COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Parecer n.º 31/2017

I. Relatório

O Senhor Presidente da Comissão dos Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República vem solicitar à Comissão Nacional de Protecção de Dados (CNPD) parecer sobre a Proposta de Lei n.º 72/XIII (doravante Proposta) que estabelece medidas de combate ao branqueamento de capitais e ao financiamento do terrorismo, transpondo parcialmente para a ordem jurídica interna a Diretiva (EU) n.º 2015/847/UE do Parlamento Europeu e do Conselho, de 20 de maio, relativa à prevenção da utilização do sistema financeiro e das atividades e profissões especialmente designadas para efeitos de branqueamento de capitais e de financiamento de terrorismo, bem como a Diretiva (UE) n.º 2016/2258 do Conselho, de 6 de dezembro, que altera a Diretiva n.º 2011/16/UE, no que respeita ao acesso às informações antibranqueamento de capitais por parte de autoridades fiscais.

A Proposta em exame estabelece ainda as medidas nacionais necessárias à efetiva aplicação do Regulamento (UE) n.º 2015/847, do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativo às informações que acompanham as transferências de fundos e que revoga o Regulamento (CE) n.º 1781/2006, e procede à alteração do Código Penal, aprovado pelo Decreto-Lei n.º 400/82, de 23 de setembro, e do Código da Propriedade Industrial, aprovado pelo Decreto-Lei n.º 36/2002, de 5 de março.

A Proposta, como resulta da exposição de motivos que a integra, vem alargar o âmbito de aplicação do regime de prevenção do branqueamento de capitais e do financiamento do terrorismo, cria um Registo Central de Beneficiário Efetivo, que será objeto de legislação específica, e dá uma especial importância à troca de informações entre autoridades, contendo normas detalhadas sobre cooperação nacional e internacional. Por último, a Proposta consagra medidas de proteção aos funcionários que comuniquem suspeitas de branqueamento de capitais, protegendo a revelação da sua identidade.

Nos termos da alínea a) do n.º 1 do artigo 23.º da Lei n.º 67/98, de 26 outubro, alterada pela Lei n.º 103/2015, de 24 de agosto (Lei de Proteção de Dados Pessoais – LPDP), compete à CNPD emitir parecer sobre disposições legais relativas 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.

II. Apreciação

Na análise da Proposta de Lei, começar-se-á por destacar três aspetos de regime que suscitam maiores reservas à CNPD quanto aos tratamentos de dados pessoais nela previstos, para em seguida se considerarem outras disposições que merecem melhoramentos ou revisão.

1. Principais aspetos de regime que suscitam reservas quanto à proteção dos dados pessoais

1.1. Em primeiro lugar, a CNPD chama a atenção para o regime relativo ao dever de identificação com a finalidade de prevenção de crimes de branqueamento de capitais e de financiamento de terrorismo, previsto na secção III do capítulo III da Proposta.

O referido regime prevê a recolha de informação relativa aos clientes e respetivos representantes, o que constitui um tratamento de dados pessoais quando incide sobre pessoas singulares. Simplesmente, ao regular os meios comprovativos dos elementos identificativos, no artigo 25.º, a Proposta reflete uma opção que suscita as mais sérias reservas à CNPD.

Na verdade, prevê o n.º 1 do artigo 25.º que a verificação da identidade das pessoas singulares se fará por via da *apresentação* de documentos de identificação válidos. Mas, logo em seguida, admite que a comprovação dos documentos apenas pode ser efetuada por três vias: i. *mediante originais, em suporte físico ou eletrónico;* ii. mediante *cópia certificada dos originais*; iii. mediante *o acesso à respetiva informação eletrónica com valor equivalente*.

Não pode deixar de se estranhar que numa matéria como esta, em que é absolutamente crucial a correta identificação dos clientes e representantes, pelo impacto que os tratamentos de dados subsequentes têm na vida das pessoas, se admita a utilização de soluções que apresentam especiais riscos de manipulação dos documentos e da identificação, como é o caso da comprovação mediante cópia certificada. Com efeito, a reprodução por fotocópia ou

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

por digitalização não assegura que não tenha havido falsificação do documento original; mesmo quando certificada a cópia, não há garantia de que a cópia e a certificação não foram objeto de manipulação após a certificação.

Assim, compreendendo-se que tem de ser encontrada solução para os casos em que as pessoas não são portadoras de documentos de identificação que permitam a autenticação eletrónica ou, por qualquer razão, não estejam em condições de o utilizar por esta via, parece mais adequado admitir a possibilidade de comprovação por um de dois meios: ou por via da recolha presencial dos dados por parte da entidade obrigada com base na leitura do documento apresentado presencialmente e aposição da assinatura do titular no documento onde os dados vão ser inscritos; ou por qualquer outro meio digital que, através de aplicação de um mecanismo que garanta a integridade e autenticidade do mesmo. Aliás, note-se que a hipótese de certidão é admitida na alínea b) do n.º 1 do artigo 38.º, o que se admite desde que seja acompanhada de um qualquer instrumento que, como se disse, garanta a integridade do conteúdo, não se percebendo porque não foi também considerada em sede do artigo 25.º.

