérias relativas à proteção de dados pessoais, considerando as competências legais da CNPD, 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 (doravante, Lei da Privacidade nas Comunicações Eletrónicas).

Atento o objeto da Proposta, delimitado no artigo 1.º, percebe-se que todas as disposições são relativas a tratamentos de dados pessoais já que os dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas são informações relativas a pessoas singulares que estabelecem ou intervêm em tais comunicações (cf. alíneas a) e b) do artigo 3.º da LPDP).

Considerando ainda o teor da Proposta, em especial a complexidade técnica da sua análise e o especial impacto que o regime nela previsto tem nos direitos fundamentais dos cidadãos, a CNPD não pode deixar de assinalar que o tempo que foi delimitado para a emissão do presente parecer é substancialmente exíguo (inferior a uma semana, se se considerar que o parecer é emitido para que os argumentos e recomendações nele vertidos sejam lidos e ponderados pelos deputados à Assembleia da República), o que condiciona todo o processo de análise do

regime e da fundamentação e argumentação a apresentar, prejudicando o exercício das funções consultivas da CNPD, bem como a utilidade efetiva do mesmo.

A CNPD lamenta que este procedimento legislativo não tenha sido estruturado de modo a assegurar às entidades que, nos termos da lei, devem ser ouvidas o tempo de análise e ponderação que a matéria, pela sua importância, em virtude da sua direta associação à dignidade da pessoa humana e aos pilares do Estado de Direito, mereceria.

## 1. Nota prévia

Importa antes do mais notar que o objeto deste diploma, tal como decorre expressa e claramente do n.º 1 do artigo 1.º, é a regulação do acesso pelo SIRP aos dados de comunicações eletrónicas que os prestadores de serviços de comunicações eletrónicas conservam («previamente armazenados») nos termos de outros diplomas legais – a saber, a Lei da Privacidade nas Comunicações Eletrónicas, e a Lei n.º 32/2008, de 17 de julho, que estabelece um regime de retenção de dados[1].

Apesar desta delimitação do objeto, o n.º 4 do artigo 1.º refere-se à «conservação e transmissão pelos prestadores de serviços de comunicações eletrónicas dos dados [...]», quando em rigor este diploma, não regula, nem pode querer regular, a conservação dos dados pelos prestadores de tais serviços, mas apenas a legitimidade para a sua transmissão.

Nessa medida, a CNPD recomenda que a expressão *conservação* seja eliminada do referido preceito[2].

---

[1] Recorda-se, a este propósito, que a CNPD considera que a Lei n.º 32/2008 contraria a Constituição e o Direito da União Europeia, com os argumentos que ficaram expostos na Deliberação n.º 641/2017, enviada à Assembleia da República e disponível em https://www.cnpd.pt/bin/decisoes/Delib/20_641_2017.pdf

[2] A título de nota prévia, destaca-se a afirmação, na exposição de motivos, de que, *tendo presente a limitação constitucional das interceções de comunicações ao domínio do processo penal, nos termos do n.º 4 do artigo 34.º da Constituição da República Portuguesa (CRP), o SIRP é objeto do escrutínio por uma Comissão de Proteção de Dados com competência exclusiva e especializada de controlo dos direitos de autodeterminação informacional os cidadãos perante o Sistema nos termos do artigo 35.º da CRP.*

O aparente esforço de equiparação de funções e poderes do órgão administrativo de controlo que esta lei, tal como a ainda vigente, prevê – a Comissão de Fiscalização de Dados do SIRP – às funções e poderes do órgão administrativo que em geral garante o direito à proteção dos dados pessoais – a Comissão Nacional de Protecção de Dados –, revelada logo na circunstância curiosa de aquela Comissão vir aqui identificada, que não no articulado,

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

## 2. Acesso a dados pessoais de comunicação: o impacto na privacidade dos cidadãos

Os dados cujo acesso a presente Proposta de Lei vem regular são dados obtidos no âmbito da prestação de serviços de comunicações eletrónicas e, como tais, dados de comunicações.

Enquanto informação relativa a pessoas singulares, identificadas – nome do cliente ou do utilizador do equipamento de comunicação – ou identificáveis – por referência ao número de identificação do equipamento móvel (IMEI), ao número do cartão (IMSI) ou do endereço IP (*Internet Protocol*) –, tais dados são dados pessoais, nos termos da alínea a) do artigo 3.º da LPDP[3], e que integram a categoria de dados sensíveis especialmente protegida pelo artigo 7.º da LPDP, em concretização dos direitos fundamentais nos artigos 26.º, n.º 1, e 35.º, em especial o n.º 3, da Constituição da República Portuguesa (CRP). São ainda especialmente protegidos pelo n.º 4 do artigo 34.º da CRP. A mesma dimensão fundamental vem consagrada nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (doravante, Carta) e no artigo 8.º da Convenção Europeia dos Direitos do Homem (doravante, CEDH).

