

Proc.7352 /2010

Parecer nº 62 /2010

O Ministério dos Negócios Estrangeiros, através do Senhor Director-Geral da Política Externa, veio solicitar à CNPD a emissão de parecer sobre o projecto de Acordo a celebrar entre Portugal e os Estados Unidos da América para a troca de informação de rastreio do terrorismo (*Terrorism Screening Information*), e dos respectivos instrumentos para o seu cumprimento: um que regula os procedimentos práticos para a troca de informações e um outro relativo aos pontos de contacto das Partes.

O texto submetido à apreciação da CNPD não se encontra ainda completo, em particular no que diz respeito às autoridades portuguesas envolvidas no âmbito do acordo. Não foi remetida qualquer documentação complementar.

Nos termos da alínea a) do nº 1 do artigo 23º da Lei 67/98, de 26 de Outubro, a CNPD é competente para a emissão do respectivo parecer, na medida em que o Acordo prevê o tratamento de dados pessoais.

O projecto de Acordo

No preâmbulo do projecto de Acordo (doravante designado por Acordo), afirma-se que os esforços conjuntos das partes para prevenir e lidar com o terrorismo internacional devem abranger a cooperação na identificação atempada de indivíduos conhecidos por estarem, ou terem estado, envolvidos em actividades que constituem terrorismo, seja na sua preparação, auxílio ou relacionadas com

actividades terroristas. Tal cooperação deve incluir a partilha de informação de rastreio relativa a «terroristas conhecidos».

Pretende-se, pois, estabelecer procedimentos adequados para o acesso e o intercâmbio desta informação, de modo a reforçar a capacidade das Partes de se protegerem contra actos de terrorismo.

É ainda declarado que o presente Acordo respeita os direitos fundamentais das pessoas.

É objecto do presente Acordo (artigo I) o estabelecimento do quadro legal aplicável às Partes na sua cooperação, tendo como finalidade a partilha e utilização de informação de rastreio do terrorismo (*terrorism screening information*), oriunda de serviços de informações ou de forças policiais, em conformidade com as respectivas legislações nacionais e com o Direito Internacional aplicável.¹

A definição de informação de rastreio do terrorismo consta do artigo II do Acordo, significando a informação de identificação, não classificada, sobre terroristas conhecidos. Esta última designação – *known terrorist* – é igualmente definida como a pessoa condenada ou constituída arguida por crime relacionado com o terrorismo ou com a actividade terrorista².

Constam ainda do elenco do artigo II, entre outras, as definições de *background information*: informação adicional além da informação relativa ao rastreio do terrorismo; e de *relevant authority*: qualquer autoridade policial, de imigração, de informações e segurança pública das Partes. No caso de Portugal, a listagem de autoridades competentes está prevista, mas ainda não inserida no texto do Acordo. No caso dos EUA, pode ser qualquer autoridade governamental federal, estadual,

¹ Na versão em Inglês (a única facultada à CNPD): «*The present Agreement establishes the legal framework applicable between the Parties in their cooperation in the sharing and use of terrorism screening information derived from intelligence and law enforcement information, in accordance with their domestic laws and the applicable International Law*» (artigo I)

² «*“Known terrorist” means a person convicted of a crime related to terrorism or terrorist activity or charged with or indicted for a crime related to terrorism or terrorist activity according to the respective domestic laws in force*» (alínea h) do artigo II)

local, territorial ou tribal, cujos alguns agentes podem ter acesso a informação fornecida ao abrigo do Acordo para alcançar os fins nele previstos.

Nos termos do Acordo, as Partes concordam em fornecer entre si acesso a informação de rastreio do terrorismo, que compreende os seguintes dados pessoais: nome completo, data de nascimento, número de passaporte ou de outro documento de identificação e a nacionalidade actual e anterior, se conhecida. Se permitido por lei e por decisão da Parte transmissora dos dados, podem ainda ser disponibilizados quaisquer outros dados identificativos, incluindo impressões digitais. Não serão partilhadas informações classificadas no âmbito deste Acordo nem ele impõe restrições à troca de informações realizada no âmbito de outros instrumentos já existentes.