Quanto à possibilidade aberta pela alínea c) do n.º 3 do artigo 25.º, de recolha e verificação dos dados eletrónicos junto das entidades competentes responsáveis pela sua gestão, cumpre esclarecer que, se se pretende com isto admitir a assinatura digital à distância, a CNPD, sem conhecer as soluções tecnológicas que irão ser adotadas, não está em condições de se pronunciar sobre a segurança e proteção a informação. Alerta-se, contudo, para o facto de esta possibilidade, se não for acompanhada de medidas tecnológicas e de segurança adequadas, implicar riscos superiores ao da utilização da reprodução do documento de identificação.

O que se acaba de expor vale também para as situações de contratação à distância, a que se refere o artigo 38.º. Com efeito, os meios de comprovação admitidos nas alíneas a) e b) do n.º1 do artigo 38.º (com a ressalva da certidão, desde que com garantias da sua integridade e autenticidade) não previnem o risco de manipulação dos documentos e com isso de adulteração da identidade dos clientes ou representantes. Repare-se que a referência à *comprovação mediante originais em suporte eletrónico* não significa a reprodução em suporte eletrónico de documentos em suporte físico, a qual implica sempre um risco acrescido que aqui, neste contexto, tem de ser evitado.

O aqui sustentado vale, de igual modo, para o disposto na segunda parte do n.º 5 do artigo 40.º, quanto ao procedimento de atualização de informação.

A este propósito, importa notar que o estatuído na primeira parte do n.º 5 do artigo 40.º suscita ainda maiores reservas. Com efeito, está a admitir-se que, sempre que em causa esteja a atualização da informação, se admita a cópia simples dos documentos para efeitos de comprovação da informação. Num procedimento deste tipo (atualização) dir-se-ia dever aplicar-se o princípio do paralelismo da forma e do procedimento. Mas, independentemente da bondade da opção legislativa aqui vertida, sempre se dirá que a cópia simples dos documentos de identificação constitui um documento sem qualquer valor jurídico probatório, precisamente pela facilidade da sua manipulação. Por essa razão, não pode a CNPD deixar de recomendar vivamente a revisão deste preceito.

De todo o modo, refira-se que, ou o legislador impõe a reprodução do documento de identificação, ou ao titular do documento devem ser sempre assegurados meios alternativos de comprovação da identidade, não podendo tal recolha assentar no consentimento livre do mesmo se não forem colocados à sua disposição outros meios para o efeito – cf. a Lei do Cartão de Cidadão, em especial o artigo 4.º.

Acrescente-se ainda que o disposto no n.º 6 do artigo 41.º, quando, no âmbito da execução dos deveres de identificação por terceiros, prevê o dever de transmissão de *cópia dos dados de identificação e de verificação da identidade*, não está a admitir nem a impor a cópia dos documentos de identificação. Reiterando-se neste preceito o que dispõe a Diretiva no n.º 2 do artigo 27.º, apenas se impõe a transmissão dos documentos comprovativos da identificação e da verificação da identidade, o que não é, nem deve ser, a cópia do documento original de identificação.

No mesmo artigo, no n.º 5, prevê-se a possibilidade de as entidades obrigadas complementarem a informação recolhida pelas entidades terceiras ou procederem a nova identificação; tal possibilidade não pode deixar de estar limitada aos meios admissíveis nos termos do artigo 25.º.

1.2. Outro traço de regime que sobressai da leitura do diploma, mas que estranhamente é afastado num artigo da Proposta prende-se com a limitação da utilização dos dados pessoais

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

recolhidos para a finalidade de prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo.

Apesar deste princípio da finalidade estar explicitado na Diretiva aqui transposta, cujo objeto e âmbito se limita a tal finalidade (cf. artigo 1.º e 41.º da Diretiva[1]), e o mesmo estar refletido no n.º 2 do artigo 57.º da Proposta, proibindo-se o seu tratamento pelas entidades obrigadas para *quaisquer outros fins*, bem como no artigo 1.º da Proposta, quando delimita o seu objeto, é introduzido no artigo 127.º uma norma a prever o acesso da Autoridade Tributária e Aduaneira a todos os dados pessoais tratados ao abrigo deste diploma, *para efeitos da apreciação e controlo do cumprimento das obrigações previstas no Decreto-Lei n.º 61/2013, de 10 de maio, e para assegurar a cooperação administrativa no domínio da fiscalidade.*

Considerando o elevadíssimo grau de ingerência na vida privada das pessoas que decorre do regime aqui proposto, o qual na ponderação dos direitos fundamentais e dos interesses públicos envolvidos apenas vem justificado pelo Direito da União Europeia para a prevenção e combate aos crimes de branqueamento de capitais e financiamento do terrorismo, não pode deixar de se alertar para a extensão do regime restritivo ao combate a outros tipos de crimes no âmbito da fiscalidade. O crime de branqueamento de capitais vem aqui expressamente visado por se tratar de um crime que surge frequentemente associado ao financiamento de terrorismo e a outras formas de criminalidade grave.

