ASSEMBLEIA DA REPÚBLICA
CONSELHO DE FISCALIZAÇÃO DO SISTEMA INTEGRADO DE INFORMAÇÃO CRIMINAL

Exmo. Senhor
Presidente da Comissão de Assuntos
Constitucionais, Direitos, Liberdades e Garantias
Prof. Doutor Bacelar de Vasconcelos
Palácio de S. Bento
1249-068 Lisboa

Ofício nº 18/CFSIIC/2018 **Data:**18/06/2018
V/Ofício: n.º 473/1.ª-CACDLG/2018 - Data: 02-05-2018 NU: 600345

ASSUNTO: Envio do Parecer sobre a Proposta de Lei n.º 126/XIII/3.ª (GOV).

Exmo. Senhor Deputado Bacelar de Vasconcelos, Senhor Presidente,

Tenho a honra de enviar a V. Exª. O Parecer deste Conselho de Fiscalização relativo ao pedido sobredito, o qual foi aprovado na sessão realizada em 15 de junho de 2018.

Com os meus melhores cumprimentos, e elevada consideração,

ASSEMBLEIA DA REPÚBLICA
Divisão de Apoio às Comissões
CACDLG
Ofício 604118
Entrada/Saída nº 655 Data: 18/6/2018

O Presidente do CFSIIC

Luís Pais de Sousa

PARECER

Sua Excelência o Senhor Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias solicitou a emissão de parecer por este Conselho sobre a Proposta de Lei n.º 126/XIII/3.ª (GOV) - que "Altera o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial".

A emissão deste parecer decorre do disposto na alínea g) do nº 6 do artigo 8º da Lei nº 73/2009, de 12 de agosto, diploma legal que criou o Conselho de Fiscalização do Sistema Integrado de Informação Criminal (CFSIIC) e estabeleceu as suas atribuições.

I - Considerações preliminares

A proposta de lei sob parecer visa alterar a Lei n.º 34/2009, de 14 de julho, que estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial, adaptando-a ao disposto no Regulamento (UE) n.º 2016/679, do Parlamento e do Conselho, de 27 de abril de 2016 ("o Regulamento"), e na Lei n.º [PL 120/XIII] que assegura a sua execução na ordem jurídica interna, assim como o disposto na Lei n.º [Reg.º PL 74/2018], que transpõe para a ordem jurídica interna a Diretiva (UE) n.º 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 ("a Diretiva").

Assim, como ponto prévio é de salientar que o assunto em análise merece as maiores cautelas, primeiramente, porque contende com matérias estruturantes da organização e funcionamento dos tribunais e, por outro lado, e não menos importante, dada a especificidade dos temas da privacidade e proteção de dados pessoais e a novidade que em alguns aspectos resulta daquele complexo normativo da EU, o que imporia uma discussão ampla de todos os intervenientes

nos vários planos de operação do sistema judicial, desde os «profissionais dos processos», à organização e especialistas na área da informática e segurança de sistemas.

Conforme exposição de motivos, a "proposta de lei introduz um conjunto de garantias que visam assegurar um elevado nível de proteção dos dados pessoais no âmbito do sistema judiciário, onde se afigura necessária uma particular preocupação com a circulação de informação no contexto da tramitação dos processos em várias instâncias e por diferentes entidades".

De acordo com o texto da proposta de lei para o artigo 1º da lei nº 34/2009, no qual é definido o seu "Objeto", esta lei adopta regras sobre "A recolha e o tratamento dos dados necessários ao exercício das competências dos magistrados, dos funcionários de justiça e dos órgãos de polícia criminal no âmbito do processo penal, bem como ao exercício dos direitos dos demais intervenientes nos processos jurisdicionais e da competência do Ministério Público".

Ora, importa assinalar que o regime jurídico que esta lei estabelece para o tratamento de dados do sistema judiciário, já de si um regime especial face à lei geral consubstanciada no Regulamento e à lei especial que transpõe a Diretiva, **não esgota as disposições específicas relativas ao tratamento de dados pessoais** pelos órgãos de polícia criminal e pelas autoridades judiciárias, designadamente quanto aos dados pessoais a tratar.

Com efeito, no âmbito da aplicação da lei nº 83/2017, de 18 de agosto, que estabelece **medidas de natureza preventiva e repressiva de combate ao branqueamento de capitais e ao financiamento do terrorismo**, são as autoridades judiciárias e os órgãos de polícia criminal (além das «entidades obrigadas») autorizadas a tratar várias categorias de dados financeiros e outros, que se mostrem relevantes para a prevenção e o combate ao branqueamento de capitais e ao financiamento do terrorismo, sendo esse tratamento considerado

feito num domínio de **proteção de um interesse público importante**, para efeito dos regimes de proteção de dados (cf. artigo 106.º[1] e artigos 57.º a 61.º).