O Acordo prevê ainda procedimentos para os casos em que as autoridades se deparem com pessoas que potencialmente possam corresponder à informação de rastreio do terrorismo fornecida pela outra Parte (*encounters*). Tais procedimentos específicos, bem como a troca de informação que lhes está subjacente, constam de Instrumento autónomo de implementação do Acordo (doravante designado por Instrumento).

Nos termos desse Instrumento, quando um indivíduo for positivamente identificado, há lugar à troca adicional de informação. A Parte autora da informação transmite à outra Parte informação de *background*; e, em sentido contrário, a Parte receptora da informação transmite informação recolhida durante o encontro.

Estes dados podem incluir fotografias, impressões digitais, cópias de qualquer material recolhido junto da pessoa (documentos, etc.), cópias de dados escritos, qualquer informação fornecida pela pessoa ou outros dados de «interesse potencial», tais como as identidades dos companheiros de viagem ou associados.

No que diz respeito às categorias de titulares dos dados, a troca de informação não é equivalente entre as Partes.

Os EUA fornecerão informação sobre: sujeitos considerados ameaças à aviação civil, sujeitos considerados operacionalmente capazes de cometer um acto terrorista, sujeitos conhecidos por serem terroristas para os quais há um mandado de detenção

federal activo e sujeitos conhecidos por serem membros de uma organização terrorista e associados a actividade terrorista.

Portugal fornecerá informação sobre sujeitos condenados ou constituídos arguidos por crime relacionado com o terrorismo ou actividade terrorista, de acordo com a lei nacional vigente.

O presente Acordo prevê que o intercâmbio de dados pessoais entre as Partes seja feito através de entidades e pontos de contacto previamente definidos. Por parte de Portugal, não consta ainda no texto do Acordo qual a entidade/autoridade com a qual serão trocados os dados. Por parte dos EUA, será o *Terrorism Screening Center* (TSC) a receber e a fornecer informação.

Apreciação

O Acordo agora em análise envolve o tratamento de dados pessoais para fins policiais, o que desde logo se reveste de uma importância acrescida, considerando o impacto que tal pode ter nos direitos, liberdades e garantias das pessoas. Por outro lado, implica o fluxo internacional de dados para um país terceiro.

À luz da Lei de Protecção de Dados (LPD), a transferência de dados pessoais para um Estado que não pertença à União Europeia «*só pode realizar-se com o respeito das disposições da presente lei e se o Estado para onde são transferidos assegurar um nível de protecção adequado*» (nº 1 do art. 19.º da Lei 67/98, de 26 de Outubro).

A Decisão-Quadro 2008/977/JAI do Conselho, de 27 de Novembro de 2008, relativa à protecção de dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, também dispõe, no seu artigo 13.º, como uma das exigências para a transmissão de dados a Estados terceiros que esse Estado assegure um nível de protecção adequado.

Por último, também o Protocolo Adicional à Convenção 108³, do Conselho da Europa, assinado e ratificado por Portugal, estipula que a transferência de dados pessoais para um Estado que não é parte na Convenção apenas poderá realizar-se se esse Estado assegurar um nível de protecção de dados adequado (nº 1 do art. 2.º).

Importa, pois, antes de mais, aferir da adequação do nível de protecção de dados oferecido pelos Estados Unidos da América, destinatário da informação no âmbito do presente Acordo. Para tal, há que ter em conta, em conformidade com o nº 2 do art. 19.º da LPD, a natureza dos dados, a finalidade e a duração do tratamento, as regras de direito, gerais ou sectoriais, em vigor no Estado em causa e as medidas de segurança respeitadas nesse Estado.

Em primeiro lugar, os EUA não aderiram à Convenção 108, de 28 de Janeiro de 1981, único instrumento internacional que regula o tratamento de dados pessoais, e aberto à assinatura de Estados não-Membros do Conselho da Europa.