Aliás, esta extensão foi equacionada pelo legislador europeu e afastada, na versão da Diretiva que veio a ser objeto de aprovação, após tomadas de posição por diferentes organismos que sublinharam o excesso de tal medida restritiva no contexto do combate ao crime de evasão e fraude fiscais[2].

Não deixa de espantar que o legislador nacional venha agora, apesar de vinculado pelo mesmo quadro jurídico europeu a que está vinculado o legislador europeu, e vinculado por uma Constituição que impõe de forma especialmente reforçada o respeito pela vida privada

---

[1] *Vide* ainda o considerando 43 da Diretiva.

[2] Cf. o parecer do Autoridade Europeia de Proteção de Dados, de 4 de julho de 2013, disponível em https://edps.europa.eu/sites/edp/files/publication/13-07-04_money_laundering_en.pdf, e ainda a carta do Grupo de Trabalho que congrega os comissários de proteção de dados dos Estados Membros da União Europeia (denominado Grupo de Trabalho do Art. 29) de 4 de abril de 2013, acessível em http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130404_aml_letter_to_ep_en.pdf

dos cidadãos, introduzir, no seio de um artigo já por si estranho (veja-se a imprecisão jurídica da epígrafe do artigo[3]), a possibilidade de acesso a toda esta informação recolhida exclusivamente para a prevenção do branqueamento de capitais e do financiamento do terrorismo e, conexamente, passível de acesso para o combate a estes crimes, para uma finalidade distinta e que não é abrangida pelo objeto do próprio diploma, nem, como é óbvio, pela Diretiva que se diz transpor.

Repare-se que entre esta informação estão, além da informação relativa a operações financeiras, os perfis de risco, criados pelas entidades financeiras e outras entidades obrigadas, sobre as pessoas singulares suas clientes ou representantes dos clientes, fruto de processos de *data mining*, como se depreende do disposto no artigo 18.º da Proposta.

A CNPD chama a atenção para o facto de os tratamentos de dados pessoais previstos na Diretiva que se visa transpor e que esta Proposta vem concretizar serem altamente restritivos dos direitos fundamentais à reserva da vida privada e à proteção dos dados pessoais (previstos nos artigo 26.º e 35.º da Constituição da República Portuguesa), expondo numa extensão e intensidade muito elevadas a vida privada das pessoas no que aos seus rendimentos, gestão do património, investimentos e despesas diz respeito, revelando até, em muitas circunstâncias, aspetos íntimos das relações pessoais das mesmas.

Por essa razão, a CNPD recomenda a revisão da solução vertida no artigo 127.º de admitir que a AT aceda a todos estes dados para a prevenção e combate a outro tipo de crimes fiscais, limitando os acessos pelas autoridades públicas ao estritamente necessário para prosseguir a finalidade, assumida na Diretiva e na Proposta, de prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo.

1.3. Em terceiro lugar, cabe destacar o conjunto de normas que na Proposta de lei em apreço confere amplos poderes de acesso e cruzamento de dados pessoais sensíveis por parte das muitas entidades públicas elencadas na Proposta.

---

[3] «Cooperação em matéria de registos e bases de dados», epígrafe cuja reformulação se recomenda, já que não tem um sentido próprio, nem segue a tradição de caracterizar a cooperação por referência às entidades ou por reporte às finalidades a prosseguir.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Para a finalidade de prevenção e combate ao branqueamento de capitais e financiamento do terrorismo compreende-se que as entidades com funções nesta matéria disponham da possibilidade de aceder e relacionar tais dados.

O que não se compreende é que tais poderes sejam atribuídos de forma genérica, por recurso a normas vagas ou abertas (admitindo o acesso a qualquer informação, por exemplo), e sem a previsão na lei das garantias adequadas de tutela dos direitos e liberdades dos cidadãos. Na verdade, há uma omissão legal quanto ao procedimento de prevenção – vulgo, processo administrativo – deixando-se a cada autoridade interveniente a liberdade ou autonomia para o tramitarem como entender, e sem garantias para os cidadãos[4]: aquelas garantias que num processo criminal, mesmo perante um concreto indício de prática de crime, são constitucional e legalmente asseguradas ao arguido, não existem aqui, quando em rigor não há indício de tal prática, mas apenas meros comportamentos desviantes em relação a um padrão discricionariamente identificado.