Por outro lado, no âmbito da Diretiva (UE) 2016/681, do Parlamento e do Conselho, de 27 de abril de 2016, relativa à utilização dos **dados dos registos de identificação dos passageiros** (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, para cuja transposição foi recentemente apresentada a Proposta de lei nº 137/XIII, está prevista a autorização de tratamento de dados PNR, não só pela unidade nacional de informação de passageiros (que aquela proposta designa por "GIP"), mas

[1] Artigo 106.º [Proteção e tratamento de dados pessoais pelas autoridades competentes]
1 - 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.
2 - Sem prejuízo de quaisquer outros tratamentos legítimos, 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, sendo aplicável, com as necessárias adaptações, o disposto no artigo 60.º
3 - Além dos dados para que remete o número anterior e sem prejuízo de quaisquer outros tratamentos legítimos, as autoridades referidas naquele número 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 Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto.
4 - É igualmente aplicável o disposto no n.º 3 do artigo 57.º e no n.º 1 do artigo 61.º
5 - As autoridades judiciárias, policiais e setoriais podem, relativamente aos dados pessoais passíveis de tratamento ao abrigo da presente lei:
a) Comunicar, transferir ou 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, designadamente no âmbito das obrigações de cooperação nacional e internacional previstas no capítulo IX;
b) Proceder à respetiva divulgação junto das entidades obrigadas, na medida em que tal releve para a prevenção e o combate ao branqueamento de capitais e ao financiamento do terrorismo.

também pelas autoridades judiciárias que recebem os dados e os resultados do tratamento efectuado pelo GIP[2].

Assim, não estando, esses regimes «especialíssimos», contemplados no objecto da Proposta de lei sob parecer (nem tão pouco na Proposta de lei nº 125XIII que visa transpor a Diretiva (UE) n.º 2016/680), o regime estabelecido como objecto da lei nº 34/2009, deveria ser consagrado **sem prejuízo dos textos legislativos que prevêem outras disposições específicas em matéria de tratamento de dados pessoais**, salvaguardando assim, designadamente, aqueles outros regimes.

II - Aplicação aos órgãos de polícia criminal

Considera-se de grande relevo que, como consta da exposição de motivos, incumba aos magistrados judiciais e do Ministério Público "a responsabilidade de assegurar a efetiva proteção dos direitos de informação, de acesso e de retificação ou de apagamento dos dados pessoais no processo, independentemente de este ser tramitado nos tribunais ou serviços do Ministério Público ou por outros serviços ou entidades que procedam ao tratamento de dados pessoais no âmbito dos processos da competência das autoridades judiciárias, no exercício de funções de coadjuvação ou de execução de decisões".

Como é sabido, nos termos da Lei da organização da Investigação criminal recai sobre os órgãos de polícia criminal um dever de cooperação mútua, garantido,

[2] DIRETIVA (UE) 2016/681 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016

Artigo 1.o [Objeto e âmbito de aplicação]

1. A presente diretiva prevê:

   a) A transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros (PNR) de voos extra-UE;

   b) O tratamento dos dados referidos na alínea a), inclusive a sua recolha, utilização e conservação pelos Estados-Membros, e o respetivo intercâmbio entre Estados-Membros.

2. Os dados PNR recolhidos nos termos da presente diretiva só podem ser tratados para fins de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, conforme previsto no artigo 6.o, n.o 2, alíneas a), b) e c).

designadamente, por um sistema integrado de informação criminal que assegure a partilha de informações entre os órgãos de polícia criminal.

O sistema integrado de informação criminal é instituído, nos termos da lei nº 73/2009, de 12 de Agosto, através da plataforma para o intercâmbio de informação criminal que assegura a interoperabilidade entre os sistemas de informação dos órgãos de polícia criminal, com vista a possibilitar a partilha de informação.

No entanto, os sistemas de informação dos órgãos de polícia criminal "são independentes uns dos outros e geridos por cada entidade competente de acordo com o quadro legal especificamente aplicável", sendo ainda reconhecido (artº 9º, n.º 5) que "os dados acessíveis através da plataforma são introduzidos, actualizados e apagados unicamente pelos utilizadores dos sistemas de cada órgão de polícia criminal, de acordo com a legislação específica que os regula".

Ora, qualidade dos dados partilhados depende da sua actualização no sistema de informação de cada OPC e da sua real correspondência com a informação constante dos processos que na quase totalidade é a sua fonte de origem.

Não obstante as autoridades judiciárias terem acesso aos dados do SIIC, não têm actualmente qualquer intervenção para que seja garantido que a informação constante dos sistemas dos OPC relativamente aos processos de que são titulares seja efectivamente correta.

É assim de louvar a proposta no n.º 4 do artigo 2º, de que "o disposto nos números anteriores é correspondentemente aplicável ao tratamento de dados pessoais pelos órgãos de polícia criminal, no âmbito do processo penal, e pelos serviços e entidades que procedam ao tratamento de dados pessoais que constem ou sejam destinados a processos da competência das autoridades judiciárias, no âmbito de funções de coadjuvação e de execução de decisões destas autoridades".

Porém, **parece insuficiente a redacção do n.º 5 do mesmo artigo** ao referir que "As especificações relativas aos dados a tratar e aos objetivos e às finalidades do

tratamento a que se refere o número anterior constam das leis de organização dos órgãos, serviços e entidades respectivas".

No contexto referido, deverá ser aquele preceito clarificado para que nessa remissão, embora necessária, seja salvaguardada a aplicação das regras adoptadas na lei objecto da proposta, mediante a respectiva ressalva, ou seja:

> **"5 - Sem prejuízo da aplicação das regras estabelecidas na presente lei, as demais especificações** relativas aos dados (...) constam das leis de organização dos órgãos, serviços e entidades respetivas".

III - Responsáveis pelo tratamento de dados

No artigo 23º n.º 1 da proposta está previsto que "Para efeitos do disposto nos regimes de proteção de dados pessoais, são responsáveis pelo tratamento de dados: (a) Os magistrados judiciais e do Ministério Público competentes, (b) Os juízes de paz e os mediadores dos sistemas públicos de mediação, e (c) As entidades supervisoras da gestão da informação.