Em segundo lugar, os EUA não detêm legislação geral federal em matéria de protecção de dados. O *US Privacy Act*, alterado em 1974, contém apenas algumas disposições parcelares, apenas aplicáveis a entidades públicas, em particular em matéria de confidencialidade e de acesso e rectificação por parte dos titulares dos dados. No entanto, os dados tratados para fins policiais estão excluídos dessa regulação.

Não existe, igualmente, qualquer autoridade independente de controlo, que supervisione o tratamento de dados pessoais.

Pode, pois, concluir-se que os EUA não oferecem um nível de protecção de dados adequado.

O nº 6 do art. 20.º da LPD admite, no entanto, a transferência de dados quando tal constituir medida necessária à prevenção, investigação e repressão de infracções penais, devendo nesse caso o fluxo ser regido «*por disposições legais específicas ou pelas convenções e acordos internacionais em que Portugal é parte*».

³ Protocolo Adicional à Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, respeitante às autoridades de controlo e aos fluxos transfronteiriços de dados, de 8 de Novembro de 2001.

Também o Protocolo Adicional à Convenção 108 e a Decisão-Quadro 2008/977/JAI do Conselho, prevêm que, em derrogação à exigência de adequação de um Estado terceiro, a transferência internacional de dados pessoais se possa realizar, se forem assegurados mecanismos suficientes de garantia de protecção da vida privada e dos direitos e liberdades fundamentais das pessoas.

Tais garantias deverão constar cabalmente do Acordo a ser celebrado entre as Partes, e que as vincula, devendo ser específicas e claras, de modo a criar a indispensável transparência e segurança jurídica.

O Estado Português deverá observar para o efeito o quadro constitucional e outras obrigações legais a que está sujeito, seja ao nível da União Europeia, seja ao nível nacional.

Passemos então à análise pormenorizada do Acordo, a fim de verificar se dele constam os mecanismos suficientes de salvaguarda dos direitos das pessoas em matéria de protecção de dados.

1. Questão prévia

Ao longo do texto do Acordo, é usado o termo “terrorismo/terrorista”, não sendo feita qualquer definição do conceito, que pode naturalmente estar sujeito a interpretações diferenciadas, o que teria sérias implicações ao nível da abrangência dos dados tratados.

Do mesmo modo, a designação de “relacionado com terrorismo/actividade terrorista” não está definida no Acordo. Em particular, estando em causa crimes concretos, é essencial que as Partes tenham o mesmo entendimento do significado e alcance dos termos usados.

Nessa medida, deve o Acordo incluir uma definição de “terrorismo” e de crimes “relacionados com terrorismo/actividade terrorista”. Sugere-se, a esse propósito, por uma questão de economia, e se for do entendimento de ambas as Partes, a simples

referência à noção de “terrorismo”, constante do art. 1.º da Decisão-Quadro 2002/475/JAI, de 13 de Junho de 2002, relativa à luta contra o terrorismo⁴, e à noção de “actividade relacionada”, descrita nos artigos 2.º e 3.º da mesma Decisão-Quadro.

2. Do responsável pelo tratamento

Os responsáveis pelo tratamento de dados, no âmbito deste Acordo, serão as entidades indicadas como pontos de contacto para a implementação do Acordo.

É imprescindível que sejam autoridades com competência, a nível da sua legislação interna, para a prevenção, investigação, detecção e repressão de infracções penais, tendo em conta a finalidade do Acordo e a natureza dos dados.

Da parte de Portugal, o texto do Acordo não identifica ainda qual será a autoridade responsável pela comunicação e utilização da informação, pelo que não nos poderemos pronunciar.

Da parte dos EUA, é indicado o *Terrorism Screening Center* (TSC)⁵, uma autoridade criada em 2003, no seguimento da Directiva Presidencial de Segurança Interna 6, de 16 de Setembro de 2003, e que funciona no âmbito do *Federal Bureau of Investigation* (FBI).