Sendo inegável o impacto que tal juízo de suspeição tem na vida das pessoas, sem possibilidade de efetiva defesa, sobram dúvidas quanto à constitucionalidade desta solução, em face das garantias que o artigo 32.º da Constituição prevê.

Assim, o reconhecimento de amplos poderes para a finalidade de prevenção ao DCIAP, no artigo 81.º, e à Unidade de Investigação Financeira, nos artigos 82.º e 83.º, nos termos genéricos em que vêm definidos (*v.g.*, acesso *a toda a informação financeira, fiscal, administrativa, judicial e policial;* acesso a *quaisquer elementos ou informações que considere relevantes para o exercício das funções*), suscitam reservas por parte da CNPD, na ausência de regras procedimentais legalmente fixadas e de mecanismos de controlo da sua atuação. Sobretudo perante uma norma que lhes atribui um poder de acesso a toda e qualquer informação pessoal independentemente da fonte e de quem a detenha, como é a consagrada no artigo 113.º.

Note-se que este artigo, tal como se encontra redigido, permite reconhecer o livre acesso aos dados de comunicações eletrónicas na posse das operadoras que prestam serviços de comunicação, quando o acesso a tais dados depende de despacho judicial.

[4] Recorda-se o que sobre este assunto se descreve no Relatório dos Serviços de Inspeção do Ministério Público ao DCIAP, quanto ao período relativo a 2009-2013, disponível em http://www.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_inspecao_dciap.pdf

A que acresce o facto de, nos termos regulados na Proposta, os deveres de segredo a que está sujeita a informação pessoal tratada serem derrogados em nome da prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo, sem intervenção de um juiz, bastando alegar necessidade do acesso à informação (cf. artigos 56.º e 124.º).

A este propósito, refira-se que na alínea d) do n.º 8 do artigo 124.º se prevê como entidade com competências operacionais no domínio da prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo o Serviço de Informações de Segurança e o Serviço de Informações Estratégicas de Defesa do Sistema de Informações da República Portuguesa (SIRP). Sucede que, de acordo com o atual quadro legal vigente, tais competências não se enquadram nas atribuições legais dos serviços do SIRP. Nem tão-pouco o poder de aceder aos dados pessoais detidos por entidades privadas – cf. o artigo 4.º e n.º 2 do artigo 9.º da Lei n.º 9/2007, de 19 de fevereiro. Pelo que esta norma legal não é, *per se*, suficiente para alargar os poderes jurídicos do SIRP. E, de todo o modo, sempre se entenderia tal solução como desnecessária e claramente excessiva, em face do reconhecimento dessa atribuição e desses poderes a outras autoridades públicas e na ausência de garantias adequadas de controlo desses acessos pelos SIRP.

A CNPD sugere, assim, a eliminação daquela alínea.

Em síntese, a CNPD recomenda a reponderação da ausência de intervenção judicial nos tratamentos de dados pessoais em matéria de prevenção criminal, por contrariar o sentido da proteção constitucionalmente assegurada, bem como a revisão do disposto nos artigos 81.º, 82.º e 113.º da Proposta, pelo carácter excessivo da atribuição legal de poderes de acesso aos dados pessoais.

Recomenda ainda a eliminação da referência aos SIRP como organismo autorizado a aceder aos dados pessoais neste contexto.

2. Outras disposições da Proposta

Consideram-se agora os restantes artigos da Proposta que levantam dúvidas em matéria de proteção de dados pessoais.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

2.1. Artigo 9.º

No capítulo II da Proposta, o artigo 9.º vem consagrar que «*Sempre que, no decurso das avaliações nacionais de risco e suas posteriores atualizações, se suscitem preocupações em matéria de proteção de dados pessoais, a Comissão de Coordenação dá conhecimento das mesmas à Comissão Nacional de Proteção de Dados, a qual se pronuncia sobre elas no prazo de 30 dias a contar da comunicação*».

Sendo certo que esta previsão legal não afeta, nem pode afetar nos termos definidos no artigo 41.º da Diretiva que a Proposta pretende transpor, as competências reconhecidas à CNPD pela LPDP, de acordo com o regime europeu de proteção de dados, importa sublinhar que a expressão «preocupações» não constitui, na tradição jurídica portuguesa, um conceito jurídico relevante e devidamente delimitado. Recomenda-se, por isso, a sua substituição por uma fórmula juridicamente adequada que exprima os receios ou dúvidas quanto ao impacto que uma dada operação sobre dados pessoais pode ter sobre a privacidade e sobre o âmbito de proteção constitucionalmente assegurado.