Na verdade, o tratamento desta informação relativa às pessoas permite conhecer com grande pormenor e extensão a sua vida privada. É que os dados de comunicação abrangem: chamadas vocais, correio vocal, teleconferência, serviços suplementares, incluindo reencaminhamento e transferências de chamadas, serviços de mensagens e multimédia, incluindo mensagens curtas (SMS), serviços de mensagens melhorados (EMS), serviços de mensagens multimédia (MMS), o código de identificação do utilizador (*user ID* – código único

---

como *Comissão de Proteção de Dados*, fracassa quando se comparam os poderes de tais organismos. E a diferença evidente revela-se mesmo no próprio texto da exposição de motivos, quando lhe imputa a competência de *controlo dos direitos* de autodeterminação informacional dos cidadãos perante o Sistema: é que a CNPD tem por função *controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei* (cf. n.º 1 do artigo 22.º da LPDP), em pleno cumprimento da função constitucionalmente imposta de *garantir a proteção dos dados pessoais* (cf. n.º 2 do artigo 35.º da CRP). Já de acordo com o teor da exposição, a *Comissão de Proteção de Dados* do SIRP visa *controlar os direitos*, em vez de controlar a utilização que dos dados pessoais é feita pelo SIRP e garantir a sua proteção, assim reforçando a conclusão que tal Comissão não está, pela sua natureza, apta a contornar os limites constitucionais ao acesso a dados pessoais relativos a comunicações.

[3] Reconhece-o expressamente o Tribunal de Justiça da União Europeia (TJUE) no acórdão de 08.04.2014, *Digital Rights Ireland Ltd.*, processos n.º C-293/12 e C-594/12, de 21.12.2016, e no acórdão *Tele 2*, processos n.º C-203/15 e C-698/15.

atribuído às pessoas quando estas se tornam assinantes ou se inscrevem num serviço de acesso ou comunicação pela Internet), identificador da célula (*cell ID* – identificação da célula de origem e destino de uma comunicação numa rede móvel). E abrangem também o nome e o endereço do assinante do serviço, o IMEI e o IMSI (para identificação do equipamento de comunicação) do emitente e do destinatário da comunicação, a linha de assinante digital (DSL), bem como os dados necessários para identificar a localização do equipamento e da célula no início da comunicação. E ainda abarcam os dados relativos à identificação da data, hora e duração da comunicação[4].

Importa também dizer que as comunicações englobam ainda os acessos aos sítios na Internet, por também tais operações implicarem comunicação eletrónica, para além dos acessos a partir das aplicações (*apps*) e outros carregamentos e atualizações de informação que os equipamentos vão fazendo automaticamente nas redes de comunicação eletrónica, sem exigir da parte do utilizador uma intervenção positiva e direta. Em suma, as comunicações há muito deixaram de se limitar à carta e à chamada de telefone fixo[5].

É bom de ver que toda esta informação revela uma ampla dimensão da vida de cada um, ao longo do dia, todos os dias.

Assim, o tratamento destes dados permite identificar quem faz ou recebe chamadas (mesmo as falhadas), quem envia ou recebe SMS, MMS, correio eletrónico, quem acede à Internet e a que sítios na Internet, portanto permitindo conhecer aspetos da vida privada e familiar das pessoas: onde se encontram ou estiveram (o que é evidente quando transportem o telemóvel ligado), com que regularidade estabelecem os contactos, que sítios da Internet consultam, etc.

Se nas sociedades democráticas a proteção das comunicações já era assegurada numa fase em que elas não representavam um meio permanente e generalizado de interação (não eram

---

[4] Cf. Acórdãos do TJUE *Digital Rights Ireland Ltd.* e *Tele 2.*

[5] Note-se que mesmo a jurisprudência nacional está ainda presa, aqui e além, a uma visão tradicional das comunicações eletrónicas. Exemplo disso é a passagem do acórdão n.º 403/2015 do Tribunal Constitucional, no ponto 13, onde se lê que a proteção constitucional do n.º 4 do artigo 34.º incide sobre o *direito à autodeterminação comunicativa*, o qual se *reporta a comunicações individuais efetivamente realizadas ou tentadas e só essas é que estão cobertas pelo sigilo das comunicações*. Esta afirmação parece assentar num conceito de comunicações que não tem correspondência no atual quadro jurídico nacional e europeu e na realidade das comunicações digitais, supondo que as comunicações individuais são as efetivamente realizadas ou tentadas, quando em rigor as comunicações individuais abrangem ainda todos os "push" de informação.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

um "instrumento de vida"), por maioria de razão todas estas comunicações que integram, praticamente em cada momento, o nosso quotidiano e que, por isso, o revelam nas suas diferentes dimensões, são – têm de ser – protegidas na atualidade.