Estas "entidades supervisoras da gestão da informação" são o CSM, o CSTAF, a PGR, o CAJP, a DGPJ, os OPC e os "serviços e entidades que procedam ao tratamento de dados pessoais nos termos do n.º 4 do artigo 2.º".

São ainda são responsáveis pelo tratamento (n.º 3) "as entidades indicadas no artigo 33.º: inspectores e secretários de inspecção, juízes presidentes, o Conselho de Acompanhamento dos julgados de Paz e a Comissão de Fiscalização da Atividade dos mediadores de Conflitos.

A noção de responsável pelo tratamento prevista no Regulamento (UE) 679/2016 (RGPD) e na Diretiva não nos parece compatível com a que a presente proposta de lei pretende estabelecer, concretamente em relação aos magistrados e juízes de paz e mediadores dos sistemas públicos de mediação, já que o responsável pelo tratamento é quem "determina as finalidades e os meios de tratamento de dados pessoais".

Ora, não serão os magistrados judicias e do MP individualmente considerados quem define as finalidades e os meios de tratamento.

Aliás, resulta dúbio o entendimento que pode ser retirado da leitura conjugada dos números 3 e 1/a) do artigo 23.º da proposta, não se descortinando o alcance visado pelo autor da proposta de lei com a formulação do número 3, colocando como responsável o Ministério Público, diferentemente dos casos da alínea 1/a), em que são responsáveis os magistrados e da alínea c) do artigo 23º e artigo 24.º, em que a responsabilidade é corporizada no órgão superior do Ministério Público, a Procuradoria-Geral da República.

Chamamos ainda especial atenção neste ponto quanto à questão da responsabilidade pelo tratamento de dados "para efeitos do disposto nos regimes de proteção de dados pessoais", o que poderá suscitar um conflito de regimes de responsabilidade, face ao disposto nos artigos 12º e ss. da lei nº67/2007, de 31 de dezembro, relativa ao regime da responsabilidade civil extracontratual do estado e demais entidades públicas.

Mais se diga que, à luz do Regulamento e da Diretiva, raras serão as hipóteses em que teremos pessoas singulares a assumirem a posição de responsáveis pelo tratamento, na medida em que, as mais das vezes, ou estarão integradas no exercício de funções no seio de organizações, as quais se poderão assumir como responsáveis pelo tratamento, ou serão subcontratadas.

Por outro lado, sempre teria de se chamar à colação o Ministério da Justiça, na medida em que assume as relações do Governo com os Tribunais e o Ministério Público, e nessa arquitetura orgânica, os serviços integrados que o corporizam estarão na posição terminológica a que o Regulamento apelidou de subcontratado, na medida em que os organismos da Justiça tratam dados por conta do responsável pelo tratamento.

Sugerimos, assim, as seguintes alterações para os números 1 e 2 do **artigo 23.º**:

> 1. **Sem prejuízo das competências dos magistrados, dos juízes de paz e dos mediadores, nos termos do número seguinte, são responsáveis**

pelo tratamento de dados, para efeito dos regimes de proteção de dados pessoais, as entidades supervisoras da gestão da informação a que se refere o artigo seguinte, relativamente ao tratamento dos dados cuja gestão lhe é atribuída.

2. É da competência dos magistrados, dos juízes de paz e dos mediadores dos sistemas públicos de mediação, relativamente aos dados tratados no âmbito dos processos que dirigem, assegurar a licitude do tratamento, bem como a efetiva proteção dos direitos de informação, de acesso e de retificação ou apagamento dos dados, oficiosamente ou mediante requerimento do respetivo titular, nos termos das leis de processo e dos regimes de proteção de dados pessoais.

IV - Sobre a autoridade de controlo

Quanto a este ponto em concreto, devemos remeter para as considerações apontadas na exposição de motivos da proposta de lei que lhe dizem diretamente respeito:

Um aspeto saliente do regime prende-se com o papel da CNPD na fiscalização da aplicação do regime da Lei n.º 34/2009, de 14 de julho, e da Lei n.º [Reg.º PL 74/2018] que transpõe a Diretiva.

Dando cumprimento às exigências que resultam da execução na ordem jurídica interna do Regulamento e da transposição da Diretiva, ***limita-se a competência da autoridade de controlo para fiscalizar o tratamento de dados no sistema judiciário.*** *Em especial,* ***exclui-se expressamente do âmbito de competência da CNPD a supervisão de operações de tratamento efetuadas pelos tribunais no exercício da função jurisdicional e pelo Ministério Público, no exercício das suas funções e competências processuais.*** *Pretende-se, deste modo, prevenir a intervenção de uma autoridade administrativa no exercício de funções judiciais, assegurando-se o respeito pela independência dos tribunais e pela autonomia do*

Ministério Público. Esta exceção é estritamente limitada às atividades processuais, não abrangendo outras atividades de registo e tratamento de dados pessoais relacionados com processos ou a eles destinados, nomeadamente dos dados inerentes à sua gestão e administração.

Por outra parte, para efeito de fiscalização dos regimes da Lei n.º 34/2009, de 14 de julho, e da Lei n.º [Reg.º PL 74/2018], que transpõe a Diretiva, e da Lei n.º [PL 120/XIII], que assegura a execução do Regulamento na ordem jurídica interna, prevê-se que a CNPD assuma uma composição especial, incluindo um magistrado judicial e um magistrado do Ministério Público.