2.2. Artigo 10.º

Não pode deixar de se assinalar, por razões de certeza jurídica, que no artigo 10.º da Proposta, sob a epígrafe *Limites* proíbe-se que as entidades obrigadas intervenham em negócios que envolvam a violação dos limites à utilização de numerário alegadamente previstos nos n.ºs 1 e 3 do artigo 63.º-E da Lei Geral Tributária. Porém, após busca aturada no Diário da República e noutras bases de dados de legislação, a CNPD não logrou encontrar tal norma.

Nesta medida, a CNPD recomenda a revisão do artigo.

2.3. Artigo12.º

Por sua vez o artigo 12.º da Proposta impõe a necessidade das entidades obrigadas definirem um sistema de controlo interno adequado à gestão eficaz dos riscos de branqueamento de capitais e de financiamento do terrorismo a que a mesma esteja exposta e ao cumprimento de normas regulamentares em matéria de prevenção do branqueamento de capitais e financiamento do terrorismo. Tais procedimentos e controlos devem ser proporcionais à

natureza, dimensão e complexidade da entidade obrigada e da atividade por esta prosseguida, compreendendo, entre outros, o desenvolvimento de políticas e procedimentos em matéria de proteção de dados pessoais.

Ao contrário das restantes políticas e procedimentos, os previstos na alínea l) do n.º 2 do artigo 12.º da Proposta têm de ser diretamente enquadrados pelo regime jurídico de proteção de dados pessoais, razão por que se recomenda a referência explícita na norma à LPDP.

2.4. Artigos 20.º e 108.º

O artigo 20.º da Proposta em análise versa a comunicação de irregularidades impondo às entidades obrigadas a criação de canais específicos, independentes e anónimos, que garantam a confidencialidade das comunicações recebidas e a proteção dos dados pessoais do denunciante e do suspeito da prática da infração, nos termos da LPDP.

O referido regime vem depois definido no artigo 108.º, aí se reiterando que é garantida a proteção dos dados pessoais do denunciante e do suspeito da prática da infração, nos termos da LPDP e que é obrigatório criar canais específicos e anónimos para a denúncia. Cumpre, todavia, assinalar que a LPDP não prevê qualquer regime de anonimato, como parece decorrer de tal remissão. Ao contrário, o entendimento da CNPD, no atual quadro legislativo, até é o de o denunciante dever estar identificado, para prevenir o crime de denúncia caluniosa, ainda que com adoção de mecanismos que impeçam o conhecimento da identidade do denunciante até ao momento em que seja exigida essa informação para defesa dos direitos do denunciado[5].

Por outro lado, importa notar que o disposto nos artigos 20.º e 108.º da Proposta parece contradizer-se, ora pressupondo a identificação do denunciante, ora afirmando o anonimato do mesmo no procedimento de denúncia – cf. n.º 1 do artigo 20.º e no n.º 6 do artigo 108.º, quando se refere a *canais anónimos* de comunicação.

Uma vez que a Proposta admite a identificação do denunciante – como decorre do n.º 6 do artigo 20.º e dos n.ºs 3, 4, e 5 do artigo 108.º – sugere-se uma redação mais coerente para o n.º 1 e alínea b) do n.º 2 do artigo 20.º e n.º 2 e n.º 6 do artigo 108.º, para que fique claro que

[5] Cf. Deliberação n.º 765/2009 da CNPD, acessível em https://www.cnpd.pt/bin/orientacoes/DEL765-2009_LINHAS_ETICA.pdf

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

a salvaguarda da confidencialidade quanto à identidade do denunciante será garantida por meio de canais de comunicação desenhados de modo a assegurar que a informação relativa à identidade do denunciante seja de acesso restrito.

2.5. Artigo 22.º

O artigo 22.º prevê que as entidades que integram o mesmo grupo, na aceção da alínea t) do n.º 1 do artigo 2.º da Proposta, partilhem informações relevantes para efeitos de prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo.

Todavia, a norma vem redigida em termos muito amplos e vagos, sem a precisão exigível a normas legais que consubstanciam a restrição de direitos, liberdades e garantias, como a que aqui está em causa ao pretender regular um tratamento de dados sensíveis (troca ou partilha de informações financeiras e patrimoniais sobre pessoas singulares). Assinale-se, por exemplo, os termos amplos em que é definido o universo de pessoas legitimadas a aceder à informação (dentro de cada grupo ou entidade do grupo), recorrendo-se ao advérbio *designadamente* na alínea b) do n.º 2 do artigo 22.º, o que retira qualquer precisão reguladora ao preceito.

2.6. Artigo 57.º

O artigo 57.º da Proposta autoriza as entidades obrigadas a realizar os tratamentos de dados pessoais necessários ao cumprimento dos deveres preventivos nela previstos, não podendo tais dados ser posteriormente tratados, com base no presente diploma legal, para quaisquer outros fins, incluindo fins comerciais.