Neste ponto, reproduz-se a elucidativa lição do Tribunal Constitucional no acórdão n.º 403/2015:

> «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 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.»

Assim, quando consideramos a tutela prevista pelo artigo 7.º da Carta, pelo artigo 8.º da CEDH e pelos artigos 26.º, 34.º e 35.º da CRP, esta tem de ser assegurada, segundo uma leitura atualista, cobrindo todas as realidades de comunicação que a tecnologia hoje oferece e, portanto, protegendo as dimensões humanas fundamentais que por via dos tratamentos dos dados pessoais são atingidas.

Em especial, a proibição de ingerência nas comunicações constante do n.º 4 do artigo 34.º da CRP não pode deixar de ser lida tendo em conta o impacto do tratamento de todos os dados pessoais acima elencados na vida privada e na liberdade dos cidadãos.

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, 4.ª ed., Coimbra Editora, anot. VII ao artigo 34.º, p. 543). 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 circunstâncias ou informações associadas aos meios de comunicação: os chamados dados de tráfego e de localização (neste sentido, Gomes Canotilho/ Vital Moreira, *ob. cit.,* anot. VIII ao artigo 34.º, p. 544; Germano Marques da Silva/ Fernando Sá, in Jorge Miranda/ Rui Medeiros, *Constituição Portuguesa Anotada*, I, 2.ª ed., Coimbra Editora, 2010, anot. XVI ao artigo 34.º, p. 774).

Por essa razão, não podem restar dúvidas de que os meios de comunicação abrangem não apenas os conteúdos respetivos mas também todos os dados àqueles referentes. Portanto, no atual quadro constitucional, qualquer ingerência de autoridades públicas em dados pessoais de comunicação só pode ocorrer nos casos previstos na lei em matéria de processo criminal.

### 2.1. *A exigência constitucional de processo criminal para a ingerência nos dados de comunicação*

Considerando o que se acaba de expor, não se vê como se possa admitir que os serviços do SIRP acedam a dados de comunicação.

Com efeito, como sintetizou o Tribunal Constitucional no acórdão n.º 403/2015 (ponto 7):

> «[...] 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 [Lei Quadro do SIRP]: (i) o princípio da constitucionalidade e da legalidade: a atividade dos serviços de informações está sujeita ao escrupuloso respeito pela Constituição e pela lei, designadamente em matéria de proteção dos direitos fundamentais das pessoas, especialmente frente à utilização de dados informatizados; (ii) o princípio da exclusividade: a atividade dos serviços está rigorosamente limitada às suas

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

> 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)».

Como a CNPD destacou no Parecer n.º 24/2017[6], recentemente emitido a propósito do Projeto de Lei n.º 480/XIII-2.ª (CDS-PP), é especialmente relevante esta passagem do acórdão: esta tripla limitação foi entendida pelo Tribunal como sendo violada pelo Decreto então sob o seu escrutínio, pois que «*[...] 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*»[7], porque pertencentes ao da investigação criminal.

Na verdade, o acesso aos dados previsto na presente Proposta visa a prossecução das atribuições do SIRP de produção de informações necessárias à preservação da segurança interna e externa, independência e interesses nacionais e unidade e integridade do Estado – concretizadas na Proposta, nos artigos 2.º e 3.º; todavia, não pode a lei ordinária reconhecer ao SIRP a legitimidade para aceder a dados para os quais a própria Constituição determina uma condição que os exclui automaticamente dessa possibilidade – ou seja, a investigação no âmbito de um processo criminal.

Desde logo, falta aqui aquilo que necessariamente tem de existir num processo criminal: os indícios de conduta criminosa. E não se diga que o teor literal daquele preceito constitucional não é aqui relevante ou constitui um mero formalismo suscetível de ser contornado pela criação de condições equivalentes[8]. Porque não há equivalência possível entre um procedimento de recolha de informação necessária à prevenção de crimes e um processo reativo como é o

[6] Acessível em https://www.cnpd.pt/bin/decisoes/Par/40_24_2017.pdf

[7] Ponto 19 do Acórdão do Tribunal Constitucional citado.

[8] Aliás, poder-se-ia mesmo invocar o disposto no n.º 2 do artigo 34.º da CRP, onde se admite a entrada no domicílio com base em ordem por autoridade judicial, para concluir que há uma diferença entre a exigência de que tal ingerência se dê por determinação legal em matéria de processo criminal e a exigência de ordem de autoridade judicial.

processo criminal – neste *há* indícios da prática de um crime, naquele *procuram-se* indícios da intenção de praticar certos crimes.