Neste cenário, que se considera em linha com os imperativos e orientações europeias, merecem-nos as maiores reservas os termos da redação da atual proposta do artigo 44.º, uma vez que afirma peremptoriamente, no nº 1, que "***A Comissão Nacional de Proteção de Dados (CNPD) é a autoridade de controlo com competência*** *para a garantia e fiscalização da aplicação dos regimes de proteção de dados pessoais e das operações de tratamento de dados pessoais nos termos previstos na presente lei.*".

Ainda que venha nos números seguintes introduzir algumas restrições a esta competência, a proposta para o nº 7 do mesmo artigo prevê, reforçando o teor do nº 1, que: "Tendo em vista o controlo e fiscalização do cumprimento das normas de proteção de dados pessoais, oficiosamente ou na sequência de queixa, **a CNPD pode aceder ao registo referido nos n.os 2 e 3 do artigo 42.º**", ou seja, ao registo que, designadamente, para além da identidade dos utilizadores, contém a "identificação dos dados consultados" e "as operações efectuadas ... designadamente operações (...) de aditamento, alteração, eliminação ou arquivamento dos dados nele [sistema] contidos".

Acreditamos que a definição da autoridade de controlo neste âmbito merece uma reflexão ponderada para dar cabal cumprimento aos imperativos do Regulamento (UE) 679/2016 que, nomeadamente no seu Considerando (20), se detém quanto a este assunto de forma distintamente explícita:

"A competência das autoridades de controlo não abrange o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional, a fim de assegurar a independência do poder judicial no exercício da sua função jurisdicional, nomeadamente a tomada de decisões. Deverá ser possível confiar o controlo de tais operações de tratamento de dados a organismos específicos no âmbito do sistema judicial do Estado-Membro".

V - Comissão de Coordenação da Gestão da Informação do Sistema Judiciário

Nas palavras da exposição de motivos, a "Comissão para a Coordenação da Gestão dos Dados Referentes ao Sistema Judicial" é revitalizada", agora com "uma nova designação, Comissão de Coordenação da Gestão da Informação do Sistema Judiciário, mais adequada às suas competências (...)".

As suas competências, tal como constam dos propostos (nº 3 do artigo 23.º e , aparecem como um misto de entidade de **coordenação**, mas também de **responsável** pelo tratamento de dados e **autoridade de controlo**.

Assim, por ex., a competência de alínea c), do nº 3 do artigo 25.º ["*Colaborar com a Comissão Nacional de Proteção de Dados no exercício dos seus poderes e na prossecução das suas atribuições relativamente à proteção e tratamento de dados pessoais no sistema judiciário*"] corresponde ao dever de cooperação com a autoridade de controlo que o artigo 26.º da Diretiva manda atribuir ao **responsável pelo tratamento**.

A competência de alínea h), do nº 3 do artigo 25.º ["*Manter um registo atualizado dos encarregados de proteção de dados (...) e receber destes toda a informação relevante para o exercício das respetivas competências*", corresponde ao exercício da competência da **autoridade de controlo**, tal como resulta do nº 4, parte final, do artigo 32.º e alíneas d) e e) do artigo 34.º da Diretiva.

Por sua vez, a competência de alínea i), do nº 3 do artigo 25.º [Ser informada pelos responsáveis pelo tratamento (...) das *violações de dados pessoais* ou do disposto na presente lei, e comunicar essas situações às entidades competentes para

efeitos penais ou disciplinares], correspondente de acordo com o artigo 30.º da Diretiva ao exercício dos poderes da **autoridade de controlo**.

E igualmente, o acesso aos registos informáticos das "pesquisas efetuadas pelas pessoas que tenham acesso às bases de dados" e as "competências de auditoria e inspecção" a que se refere o **nº 3 do artigo 38º**, bem como, a comunicação imediata, aos membros da Comissão, de qualquer acesso irregular, prevista na **alínea e), nº 2 do artigo 29.º**, correspondem a funções do responsável e da autoridade de controlo, nos termos do artigo 58.º do Regulamento (cf. alíneas a), b) e e)) e dos artigos 25.º e 46º da Diretiva.

Ora, parece óbvio que pela sua composição e sede a Comissão de Coordenação da Gestão da Informação do Sistema Judiciário não cumpre o requisito de independência, nem a exigência de *"organismo específico no âmbito do sistema judicial"*, para que lhe possa ser confiada essa missão de controlo das operações de tratamento de dados no sistema judiciário.

Sendo imprescindível uma tal Comissão para dar resposta às reais necessidades de coordenação e articulação das entidades directamente envolvidas no sistema judiciário, já quanto às atribuições de controlo do tratamento de dados, a sua composição afasta qualquer mais-valia, à luz dos princípios da separação de poderes e da independência dos tribunais.

Ou seja, se o controlo da actividade judiciária no âmbito do desempenho da função jurisdicional, não pode ser cometida à CNPD, como autoridade de controlo nacional, apesar da sua independência, mas dada a natureza de entidade «administrativa», muito menos poderá uma entidade presidida e constituída em sede do executivo, assumir tal missão.

Não será assim aceitável o poder que a proposta de lei no nº 3 do artigo 38º dá aos membros da Comissão para aceder aos registos informáticos das "pesquisas efetuadas pelas pessoas que tenham acesso às bases de dados...", nem a comunicação imediata, aos membros da Comissão, de qualquer acesso irregular, prevista na alínea e), nº 2 do artigo 29.º, que, além disso, neste caso, suscitaria a questão de como operacionalizar uma medida de segurança especial que

(também ela com a necessária segurança e confidencialidade) garanta "que qualquer acesso irregular seja de imediato comunicado aos membros da Comissão", composta no mínimo por 20 membros.