A autorização expressa, por via legal, de todos os tratamentos necessários ao cumprimento dos deveres preventivos do branqueamento de capitais e do financiamento do terrorismo, recorrendo a uma fórmula genérica em detrimento da enumeração dos mesmos, contraria o disposto no artigo 30.º da LPDP, que exige que os diplomas que pretendam servir de base regulatória dos tratamentos de dados pessoais sejam precisos na definição dos elementos dos tratamentos.

Por outro lado, considerando que a proibição de desvio de finalidade vem já consagrada na alínea b) do n.º 1 do artigo 5.º da LPDP, não se alcança o sentido ou função do n.º 4 do artigo

57.º da Proposta, quando refere que o disposto no n.º 2 *não prejudica os tratamentos de dados pessoais aí referidos com base em outras disposições legais, nomeadamente* na LPDP.

Por um lado, o disposto nesta norma nada acrescenta ao regime em termos de garantias dos direitos fundamentais dos cidadãos no âmbito dos tratamentos de dados pessoais sobre que incide a Proposta. Por outro lado, quando a Diretiva que a presente proposta vem transpor e este mesmo diploma limitam a utilização dos dados pessoais recolhidos e criados no âmbito dos tratamentos aqui regulados à finalidade de prevenção do branqueamento de capitais e de financiamento do terrorismo, não pode esta norma pretender deixar espaço para que outros diplomas legais venham estender a sua utilização para finalidades distintas, especialmente numa secção que se refere apenas ao tratamento de dados pelas entidades obrigadas.

A CNPD recomenda, por isso, a eliminação do n.º 4 do artigo 57.º.

2.7. Artigos 61.º e 106.º

O artigo 61.º regula a comunicação, transmissão e interconexão de dados. Este artigo levanta várias questões.

Em primeiro lugar, do disposto no n.º 1 resulta que, na medida em que a prevenção e o combate ao branqueamento de capitais e ao financiamento do terrorismo são expressamente reconhecidos como um domínio de proteção de um interesse público importante (cf. n.º 3 do artigo 57.º), a transferência de dados para um Estado que não assegure um nível de proteção adequada pode ser permitida pela CNPD (artigo 20.º, n.º 1, alínea c), da LPDP).

Sublinha-se, no entanto, que esta possibilidade de transferência, tal como vem sendo interpretada pelo Grupo de Trabalho do Art. 29, não abrange a transferência massiva e sistemática de dados pessoais[6].

Em segundo lugar, no que à interconexão de dados pessoais diz respeito, o n.º 3 do artigo 61.º dispõe que «*as entidades obrigadas podem igualmente estabelecer mecanismos de interconexão de dados com qualquer uma das autoridades, pessoas ou entidades a quem, ao abrigo do disposto no número anterior, possam comunicar ou transferir os mesmos*».

---

[6] Cf. Carta de 8 de novembro de 2013, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131108_2nd_letter_aml_cft_directive_regulation_en.pdf

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Paralelamente, também se prevê no n.º 5 do artigo 106.º que as autoridades judiciárias, policiais e setoriais podem estabelecer mecanismos *de interconexão de tais dados com outras autoridades com responsabilidades no domínio da prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo, ainda que situadas em países terceiros.*

Convém, a este propósito, recordar que, nos termos da alínea i) do artigo 3.º da LPDP, a interconexão de dados é uma forma de tratamento de dados pessoais que consiste na possibilidade de relacionamento dos dados de um ficheiro ou sistema de informação com os dados de um outro ficheiro ou sistema mantido por responsáveis distintos, ou pelo mesmo responsável com outra finalidade.

Tendo presente o conceito de interconexão de dados, sugere-se a reformulação daqueles preceitos, já que não há, em rigor, interconexão de dados entre entidades ou pessoas, mas sim entre ficheiros ou sistemas de informação.

Acresce que a autorização genérica de interconexão, sem especificar as bases de dados entre as quais se realizará a interconexão e os demais elementos obrigatórios previstos no artigo 30.º da LPDP, prejudica que estas normas possam funcionar como base legal suficiente para regular todo este tratamento de dados.

A CNPD sugere, portanto, a reformulação do n.º 3 do artigo 61.º e do n.º 5 do artigo 106.º, no sentido de clarificar e densificar os respetivos conteúdos.

Em terceiro lugar, atente-se ainda no artigo 106.º, para destacar que as autoridades judiciárias, policiais e setoriais ficam autorizadas a tratar, enquanto responsáveis por tais tratamentos, os dados pessoais e meios comprovativos a que se refere o artigo 58.º para fins de prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo, abrindo-se no n.º 3 o leque de dados pessoais suscetíveis de tratamento. Com efeito, aí se acrescenta que podem ainda tratar *os demais dados pessoais* que se mostrem relevantes para a prevenção e o combate ao branqueamento de capitais e ao financiamento do terrorismo, em conformidade com o disposto na LPDP.