E como se referiu no mesmo Parecer n.º 24/2017, o Tribunal Constitucional, de forma eloquente, foi perentório na delimitação da proteção constitucional, 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"»[9].
>
> «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».

Assim, se concluindo que, por via desta Proposta, se desrespeitam as barreiras constitucionais à restrição dos direitos fundamentais dos cidadãos, tal como previstas no n.º 4 do artigo 34.º da CRP.

### *2.2. O procedimento de acesso e a sua não equivalência ao processo criminal*

A presente Proposta pretende criar um conjunto de condições e limites ao tratamento de dados pessoais a realizar pelo SIRP que possam transformar o procedimento de acesso num procedimento equivalente ao do processo criminal, procurando com isso contornar o limite autorizativo do acesso fixado no n.º 4 do artigo 34.º da CRP.

---

[9] Ponto 17 do Acórdão do TC citado.

Todavia, como se procurará demonstrar em seguida, o regime aqui proposto constitui uma resposta paliativa aos obstáculos estruturais que o Tribunal Constitucional identificou no diploma legal de 2015, tal como a CNPD já havia concluído no Parecer n.º 24/2017 sobre o outro projeto de lei entretanto submetido à sua consulta. Se não, vejamos.

Para o efeito, institucionaliza-se um procedimento de controlo prévio e de acompanhamento que compete a uma *formação das secções criminais do Supremo Tribunal de Justiça*. Tal "formação" é composta pelos presidentes das secções criminais e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções (cf. n.º 1 do artigo 4.º e artigo 7.º).

Desde logo, não é clara a natureza jurídica desta, assim denominada, "formação", embora se afigure tratar de um órgão administrativo. Ao não caracterizar a referida "formação de secções criminais", sem explicitar se a atividade da mesma corresponde ao exercício da função jurisdicional e se portanto oferece as garantias a esta associadas nos termos constitucionalmente estabelecidos, a Proposta não define com precisão as condições equivalentes às exigidas no n.º 4 do artigo 34.º da CRP.

Como a CNPD teve recentemente oportunidade de referir no Parecer n.º 24/2017, este tipo de previsão «cria ainda maior confusão naquilo que se pretende vir a ser o novo enquadramento legal de acesso a estes dados por parte do 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, [esta intermediação] coloca dois desafios de difícil compatibilização. Por um lado, [tentando judicializar] o controlo do acesso aos dados [quer-se imprimir] ao procedimento uma natureza judicial até aqui desconhecida, o que claramente pretende responder a uma das objeções do [Tribunal Constitucional], 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. [...] E não é, seguramente, por se introduzir a intermediação [de uma "formação" de juízes] que se estabelece a natureza 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.»

Na verdade, ainda que se reconheça estar este regime, por comparação com propostas e projetos de lei anteriores sobre esta matéria, mais densificado, com especificação dos requisitos do requerimento de autorização de acesso, bem como com delimitação temporal da mesma (cf. artigos 8.º, n.ºs 2 e 3, e 9.º), prevendo ainda um (aparente) controlo sucessivo, a intervenção desta "formação" não basta para assegurar os direitos fundamentais dos cidadãos que no processo criminal são reconhecidos.

No que ao controlo prévio diz respeito, chama-se a atenção para o facto de figurar como pressuposto da autorização que *a diligência seja adequada, necessária e proporcional para a obtenção de um alvo ou de um intermediário determinado, ou para obtenção de informação que seria muito difícil ou impossível de obter de outra forma ou em tempo útil* – cf. alíneas a) e b) do n.º 1 do artigo 5.º da Proposta.

Os termos vagos, por recurso a numerosos conceitos imprecisos, com que vem descrito o quadro circunstancial que pode justificar o acesso logo demonstra que a lei se limita a definir uma mera moldura normativa não densificada, conferindo um amplíssimo poder discricionário de apreciação em matéria de restrição de direitos, liberdades e garantias que reclama, por isso mesmo, padrões e limites legais bem definidos para a concretização da restrição.

Acresce não se perceber o que se pretende com o disposto no n.º 2 do artigo 5.º. A *proibição de interconexão em tempo real com as bases de dados dos operadores de telecomunicações e Internet para o acesso direto em linha aos dados requeridos* suporta a interpretação, *a contrario*, de que pode ser autorizada a interconexão em diferido. Porém, a interconexão é uma específica operação sobre dados pessoais, que não se confunde com o acesso aos dados (cf. alínea i) do artigo 3.º da LPDP), pelo que a autorização de acesso não legitima uma interconexão. De resto, nesta matéria e considerando que se pretende um acesso pontual a dados de comunicação (cf. alínea a) do n.º 2 do artigo 8.º), a autorização de interconexão teria sempre de se ter por desnecessária para a finalidade visada e excessiva, pelo impacto que teria na vida privada e familiar das pessoas visadas.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