O TSC é responsável pela chamada “Terrorist Watchlist” (*Terrorist Screening Data Base*), que pretende coordenar e centralizar no plano nacional toda a informação identificativa de terroristas conhecidos ou suspeitos, para apoio de outras agências governamentais que procedem, na linha da frente, ao rastreio de terroristas, designadamente aquando da obtenção de vistos, controlo de fronteiras, embarque aéreo, imigração e aquisição de nacionalidade.

⁴ JOL 164/3 de 22.6.2002

⁵ <http://www.fbi.gov/about-us/nsb/tsc/tsc>

Nesse sentido, o TSC recolhe informação em várias agências norte-americanas e em países estrangeiros, que depois partilha de volta, a fim de ser possível verificar se um determinado indivíduo consta da lista de terroristas.

Nesta medida, o TSC é uma autoridade competente para o tratamento dos dados pessoais, trocados no âmbito do Acordo.

Importa precisar, de todo o modo, que a transmissão, a nível interno, das informações obtidas não deve ser regida pelo mero critério do «*need-to-know*» (art.VIII n.º 1), mas sim obedecer ao mais exigente princípio da proporcionalidade, aliás consagrado no art. III para as transferências internacionais.

Ainda a este propósito, importaria eliminar a expressão «*other than name (...) or citizenship*», no n.º 3 do artigo VIII, pois também em relação aos dados aí contemplados se justificaria a restrição constante dessa norma.

3. Da finalidade do tratamento

A finalidade do tratamento não é claramente especificada no texto do Acordo. Com efeito, apenas o preâmbulo do Acordo se refere genericamente ao objectivo de identificar indivíduos conhecidos pela sua participação directa ou indirecta em actividades terroristas, não sendo explícito o fim que se pretende alcançar com essa identificação.

O objecto do Acordo remete apenas para a partilha e utilização de determinado tipo de informação (*terrorist screening information*), não estando claro qual a sua finalidade. Só lendo o site oficial do TSC tal se torna mais evidente.

Deve, por isso, o Acordo determinar a finalidade específica do tratamento dos dados, o que se torna indispensável para apurar das condições de legitimidade do tratamento bem como da sua proporcionalidade.

Na verdade, este Acordo parece pressupor a transmissão de grandes volumes de dados, sob a forma de listagens de pessoas, e não na troca de informação concreta

relativamente a uma pessoa em particular, baseada num caso ou numa investigação concreta, o que levanta sérias dúvidas quanto à sua proporcionalidade.

Na perspectiva do regime jurídico português, apenas uma transferência concreta, caso a caso, respeitaria devidamente a exigência da proporcionalidade, um dos princípios básicos da protecção de dados pessoais.

Deve, por isso, a troca de informações prevista no Acordo basear-se na necessidade concreta da investigação criminal de cada uma das Partes e não num quadro de partilha generalizada de dados pessoais, em forma de listagens, claramente excessivas.

Ainda no que diz respeito ao princípio da finalidade, o Acordo prevê, na alínea a) do art. 3.º a possibilidade de tratamento de dados posterior para outras finalidades não incompatíveis, que não são, no entanto, explicitadas.

Esta redacção é demasiadamente abrangente, desconhecendo-se quais os critérios de avaliação para determinar o uso compatível ou não dos dados.

Deve, assim, o texto ser reformulado de modo mais restritivo e específico, e deve incluir a obrigação de solicitar consentimento prévio escrito à Parte que transmitiu os dados antes de qualquer utilização para outras finalidades, devendo o pedido de consentimento ser fundamentado e explicitar qual a finalidade pretendida. O consentimento também deverá ser dado por escrito.

4. Das categorias de dados

Embora o Acordo se refira sempre a dados de identificação (*identifying information*), o que por si só caberia numa única categoria de dados, a verdade é que são tratados outros dados pessoais além dos que permitiriam estritamente proceder à identificação de uma pessoa.