Ou seja, deverão ser conferidas a esta Comissão as funções de coordenação e articulação, a que correspondem as alíneas a), b), d) e f), do artigo 25.º, **devendo ser excluídas as atribuições das alíneas c), e), g), h) e i), do artigo 25.º**, bem como o acesso aos dados das pesquisas previsto no **n.º 3 do artigo 38º** e a comunicação imediata de qualquer acesso irregular prevista na **alínea e), nº 2 do artigo 29.º**, por serem reservadas aos responsáveis pelo tratamento e à respectiva autoridade de controlo competente.

VI - Desenvolvimento aplicacional – relação com o MJ / IGFEJ

a) No **artigo 25.º**, sobre a Comissão de Coordenação da Gestão da Informação do Sistema Judiciário, está previsto **no nº 6, alínea c)** que o conselho coordenador é integrado por: Dois representantes (...) designados pelo Instituto de Gestão Financeira e Equipamentos da Justiça, I. P., *"enquanto entidade com **competência pela apresentação de propostas** de conceção, execução e manutenção dos recursos tecnológicos e dos sistemas de informação da justiça* e (...) *pela **elaboração de propostas** de articulação com o plano estratégico..."*, competências estas que estão em concordância com as atribuições daquela Comissão, designadamente as estabelecidas nas alíneas *b)* e *d)* [respectivamente, *"Assegurar a cooperação no desenvolvimento das aplicações informáticas necessárias à tramitação dos processos e à gestão do sistema judiciário"* e *"Definir orientações (...) tendo designadamente em conta as prioridades em matéria de desenvolvimento aplicacional (...)"*.

No entanto, contraditoriamente, no **artigo 26.º, n.º 1** lê-se que *"Compete ao Instituto de Gestão Financeira e Equipamentos da Justiça, I. P., (...) a definição, a conceção, o desenvolvimento e a manutenção das aplicações informáticas"* e **no n.º 2** que *"No âmbito das competências referidas no número anterior, o IGFEJ deve*

comunicar à Comissão (...), podendo a Comissão apresentar propostas de desenvolvimento das aplicações informáticas".

Ora, sendo a Comissão presidida pela entidade que tutela o IGFEJ, **não faz sentido a inversão de papéis** que a redacção destes números documenta, pelo que deverão ser corrigidos, para traduzir, em harmonia com o artigo 25º, a normal relação de subordinação, substituindo-se o segmento, acima transcrito, do **artigo 26.º, n.º 1** por:

> "1. Compete ao Instituto de Gestão Financeira e Equipamentos da Justiça, I.P., (...) **a apresentação de propostas** de conceção, desenvolvimento e manutenção das aplicações informáticas (...)",

e o segmento transcrito do **n.º 2**, por:

> "2. *No âmbito das competências referidas no número anterior, o IGFEJ deve comunicar à Comissão* (...), **cabendo à Comissão aprovar as propostas de desenvolvimento das aplicações informáticas apresentadas pelo IGFEJ**, bem como (...)".

b) Por outro lado, como acima se referiu, em conformidade com os regimes de protecção de dados, o IFGEJ é considerado subcontratante em relação às entidades responsáveis pelo tratamento de dados indicadas no artigo 24º da lei nº 34/2009.

Com efeito, «Responsável pelo tratamento» nos termos da Diretiva, de forma mais restritiva que no Regulamento, é "Uma **autoridade pública competente**, ou qualquer outro organismo ou entidade designados pelo direito de um Estado-Membro para exercer a **autoridade pública e os poderes públicos "para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública"**.

Por sua vez, nos termos definidos, quer pelo Regulamento (artigo 4.º), quer pela Diretiva (artigo 3.º), «Subcontratante» [é] uma pessoa singular ou coletiva, a

autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

O artigo 22º da Diretiva, cuja transposição é objeto da Proposta de lei nº 125XIII, prevê várias obrigações do subcontratante em relação ao responsável pelo tratamento, no sentido deste poder cumprir as suas obrigações de protecção dos dados, designadamente as que são sua obrigação exclusiva; obrigações semelhantes são estabelecidas nos artigos 28.º e 29.º do Regulamento.

Neste contexto, considerando que na lei nº 34/2009 são atribuídas determinadas competências ao IGFEJ, no âmbito do tratamento de dados, deverá ser aditado um preceito que pelo menos consagre as obrigações correspondentes ao artigo 28º e 29.º do Regulamento e artigo 22º da Diretiva, designadamente que:

- Só aja de acordo com as instruções do responsável pelo tratamento;
- Preste assistência ao responsável pelo tratamento por todos os meios adequados de modo a assegurar o cumprimento das disposições relativas aos direitos do titular dos dados;
- Disponibilize ao responsável pelo tratamento as informações necessárias para demonstrar o cumprimento do disposto no presente artigo;

Ou, em alternativa, um preceito que remeta para a previsão da lei que transpõe a Diretiva para o direito nacional [Proposta de Lei n.º 125XIII-3ª]:

> **Para efeito do disposto nos regimes de protecção de dados, o IFGEJ é considerado subcontratante em relação às entidades responsáveis pelo tratamento de dados indicadas no artigo 24º da presente lei, sendo-lhe aplicável com as devidas adaptações o disposto nos artigos 23º e ss. da lei n.º [Proposta de Lei n.º 125XIII-3ª].**

VII - Interoperabilidade com outros sistemas – acesso ao sistema da UIF e da "UIP"

A proposta de lei, em alteração do artigo 37º da lei nº 34/2009, vem aditar à lista de sistemas com susceptibilidade de interoperabilidade constante do **n.º1** desse preceito, entre outros, os sistemas das ***"Unidades de Informação Financeira e de Informações de Passageiros"*** (conforme alínea *t*), do artigo 37.º, na redacção da proposta).