É certo que esta Proposta vai um pouco mais longe do que os projetos de lei anteriores sobre esta matéria, ao atribuir à referida "formação" de juízes o poder de controlar o acesso aos dados, por via da previsão de um ato de validação do acesso pelo SIS e pelo SIED (cf. artigo 7.º e n.º 2 do artigo 11.º). Todavia, em nenhum preceito se explica em que termos se realiza tal validação, ou seja, à referida "formação" não são atribuídos poderes efetivos de fiscalização, tão-pouco se definem as condições do seu exercício. E o silêncio da Proposta quanto a efetivos poderes de verificação dos dados transmitidos deixa espaço para a presunção de que tal validação seja meramente formal ou automática, em nada garantindo os direitos fundamentais dos cidadãos.

Aliás, o mesmo se diga quanto aos poderes reconhecidos no n.º 3 do artigo 11.º. Este preceito atribui à "formação" das secções criminais poderes de cancelar o acesso e de ordenar a destruição dos dados, só que não explica em que circunstâncias e por que via terá tal "formação" conhecimento dos exatos termos em que o acesso está a decorrer, pelo que esta norma aparenta ser letra morta.

E, no entanto, os números seguintes do artigo 11.º preveem comunicações das decisões de cancelamento e de destruição; ou seja, prevê-se a comunicação das decisões da "formação" dos juízes, mas não se explica nem se define com base em que elementos pode a "formação" tomar tais decisões.

Poder-se-ia ainda pensar que o acompanhamento do Ministério Público, anunciado no n.º 1 do artigo 1.º da Proposta, poderia aqui servir de alguma utilidade, mas na verdade em momento algum se explicita em que consiste esse acompanhamento[10].

Com efeito, não se alcança qual é a função do Ministério Público neste procedimento, não havendo qualquer norma na Proposta que especifique o sentido e o conteúdo dessa intervenção. Apenas se prevê a comunicação ao Procurador-Geral da República (PGR) do «processo de autorização de acesso aos dados», especificando-se o dever *de dar conhecimento* ao PGR do correspondente pedido elaborado pelos diretores do Serviço de Informações de Segurança ou do Serviço de Informações Estratégicas de Defesa, da transmissão diferida dos dados e da decisão de cancelamento de acesso e de destruição dos

[10] Com exceção do disposto no artigo 12.º, quando prevê a comunicação imediata ao Procurador-Geral da República os factos indiciários de crimes – ainda que, estranhamente se limite aos previstos no artigo 3.º, deixando de fora os referidos no artigo 2.º, em especial o respeitante à criminalidade altamente organizada.

dados (n.º 2 do artigo 4.º, n.º 1 do artigo 8.º, n.º 1 do artigo 10.º e n.º 4 do artigo 11.º). Somente a propósito da previsão de dar a conhecer a decisão de cancelamento de acesso e de destruição dos dados se especifica a finalidade dessa comunicação: *para efeitos do exercício das suas competências legais*, ainda que não se indiquem quais sejam as competências legais relevantes neste contexto, por, tanto quanto se sabe, não dispor o Ministério Público nem o PGR de competências específicas em matéria de acesso aos dados pessoais contidos em bases de dados de prestadores de serviços de comunicações eletrónicas.

Não pretendendo pôr em causa a eventual relevância do papel do Ministério Público neste procedimento, não pode deixar de se estranhar a ausência de densificação da função e natureza de tal intervenção, num procedimento que se pretenderia particularmente reforçado em garantias para se poder equiparar a um processo criminal.

Nos termos em que vem descrita, a intervenção do Ministério Público no procedimento, se é que de intervenção se pode em rigor falar, parece somente criar uma aparência de garantia dos direitos dos cidadãos e da legalidade do procedimento, a qual não se encontra minimamente consubstanciada no presente regime nem, por remissão, noutros regimes legais.

Mesmo a garantia dos direitos de acesso e de retificação dos dados, previstos no n.º 1 do artigo 35.º da CRP, aqui concretizada por via da Comissão de Fiscalização de Dados do SIRP, está muito enfraquecida, por comparação com o regime geral nos processos de investigação criminal, desde logo por força da intensidade dos poderes desta Comissão sobre o SIRP. De facto, não se impõe aos Diretores do SIS e SIED um dever de colaboração e de prestação de todas as informações que lhes forem solicitadas (como sucede, por exemplo, no artigo 24.º, n.º 1, da LPDP), mas antes a mera prestação de um *especial apoio*, não estando por isso afastado que a natureza secreta da atividade do SIRP justifique a negação da prestação de qualquer informação.