Desde logo, sendo transmitidos dados relativos a diferentes categorias de pessoas, presume-se que a informação relacionada com as diferentes categorias de titulares,

bem como dados relativos às diferentes situações são igualmente objecto de tratamento.

No entanto, a extensão dos dados tratados não está suficientemente inscrita no texto do Acordo ou é omissa.

No n.º 3 do art. IV do Acordo, são elencados dados específicos que se prendem com a identificação das pessoas (nome completo, data de nascimento, n.º de passaporte ou de outro documento de identificação e nacionalidade actual e anterior).

No n.º 4 do mesmo artigo, admite-se a comunicação de outros dados «de identificação» disponíveis, apenas se explicitando as impressões digitais.

Já nos números 4.b e 5 do Instrumento, está previsto o tratamento de outras categorias de dados pessoais, designadamente informação de *background* e o nível de ameaça que um indivíduo pode representar.

Na realidade, se nuns artigos, as categorias de dados estão bem definidas, noutros são extremamente vagas, como é o caso da definição de *background information* (art. II do Acordo), que significa qualquer informação adicional além da informação de rastreio.

A omissão ou generalização dos dados tratados é contrária ao princípio da necessidade, adequação e pertinência e impede a avaliação correcta da proporcionalidade do tratamento e da qualidade dos dados.

Assim sendo, todas as categorias de dados pessoais tratados devem constar, com a maior precisão possível, do texto do Acordo (e não do Instrumento), sugerindo-se que sejam reunidas num artigo autónomo e não dispersas pelo articulado.

5. Das categorias dos titulares

As categorias dos titulares dos dados não constam do Acordo, mas do Instrumento. Resulta do texto uma diferenciação entre as categorias de titulares transmitidas pelos EUA e as transmitidas por Portugal.

Tal facto parece resultar de quadros legais distintos e de, na verdade, não se tratar de uma troca equivalente de informação, na medida em que a informação comunicada aos EUA visa alimentar uma base de dados concreta (*Terrorist Watchlist*), que não tem aqui paralelo, recebendo Portugal acesso a essa lista para efeitos de identificar no seu território pessoas que eventualmente constem da lista norte-americana e agir em conformidade com a informação e as indicações que obtiver nesse âmbito.

Assim, o Instrumento prevê, no seu n.º 1, a transmissão por parte dos EUA de dados relativos a sujeitos considerados uma ameaça à aviação civil; sujeitos considerados operacionalmente capazes de cometer um acto terrorista; sujeitos conhecidos por serem terroristas sobre os quais impende um mandado de detenção activo norte-americano e sujeitos conhecidos por pertencerem a uma organização terrorista e associados a actividade terrorista.

No seu n.º2, prevê-se que Portugal transmita dados relativos a condenados e arguidos por crime relacionado com o terrorismo ou actividade terrorista.

Estas são as categorias de titulares dos dados explicitamente elencadas. No entanto, no n.º 8 do Instrumento, prevê-se igualmente que sejam recolhidos dados de "companheiros de viagem" e de "associados" de pessoa que tenha sido positivamente identificada como constando da lista.

Antes de mais, considera-se que a descrição exaustiva das categorias de titulares tratadas, porque substantiva e não procedimental, deve estar fixada no texto do Acordo e não no Instrumento.

Em segundo lugar, alerta-se para o facto de não resultar, do texto do Acordo ou do Instrumento, qualquer diferenciação entre as diferentes categorias de pessoas, no que diz respeito ao tratamento dos seus dados, designadamente quanto ao grau de fiabilidade da informação, em função da sua fonte e da sua natureza. Com efeito, não parece haver qualquer diferenciação entre informações factuais e informações que podem resultar de avaliações mais ou menos objectivas.

De acordo com a Recomendação R (87) 15 do Comité de Ministros do Conselho da Europa, que regula o uso de dados pessoais no sector policial, no Princípio 3.2, é

preconizada uma separação entre os dados factuais e os dados baseados em opiniões ou avaliações pessoais.