Ao mesmo tempo, em alteração ao artigo 38.º, a proposta de lei vem alargar o acesso a esses sistemas, até agora circunscrito aos *magistrados e funcionários de justiça que os coadjuvam*, de modo que também "(...) *os administradores judiciais provisórios, os administradores de insolvência e os agentes de execução podem aceder aos dados constantes dos sistemas referidos (...) para fins de identificação, localização ou contacto atualizados (...):*

a) De quaisquer intervenientes em processos jurisdicionais e da competência do Ministério Público;

b) Da situação processual dos arguidos em processo penal;

c) De bens".

Resulta assim da conjugação do artigo 37.º, alínea *t*), com o disposto no artigo 38º, alínea *c*) da lei nº 34/2009, na redação dada pela proposta de lei, que **os administradores judiciais provisórios, os administradores de insolvência e os agentes de execução podem aceder aos dados constantes do sistema da Unidade de Informação Financeira para fins de identificação e localização de bens**.

Ora, a Unidade de Informação Financeira (UIF) trata um alargado conjunto de dados financeiros e outros, que se mostrem relevantes para a prevenção e o combate ao branqueamento de capitais e ao financiamento do terrorismo, nos termos da Lei nº 83/2017, de 18 de agosto, que estabelece medidas de natureza preventiva e repressiva de combate ao branqueamento de capitais e ao financiamento do terrorismo.

Os dados são recolhidos pelas "*entidades obrigadas*" (artigo 57.º, nº 2) tendo como "***finalidade exclusiva*** *a prevenção do branqueamento de capitais e do financiamento do terrorismo, não podendo tais dados ser posteriormente tratados, com base na presente lei, para quaisquer outros fins ...*".

A UIF (como "autoridade competente") trata esses dados pessoais, nos termos do artigo 106.º (cf. n.º 2), da referida lei "**para fins de prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo, (...)**".

Afigura-se assim **desproporcionado e incompatível com a finalidade da recolha**, o acesso a esse sistema da UIF, pelo menos, quando atribuído aos administradores judiciais provisórios, aos administradores de insolvência e aos agentes de execução para fins de identificação e localização de bens.

O mesmo acontece com o acesso aos dados tratados pela "Unidade de Informações de Passageiros", certamente, a unidade nacional de Informações de passageiros prevista na citada Diretiva (UE) 2016/681, do Parlamento e do Conselho, de 27 de abril de 2016, relativa à utilização dos **dados dos registos de identificação dos passageiros** (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, para cuja transposição foi recentemente apresentada a Proposta de lei nº 137/XIII.

Por esta unidade serão tratados 19 categorias de dados, entre eles, "todas as informações sobre as modalidades de pagamento...", mas nos termos do n.º2 do artigo 1.º, "**os dados PNR recolhidos nos termos da diretiva só podem ser tratados para fins de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave**".

Estes dois exemplos são suficientemente explícitos para se concluir pela necessidade de **reponderar a proposta de redação dos artigos 37.º e 38.º**, porquanto, se por um lado introduz, para todos os sistemas, uma **indiscriminada exigência de intervenção prévia** da autoridade nacional de controlo (porventura não justificável para alguns dos sistemas constantes da lista), por outro, admite

indiscriminadamente o **acesso a sistemas com dados pessoais para efeitos não compatíveis com as finalidades** para que foram recolhidos e por entidades que nenhuma relação têm com as atribuições para cujo exercício foi legalmente autorizada a recolha.

VIII - Outros aspectos de melhoria da proposta de lei

- **Artigo 1º nº 1**

Relativamente ao Artigo 1º nº 1, consideramos que a terminologia utilizada nas alíneas a), b) e c), não é a adequada quando se refere "**A recolha e o tratamento** de dados...".

Com efeito, a recolha é uma das operações de tratamento de dados, conforme consta do artigo 4.º do Regulamento (UE) 679/2016 e, de forma coincidente, no artigo 3º da Diretiva (UE) 680/2016, sob a epígrafe "Definições":

> «Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como **a recolha**, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

Assim, no contexto daquele preceito que define o "Objeto" da lei nº 34/2009, para adoção de uma técnica legislativa que vá de encontro à terminologia técnica utilizada nos normativos europeus, **sugerimos a eliminação da referência autónoma à "recolha"** fazendo-se apenas menção ao "tratamento dos dados necessários...".

Ou, se algum interesse se descortinar em sublinhar a referência àquela operação de tratamento de dados, então será de substituir a expressão constante da

proposta de lei pela expressão mais adequada: "**A recolha e demais operações subsequentes de tratamento de dados...**"

Apesar de eminentemente terminológica, esta alteração é de significativa importância, não só para que no âmbito da legislação nacional se tenha um respaldo correto das definições adotadas com o objetivo primordial de harmonizar a legislação em matéria de proteção de dados em todos os Estados Membros, mas também, para que se inclua e enquadre a recolha nos princípios de tratamento de dados pessoais, designadamente o princípio da minimização, posto que é precisamente nesse primeiro momento, da recolha, que se incumpre, as mais das vezes, com as bases de licitude do tratamento de dados pessoais ao obter dados que não são necessários ou que não têm uma finalidade específica que tornem o seu tratamento licito.