Em suma, a falta de previsão de garantias efetivas do respeito pelos direitos fundamentais dos cidadãos, inquina este regime, não sendo o mesmo suficiente para cumprir as exigências constitucionais à ingerência nas comunicações eletrónicas. Como referiu o Tribunal Europeu dos Direitos do Homem (TEDH), «onde, como aqui, um poder do executivo é exercido em

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

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 de 6.06.2006, Caso SEGERSTEDT-WIBERG e outros c. Suécia, pedido n.º 62332/00)[11].

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 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. O que aqui não sucede.

Nestes termos, a CNPD entende que a institucionalização de um controlo prévio e sucessivo 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 na Proposta (por violação do n.º 4 do artigo 34.º e do n.º 2 do artigo 18.º da CRP).

Com o mesmo fundamento, por não estar assegurado o controlo (prévio e sucessivo) 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, parece poder concluir-se pela violação do n.º 1 do artigo 8.º da Convenção Europeia dos Direitos Do Homem e, paralelamente dos artigos 7.º e 8.º da Carta, bem como do n.º 1 do artigo 26.º e 35.º da CRP.

[11] Esta é, aliás, a jurisprudência constante do Tribunal Europeu dos Direitos do Homem - 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.

## 3. As categorias legais de dados

A terminar a apreciação da Proposta de Lei a CNPD assinala que a classificação dos dados de comunicação nela assumida parece pretender fugir ao atual enquadramento constitucional e legal para o tratamento daqueles dados, não sendo por isso admissível na ordem jurídica nacional.

Com efeito, no artigo 1.º da Proposta começa-se por definir o objeto do diploma, especificando-se que o mesmo regula um procedimento especial de *acesso a dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas*.

Esses dados, como se referiu supra, são armazenados ao abrigo de diplomas legais que definem as categorias de dados pessoais suscetíveis de conservação, e que se reconduzem a *dados de tráfego* e *dados de localização* – cf. as definições contidas no n.º 1 do artigo 2.º da Lei da Privacidade nas Comunicações Eletrónicas, que transpôs as Diretivas relativas ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.

São, pois, estas as categorias de dados suscetíveis de armazenamento na ordem jurídica portuguesa, pelo que são estas as categorias suscetíveis de ser objeto de acesso pelo SIRP.

3.1. Todavia, a Proposta, no n.º 2 do artigo 1.º, reporta-se a uma categoria aparentemente nova: *dados de telecomunicações e Internet*. Dir-se-ia reconduzir-se ela aos dados de comunicação, tal como se encontram definidos na alínea a) do n.º 1 do artigo 2.º da Lei da Privacidade nas Comunicações Eletrónicas – *qualquer informação trocada ou enviada entre um número finito de partes mediante a utilização de um serviço de comunicações eletrónicas acessível ao público*. Mas na definição apresentada, a Proposta distingue as duas categorias como se elas não tivessem uma natureza comum e fossem meras realidades somadas sob aquela designação.[12] [13]

---

[12] Note-se que a expressão «banco de dados» não é um conceito técnico utilizado em Portugal; é uma expressão comum apenas na língua portuguesa do Brasil, sugerindo-se, por isso, a sua substituição por *bases de dados,* que se julga ser a realidade aqui em vista.

[13] Não pode deixar de se assinalar, antes do mais, a linguagem obsoleta empregada na definição dos dados de telecomunicações, ao reportar-se a *prestação de serviços telefónicos*, quando, como é bom de ver, hoje as comunicações abrangem um conjunto de trocas ou envio de informações que não envolve a utilização daquele específico tipo de serviço. Considerando, por exemplo, as chamadas de voz, estas podem ser estabelecidas

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Na verdade, todas as informações (ou registos) abrangidos pelo conceito de «dados da Internet» são comunicações para efeito dos diplomas legais que preveem a sua conservação, estando sujeitas ao regime jurídico comum de tratamento dos dados de comunicação por terem a mesma natureza. Em especial, destaque-se que o simples acesso a um sítio na Internet implica o estabelecimento de uma comunicação entre o equipamento do utilizador da Internet e o sistema que disponibiliza o referido sítio, sendo certo que para o seu estabelecimento a prestadora dos serviços de comunicações eletrónicas recolhe informação relativa ao endereço de IP (*Internet Protocol*) que foi atribuído ao equipamento que o cidadão está a usar (telemóvel, *tablet*, etc.) e que o identifica, bem como o endereço do sítio ou página a que o cidadão está a ligar-se (URL), a data e hora do acesso, a localização, etc. Em suma, trata-se de um conjunto alargado de informação relativa a uma pessoa singular identificada ou identificável no âmbito de uma comunicação e que revela muito da sua vida privada.