A previsão geral e genérica de tratamento de dados pessoais, sem precisar as categorias de dados abrangidas prejudica a possibilidade de este preceito servir de base legal legitimadora do acesso a outros dados pessoais que não venham especificamente previstos na Proposta – de acordo com o artigo 30.º da LPDP, que exige a especificação das categorias dos dados

pessoais.

Finalmente, ainda quanto ao artigo 106.º assinala-se o previsto no n.º 1. Aí se pode ler que *o disposto na presente lei não prejudica nem é prejudicado pelas disposições relativas ao tratamento de dados pessoais no quadro da cooperação policial e judiciária em matéria penal.*

A CNPD não pode deixar de assinalar a expressão inaudita «não prejudica nem é prejudicado», que torna inútil, para não dizer absurda, esta disposição. Na verdade, em caso de conflito ou contradição entre os dois regimes legais – o que para o legislador parece não poder ocorrer –, não se alcança qual o regime prevalecente. E, no entanto, considerando que a Proposta regula, quase do princípio ao fim, tratamentos de dados pessoais, não deixa de se estranhar que se possa afirmar, à partida, como certo que não existe qualquer desajustamento ou incoerência entre os dois regimes legais.

A CNPD recomenda, por isso, a revisão desta norma, ou mesmo a sua eliminação, deixando a resolução de eventuais problemas de aplicação de lei aos princípios jurídicos bem sedimentados na nossa ordem jurídica.

2.8. Disposições transitórias

Chama-se a atenção para as incongruências detetadas nos n.ºs 2 e 3 do artigo 188.º. No n.º 2 faz-se referência aos prazos previstos no número anterior, quando no n.º 1 não se prevê qualquer prazo; no n.º 3 faz-se referência ao disposto nos n.ºs 3 e 4, sem que se saiba a que artigo se reportam.

2.9. Indeterminação normativa quanto aos tratamentos de dados pessoais

A Proposta de Lei em apreço adota uma técnica de regulação dos tratamentos de dados pessoais que não cumpre, plenamente, as exigências do artigo 30.º da LPDP. Com efeito, a previsão geral e genérica de tratamento de dados pessoais, sem precisar as exatas categorias de dados abrangidas, as exatas interconexões de dados ou as categorias e entidades que estão legitimadas a transmitir dados, prejudica a possibilidade de uma série de normas da Proposta servirem de base legal legitimadora do tratamento dos dados.

É o que sucede, para além das normas já mencionadas supra, por exemplo com o n.º 1 do

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

artigo 32.º («pelo menos»), a alínea a) do n.º 6 do artigo 36.º («informação adicional»), alínea c) do n.º 1 do artigo 44.º («pelo menos»), o n.º 4 do artigo 95.º («a qualquer pessoa as informações e os elementos que considerem relevantes para o exercício das duas funções»), e os n.ºs 5 e 6 do artigo 111.º («pelo menos», «nomeadamente», «toda e qualquer circunstância [...] que, pela gravidade, frequência ou quaisquer outras circunstâncias atendíveis, sejam relevantes [...] de acordo com as características, a complexidade e a dimensão da entidade obrigada»). Aqui se denota a falta de precisão normativa imprescindível à regulação dos tratamentos de dados pessoais, sem se delimitar as categorias de dados pessoais ou o universo das pessoas singulares abrangidas, como se uma norma aberta, recorrendo a advérbios ou outras expressões meramente exemplificativas ou a conceitos genéricos, pudesse legitimar a restrição, com esta intensidade e extensão, de direitos, liberdades e garantias.

A CNPD alerta, assim, para a inadmissibilidade, em matéria de tratamento de dados pessoais que constituem intensas restrições dos direitos, liberdades e garantias, de normas genéricas, que abrem a porta ao tratamento de todo e qualquer dado ou relativo a toda e qualquer pessoa singular, sem se delimitar por critérios objetivos e seletivos o universo objeto do tratamento.

2.10. Regulamentação da Proposta de Lei

São vários os artigos da Proposta que remetem para regulamentação administrativa a definição de aspetos de regime dos tratamentos de dados pessoais aqui previstos.

Importa notar, em primeiro lugar, que essa regulamentação tem de estar em conformidade com o presente regime legal e com a Diretiva que este visa transpor, não sendo admissível que se contrarie por via de regulamento administrativo, o regime legal.