Pela mesma ordem de razões, é também de assinalar que **deixa de fazer sentido a alínea d),** cujo teor ["*d) O registo e o tratamento dos dados referidos nas alíneas a), b) e c);*"], corresponde à versão original em vigor da lei nº 34/2009, acrescida de "... e tratamento".

Se é certo que na versão original em vigor, a referência ao "registo" era necessária, uma vez que as mencionadas alíneas a), b) e c) respeitavam apenas à operação de "recolha", com a nova [proposta de] lei todas as operações passam a estar incluídas no conceito de "tratamento".

Mutatais mutandis, o que ocorre com a alínea d), ocorre também com as alíneas f), g) e h), pelo que deverão ser eliminadas, pois não sendo viável discriminar todas as operações em que o tratamento de dados se desdobra, afigura-se contraproducente discriminar apenas algumas.

- **Artigo 1º nº 2**

Este preceito começa por referir que "A presente lei "complementa o disposto ..." no Regulamento e na lei que transpõe a Diretiva.

Ora, esta lei não "**complementa**", no limite concretiza, define ou adequa, de acordo com o previsto nos restantes diplomas comunitários e nacionais, nomeadamente na Directiva (UE) 680/2016 e no Regulamento (UE) 679/2016.

O preciosismo técnico é particularmente relevante no que respeita ao Regulamento, na medida em que a principal diferença entre o Regulamento e uma Diretiva reside precisamente no facto do primeiro ter aplicabilidade direta em todos os Estados Membros, enquanto a segunda carece de transposição para os ordenamentos jurídicos internos.

Afigura-se aquela terminologia desadequada, por equívoca, pois inculca a ideia de que esta lei estabelece um regime complementar, portanto apenas subsidiariamente aplicável, quando se trata efectivamente de um regime especial, aplicável em primeira linha ao tratamento de dados no sistema judiciário, dentro da margem de manobra que o Regulamento e a Directiva deixam ao legislador nacional.

Sugere-se que em vez de "A presente lei complementa o disposto... ", seja usada a expressão:

> **"A presente lei concretiza e adequa ao tratamento de dados no âmbito da actividade judiciária o disposto..."**

- **Artigos 17º e 18º**

Referindo-se, estes preceitos, ao tratamento de dados de outros sujeitos processuais e de testemunhas, importa indagar da necessidade de recolha de determinados dados pessoais destes sujeitos, designadamente, o número da **telecópia**.

Apenas devem ser recolhidos os dados estritamente necessários à prossecução da finalidade dessa recolha. Nesse sentido, sempre que se pretenda elencar os dados pessoais a serem tratados licitamente neste âmbito, deve averiguar-se qual a sua real necessidade em concreto. Caso contrário, estaremos a afrontar o corolário do princípio da minimização que se quis erguer nesta sede.

- **Artigo 40º nº 3 e Artigo 42º nº 2**

Estes preceitos mantêm a referência a "responsável pela gestão dos dados" (mantendo a redacção da Lei 34/2009).

Não nos parece a terminologia correcta. Sugerimos substituição por "**responsável pelo tratamento**".

Além disso, o **nº 2 do artigo 42.º** prevê que para o registo electrónico referido no n.º 3 do artigo 29.º deve ser "periodicamente comunicado" aos responsáveis (...).

Por razões de segurança e confidencialidade o registo não deverá ser "periodicamente comunicado", mas sim, estar acessível ao responsável pelo tratamento para poder exercer as suas responsabilidades, pelo que se sugere a alteração da segunda parte do preceito para:

> **"(...), devendo esse registo estar permanentemente disponível ao responsável pelo tratamento dos dados, para efeitos de auditoria aos acessos e demais operações de tratamento".**

- **Artigo 45.º**

O n.º 2 do artigo 45.º da lei n.º 34/2009 faz referência às alíneas *a)* e *b)*, do nº 1 do artigo 25.º, o que deixou de fazer sentido no texto da proposta de lei, pelo que deverá ser corrigido para passar a indicar as disposições correspondentes.

- **Artigo 46º nº 1, da lei n.º 34/2009**

Para a utilização de uma linha terminológica idêntica nos vários diplomas que regulam as matérias de proteção de dados pessoais, sugere-se o emprego da expressão **"dados anonimizados"** em substituição de **"de forma não nominativa"**.

Este preciosismo terminológico encontra guarida no facto de, para as finalidades estatísticas, ser possível reduzir (ou mesmo eliminar) o risco de tratamento desnecessário de dados pessoais, pois sendo eles anonimizados, deixam de ser considerados dados pessoais. Isto é, através de um processo de anonimização, que nunca afetará as finalidades de utilização estatística, será possível eliminar as referências pessoais que permita identificar uma pessoa singular; sendo esta dissociação efetuada de forma irreversível, ou seja, que não mais permite a agregação, estamos precisamente perante um processo de anonimização.