E, dentro do conceito de comunicações, tais informações reconduzem-se aos «dados de tráfego», definidos na Lei da Privacidade nas Comunicações Eletrónicas como *quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma* (cf. alínea e) do n.º 1 do artigo 2.º daquela lei), porque em todos aqueles casos (*v.g.,* envio de mensagens, envio de correio, acesso a um sítio na Internet) estabelece-se uma comunicação entre um número finito de partes através de uma rede de comunicações, sendo que essa informação é necessária para o envio da comunicação ou para efeitos de faturação. Por isso, não se alcança a ressalva, na parte final do conceito de dados de Internet, apresentado na alínea b) do n.º 1 do artigo 1.º da Proposta, relativa a «quando não deem suporte a uma concreta comunicação».

Acresce que a classificação dos dados pessoais, como aliás qualquer classificação jurídica, só deve ser invocada ou recebida nos textos legislativos se para as categorias diferenciadas se previr um regime jurídico diferenciado; todavia, apesar desta autonomização, o legislador no restante articulado refere-se sempre conjuntamente a ambas («dados de telecomunicações e Internet»).

---

diretamente através dos serviços das operadoras de comunicações, mas também através de outros fornecedores de serviços de comunicações, nomeadamente redes sociais e fornecedores de comunicações OTT (*i.e.,* serviços de comunicações de conteúdos, quer sejam áudio, vídeo ou outros, que assentam sobre aplicações que usam a Internet – WhatsApp, Skype, Viber), não se alcançando a razão por que este tipo de comunicação mereça menos proteção nestes ambientes do que noutras redes de comunicação.

A CNPD entende, assim, que a diferenciação entre dados de telecomunicações e dados de Internet não tem qualquer enquadramento jurídico ou técnico, assentando mesmo num erro de perceção do que é uma comunicação, devendo por isso ser eliminada. Demais, o termo "telecomunicações" não é já empregue nos diplomas europeus e nacionais vigentes sobre comunicações eletrónicas e em especial na Lei da Privacidade nas Comunicações Eletrónicas, devendo, por razões de clareza jurídica e de uniformidade concetual e normativa, ser substituído pelo conceito de *comunicações eletrónicas.*

3.2. A Proposta, no n.º 3 do artigo 1.º, prossegue ainda na classificação dos dados pessoais armazenados pelas prestadoras de serviços de comunicações eletrónicas, para distinguir, dentro da categoria dos «dados de telecomunicações e Internet», três categorias de dados. Inspira-se o legislador numa classificação de fonte doutrinal e jurisprudencial que o Tribunal Constitucional recuperou no acórdão n.º 403/2015, a qual acrescenta, aos dados de conteúdo e aos dados de tráfego os *dados de base*. Estes vêm definidos como dados relativos à conexão de rede, *i.e.,* os elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respetivo serviço e que são prévios a qualquer comunicação. E que o Tribunal exemplifica com o número de telefone, endereço eletrónico e contrato de ligação à rede (cf. ponto 15). Ou seja, o Tribunal Constitucional distingue os *dados de base*, prévios e pressuposto de comunicações, dos *dados de tráfego,* que correspondem às informações necessárias ao estabelecimento de uma comunicação individual e concreta. Esta classificação é, como se disse, acolhida na Proposta de Lei em apreço.

A Proposta define, então, os dados de base como *dados para acesso à rede pelos utilizadores, compreendendo a identificação e morada destes, e o contrato de ligação à rede*.

Simplesmente, estes dados estão, de acordo com os diplomas legais que permitem na ordem jurídica portuguesa a recolha e conservação dos dados de comunicação (Lei da Privacidade nas Comunicações Eletrónicas e Lei n.º 32/2008), incluídos na categoria dos *dados de tráfego*. Eles são, de facto, *dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma* (cf. alínea e) do n.º 1 do artigo 2.º da Lei da Privacidade nas Comunicações Eletrónicas). Nessa medida, não se alcança como se possa pretender diferenciar os alegados dados de base, conceito de origem doutrinal (que remonta a 1990 e a Yves Poullet), sem qualquer correspondência na lei nacional

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

ou no regime jurídico europeu que esta transpôs, e que estão sujeitos ao regime jurídico de tratamento dos dados de tráfego.

A CNPD considera, por isso, que a autonomização legal dos dados de base, em relação aos dados de tráfego, contradiz o regime jurídico garantístico da privacidade das comunicações eletrónicas previsto no Direito nacional e da União e afeta a proteção constitucionalmente assegurada pelo n.º 4 do artigo 34.º da CRP, ao subtrair ao âmbito objetivo da proteção constitucional e legal um conjunto de informação comunicacional que a mesma claramente abarca.

Na Proposta, distinguem-se ainda os *dados de localização do equipamento* de comunicação, quando não deem suporte a uma concreta comunicação. Estando implícito que, quando os dados de localização sirvam de suporte a uma concreta comunicação, integram a categoria dos dados de tráfego – o que, aliás, é reconhecido pelo Tribunal Constitucional no acórdão já citado, em conformidade com o que decorre da Diretiva 2002/58/CE, em especial do considerando 15.