Em segundo lugar, destaca-se que não pode por via regulamentar alargar o regime legal dos tratamentos de dados pessoais, já que tal alargamento representa a extensão ou aumento da restrição de direitos, liberdades e garantias, o que, nos termos do n.º 2 do artigo 18.º da Constituição, só pode ocorrer por via legislativa.

Em todo o caso, sempre que tais regulamentos venham complementar o regime legal, inovando, devem os mesmos ser sujeitos a consulta da CNPD, em conformidade com o sentido da imposição n.º 2 do artigo 22.º da LPDP.

Assinalam-se particularmente os poderes regulamentares previstos no artigo 43.º, no n.º 2 do artigo 72.º, no n.º 7 do artigo 76.º e no artigo 94.º.

Em especial, chama-se a atenção para o artigo 112.º, n.º 2, da Proposta, que remete para regulamento da Autoridade de Segurança Alimentar e Económica a criação de uma base de dados com o registo atualizado dos prestadores de serviços a sociedades, a outras pessoas coletivas ou a centros de interesses coletivos sem personalidade jurídica, definindo através de regulamentação os elementos a ele sujeitos, as respetivas obrigações de atualização e os demais termos necessários ao funcionamento do mesmo. A remissão para este regulamento da criação de uma nova base de dados pessoais parece configurar uma deslegalização proibida pela Constituição (cf. n.º 5 do artigo 112.º da CRP).

Nota-se ainda que todo o regime proposto pressupõe a recolha e a troca de informações entre entidades obrigadas, entre estas e as autoridades públicas e entre as diferentes autoridades públicas, numa teia de comunicações que, considerando a elevada sensibilidade da informação pessoal (e que abrange e dos juízos de valor que sobre as pessoas são feitos, refletidos nos perfis de risco), devem estar dotadas das melhores soluções tecnológicas atualmente disponíveis e de medidas técnicas e organizativas de elevada segurança.

Justifica-se, por isso, a expressa previsão de tal obrigação no diploma, a acrescer à simples remissão para os artigos14.º e 15.º da LPDP.

III. Conclusões

Com os fundamentos acima desenvolvidos, para além das pontuais recomendações expostas no ponto II. 2, a CNPD:

1. Chama a atenção para a necessidade de, na definição dos meios comprovativos da identificação, se afastarem soluções que apresentam especiais riscos de manipulação dos documentos e da identidade, como sucede com admissibilidade de cópia simples dos documentos (também de identificação) aquando da atualização da informação, e de comprovação mediante cópia certificada;

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

2. Recomenda a revisão do artigo 127.º, que admite que o conjunto dos dados pessoais sensíveis (*v.g.,* relativos a transações financeiras, perfis de risco) recolhidos para a prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo seja acedido pela AT para a prevenção e combate a outro tipo de crimes fiscais, no sentido de limitar os acessos pelas autoridades públicas ao estritamente necessário para prosseguir a finalidade, assumida na Diretiva e na Proposta, de prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo, sob pena de inconstitucionalidade do artigo por violação do princípio da proporcionalidade;
3. Recomenda também a revisão do disposto nos artigos 81.º, 82.º e 113.º da Proposta, pelo carácter aberto e, consequentemente, excessivo da atribuição legal de poderes de acesso aos dados pessoais em sede de prevenção criminal pelos organismos públicos com atribuições de prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo;
4. Recomenda ainda a definição, na Proposta, de regras de procedimento e controlo para a atividade de tais organismos e com a previsão na lei das garantias adequadas de tutela dos direitos e liberdades dos cidadãos – garantias que num processo criminal, mesmo perante um concreto indício de prática de crime, são constitucional e legalmente asseguradas ao arguido, vêm aqui negadas, quando em rigor não há indício de tal prática, mas apenas meros comportamentos desviantes em relação a um padrão discricionariamente identificado;
5. Recomenda finalmente a eliminação da referência aos SIRP como organismo autorizado a aceder aos dados pessoais neste contexto, uma vez que, no atual quadro legal vigente, tais competências não se enquadram nas atribuições legais daqueles serviços, não bastando esta norma para a alteração de tais atribuições: por outro lado, tal solução é desnecessária e claramente excessiva, em face do reconhecimento dessa atribuição e desses poderes a outras autoridades públicas e na ausência de garantias adequadas de controlo desses acessos pelos SIRP.
6. Alerta para a necessidade de revisão do diploma, por forma a eliminar as fórmulas genéricas e abertas de regulação dos tratamentos de dados pessoais, que abrem a porta ao tratamento de todo e qualquer dado ou relativo a toda e qualquer pessoa

singular, sem se delimitar por critérios objetivos e seletivos o universo objeto do tratamento, as quais são inadmissíveis quando tais tratamentos consubstanciam intensas restrições dos direitos, liberdades e garantias;

É este o Parecer da CNPD.

Lisboa, 16 de maio de 2017

Filipa Calvão (Presidente)