CONCLUSÕES:

1ª – O regime estabelecido como objecto da lei nº 34/2009, no seu artigo 1º, deverá ser consagrado "sem prejuízo dos textos legislativos que prevêem **outras disposições específicas em matéria de tratamento de dados pessoais"**, salvaguardando, designadamente, o tratamento de dados pelas autoridades judiciárias e órgãos de polícia criminal "para fins de prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo", em conformidade com a Lei nº 83/2017, de 18 de agosto, bem como o tratamento dos dados PNR recolhidos nos termos da Diretiva (UE) 2016/681, para fins de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave;

2ª – A aplicação do regime da Lei nº 34/2009 ao tratamento efectuado pelos **órgãos de polícia criminal**, no âmbito de funções de coadjuvação e de execução de decisões autoridades judiciárias, deve ser clarificada no que respeita à remissão feita **no n.º 5 do artigo 2.º** para as respectivas leis de organização, introduzindo no

preceito a expressa ressalva dessa aplicação: "Sem prejuízo da aplicação das regras estabelecidas na presente lei, as demais especificações relativas aos dados (...) constam das leis de organização dos órgãos, serviços e entidades respetivas";

3ª – Por compatibilidade com a noção de **responsável pelo tratamento** prevista no Regulamento e na Diretiva, segundo a qual, «responsável pelo tratamento» é quem "determina as finalidades e os meios de tratamento de dados pessoais", e face ao regime próprio de responsabilidade conforme disposto nos artigos 12º e ss., da Lei n.º 67/2007, de 31 de dezembro, relativa ao regime da responsabilidade civil extracontratual do estado e demais entidades públicas, não deverão os magistrados ser nomeados responsáveis "para efeitos do disposto nos regimes de proteção de dados pessoais", sem prejuízo das suas competências relativamente à protecção de dados nos termos da lei do processo, alterando-se nos termos do ponto III supra, os **números 1 e 2 do artigo 23.º**.

4ª – A definição e atribuições da **autoridade de controlo**, nos termos da proposta de lei para o **artigo 44.º** da lei n.º 34/2009, merece uma reflexão ponderada para cabal cumprimento dos imperativos da Diretiva concretizados no seu artigo 45.º, nº 2, bem como do Regulamento, nomeadamente explicitados no seu Considerando (20), em apelo da garantia da independência do poder judicial no exercício da sua função jurisdicional, no sentido de confiar o controlo de tais operações de tratamento de dados **a organismos específicos no âmbito do sistema judicial**.

5ª – A **Comissão** de Coordenação da Gestão da Informação do Sistema Judiciário, pela sua composição e sede não cumpre o requisito de independência, nem a exigência de "*organismo específico no âmbito do sistema judicial*", pelo que deverão ser-lhe conferidas as funções de coordenação e articulação, a que correspondem as alíneas a), b), d) e f), do artigo 25.º, **devendo ser excluídas as atribuições das alíneas c), e), g), h) e i), do artigo 25.º**, bem como o acesso aos dados das pesquisas previsto no **n.º 3 do artigo 38º** e a comunicação imediata de qualquer acesso irregular prevista na **alínea e), nº 2 do artigo 29.º**, por serem reservadas

aos responsáveis pelo tratamento e à respectiva autoridade de controlo competente.

6ª – O disposto nos **números 1 e 2 do artigo 26.º** deverá ser harmonizado com o disposto no artigo 25.º, no que respeita às competências relativas da Comissão de Coordenação da Gestão da Informação do Sistema Judiciário e do Instituto de Gestão Financeira e Equipamentos da Justiça, I.P., quanto à apresentação de propostas para o desenvolvimento e manutenção aplicacional, corrigindo-se os segmentos assinalados no ponto VI-a) supra;

7ª – Face aos regimes de protecção de dados e especialmente da Diretiva, no que respeita à nomeação do responsável pelo tratamento de dados e à sua relação com o **subcontratante** e considerando que na lei nº 34/2009 são atribuídas determinadas competências ao Instituto de Gestão Financeira e Equipamentos da Justiça, I.P. no âmbito do tratamento de dados, deverá ser aditado um preceito que encarregue aquele Instituto de cumprir em relação ao responsáveis pelo tratamento pelo menos as obrigações correspondentes ao artigo 22º da Diretiva, nos termos do ponto VI-b) supra;

8ª – No domínio da interoperabilidade e acesso a outros sistemas, deve ser reponderada a proposta de redação dos **artigos 37.º e 38.º**, porquanto, se por um lado introduz, para todos os sistemas, uma indiscriminada exigência de intervenção prévia da autoridade nacional de controlo (porventura não justificável para alguns dos sistemas constantes da lista), por outro, admite indiscriminadamente o acesso a sistemas com dados pessoais para efeitos **não compatíveis com as finalidades para que foram recolhidos** e por entidades que nenhuma relação têm com as atribuições para cujo exercício foi legalmente autorizada a recolha, conforme se explicita no ponto VII supra;

9ª – Pelo menos **deve ser impedido o acesso**, pelos administradores judiciais provisórios, administradores de insolvência e agentes de execução, para fins de identificação e localização de bens, ao sistema da Unidade de Informação Financeira, que é autorizado pela Lei nº 83/2017, de 18 de agosto, "para fins de

prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo", bem como ao sistema da Unidade de Informações de Passageiros, de tratamento dos dados PNR, a recolher nos termos da Diretiva (UE) 2016/681 (proposta de lei n.º 137XIII) "para fins de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave";

10ª - Pelas razões e nos termos para cada um especificados no ponto VIII supra, sugerem-se alterações nos seguintes preceitos: artigo 1º nº 1, artigo 1º nº 2, artigos 17º e 18º, artigo 40º nº 3 e artigo 42º nº 2, artigo 45.º, e artigo 46º nº 1, da lei n.º 34/2009.

Lisboa, 15 de junho de 2018

António Gameiro, Pedro Marinho Falcão, Rui Moreira, António Moreira (relator)

Luís Pais de Sousa (Presidente)