Todavia, também esta autonomização tem de ser devidamente delimitada, já que a posição geográfica do equipamento terminal (ou seja, do dispositivo do utilizador para a comunicação, *v.g.,* telemóvel, portátil) é sempre necessária – e, portanto, é recolhida pelas operadoras que prestam os serviços de comunicação – para o efeito de fornecer o serviço de comunicação.

Como se explicou supra (em 2.), nos dias de hoje ocorrem comunicações mesmo quando o utilizador do equipamento de comunicação não o aciona direta e intencionalmente: as atualizações do correio eletrónico, que se realizem de *x* em *x* minutos, as mensagens que se recebem nos *chats*, etc., o que significa que as comunicações são praticamente constantes, mesmo quando os cidadãos utilizadores dos equipamentos nada fazem.

Por isso, cumpre assinalar que esta distinção quanto aos dados de localização – os que servem de suporte a uma comunicação e os que não servem de suporte a uma comunicação – é algo artificiosa, sendo certo que as situações em que a localização do equipamento não esteja associada diretamente à realização de comunicações são relativamente residuais. Reconduzem-se elas apenas à hipótese prevista no n.º 3 do artigo 7.º da Lei da Privacidade

nas Comunicações Eletrónicas: tratamento para a finalidade de prestação de serviços de valor acrescentado.

De todo o modo, mesmo quanto aos dados de localização para efeito de prestação de serviços de valor acrescentado, a intrusão na vida privada e o condicionamento da liberdade dos cidadãos, que o acesso a tais dados sempre representa, constitui uma restrição destes direitos fundamentais, bem como do direito à proteção dos dados. Tal restrição, para se ter como conforme à Constituição, teria de estar definida na lei com pressupostos (de autorização) bem densificados, que prevenissem um acesso generalizado a tais dados, e com garantia de efetiva fiscalização do respeito pelas condições e limites impostos na autorização, bem como com poderes efetivos de realização do exercício dos direitos de acesso e de retificação. Como resulta do que se disse supra, em 2.2., as regras definidas na Proposta de Lei não oferecem garantias suficientes da tutela daqueles direitos fundamentais, pelo que, na perspetiva da CNPD, também quanto ao acesso a estes dados de localização residuais esta Proposta não respeita os limites definidos na Constituição, na Carta e na CEDH.

## III. Conclusão

A CNPD entende que a Proposta de Lei viola a proibição de ingerência nas comunicações eletrónicas prevista na Constituição da República Portuguesa, bem como as normas da Constituição, da Carta dos Direitos Fundamentais da União Europeia e da Convenção Europeia dos Direitos do Homem que tutelam a vida privada e familiar, a proteção dos dados pessoais e a privacidade nas comunicações, com os seguintes fundamentos:

1. Na medida em que as comunicações são hoje um meio permanente e generalizado de interação e que também por isso revelam múltiplas dimensões da vida privada e familiar, as normas que tutelam aquelas dimensões humanas fundamentais têm de ser interpretadas como abrangendo, no seu âmbito de proteção, todos os meios de comunicação e todos os dados pessoais a eles referentes;
2. A proibição de ingerência nas comunicações constante do n.º 4 do artigo 34.º da Constituição abrange todos os dados de comunicação, pelo que o acesso aos dados

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

de comunicação previsto na Proposta de Lei não está coberto pela autorização constitucional, a qual é restrita à matéria de processo criminal;

3. A institucionalização de um controlo prévio e um aparente controlo sucessivo por uma "formação" de juízes, nos termos descritos na Proposta, não é equiparável a um processo criminal, não assegurando as garantias dos direitos fundamentais constitucionalmente previstas;
4. A classificação dos dados de comunicação assumida na Proposta contraria as normas legais (nacionais e europeias) de proteção da privacidade, que definem um mesmo regime jurídico de proteção para todos esses dados, por essa via subtraindo de tal proteção jurídica certo tipo de dados em contradição com o atual quadro constitucional e legal;
5. Os dados de localização relativos à prestação de serviços de valor acrescentado são os únicos dados que não servem de suporte às comunicações, não integrando a categoria de dados de tráfego, mas, enquanto dados pessoais sensíveis reveladores da vida privada e familiar, o correspondente acesso pelo SIRP constitui uma restrição aos direitos fundamentais ao respeito pela vida privada e à proteção de dados pessoais, cujos pressupostos de autorização e garantias previstos na Proposta não estão conformes com a Constituição, a Carta e a Convenção Europeia dos Direitos do Homem.

É este o parecer da CNPD.

Lisboa, 30 de maio de 2017

Filipa Calvão (Presidente)