A este propósito, sublinha-se a definição de «terrorista conhecido» (alínea h) do art. II do Acordo), como sendo uma pessoa condenada ou constituída arguida. Ora, à luz da legislação portuguesa, o princípio da presunção da inocência é um direito fundamental, pelo que a atribuição da qualificação de terrorista (conhecido) a uma pessoa que não tenha sido objecto de uma condenação por esse crime é manifestamente violadora dos princípios que fundam o Estado de Direito.

Face à Constituição portuguesa, e do princípio da presunção da inocência nela consagrado, só quem tenha sido objecto de condenação com trânsito em julgado pelo crime de terrorismo pode ser qualificado de “terrorista”.

6. Da qualidade dos dados

O princípio da qualidade dos dados é basilar no regime de protecção de dados, pelo que os dados transmitidos devem ser rigorosos, completos, actuais, bem como adequados, relevantes e não excessivos em relação à finalidade para que são tratados.

O Acordo contém, no artigo III, normas gerais relativamente a estes princípios, nomeadamente que só serão tratados pelo tempo necessário para a finalidade para que foram recolhidos e posteriormente tratados. Porém, não é definido qualquer prazo máximo de conservação dos dados. Atento o limite temporal indeterminado da *Terrorist Watchlist* norte-americana e do objectivo genérico de rastreio do terrorismo, sempre na perspectiva da prevenção, teme-se que os dados possam ficar indefinidamente naquela base de dados.

O Acordo deveria prever um prazo máximo de conservação dos dados, sem prejuízo de poder ser prorrogado caso os dados se mostrassem efectivamente necessários, o que obrigaria a revisões periódicas da sua relevância e do próprio conteúdo do registo.

Deveriam também ser estabelecidas regras para a fixação de diferentes prazos de conservação, consoante as categorias de dados.

Importa salientar igualmente que, em Portugal, nos termos da legislação que regula a identificação criminal, o registo criminal é cancelado após um determinado período legalmente estabelecido, o que no caso de crimes com sentença superior a 8 anos de prisão é de 10 anos após a extinção da pena, desde que não tenha ocorrido nova condenação⁶, ou após falecimento do titular⁷.

Assim sendo, não deverão os dados pessoais ser mantidos por um Estado terceiro, quando no quadro da legislação nacional eles já não podem ser conservados.

Por outro lado, convém sublinhar a importância do princípio da actualização dos dados e do seu rigor. O artigo VIII do Acordo prevê que a Parte receptora da informação actualize, de forma expedita, os seus registos (rectificação ou eliminação), logo que notificada de alterações, bem como a não utilizar ou a confiar em informação que já tenha sido substituída por outra mais actual.

Ora a actualização prevista é fundamental. Contudo, essa actualização deveria suprimir o histórico de informações desactualizadas, sem prejuízo da manutenção de registos para efeitos de auditoria, por um período de tempo limitado, separados da restante informação. Deste modo, se garantiria que não era utilizada informação errónea.

O Acordo deve pois prever mecanismos que obriguem as partes a eliminar os dados, por força do seu direito nacional, sob pena de violação dos direitos e liberdades dos cidadãos.

⁶ Cfr. alínea a) do n.º 1 do artigo 15.º da Lei 57/98, de 18 de Agosto, com as alterações introduzidas pela Lei 114/ 2009, de 22 de Setembro.

⁷ Cfr. n.º 4 do mesmo artigo.

7. Das transmissões subsequentes de dados

No contexto de transmissões subsequentes de dados, que está presente neste Acordo, pois o TSC partilha informação da sua base de dados com várias agências governamentais norte-americanas e com países estrangeiros, a qualidade dos dados assume uma especial importância.

Nesse sentido, o Acordo deve conter garantias que obriguem as Partes a retransmitir todas as actualizações de dados introduzidas em registos anteriormente disponibilizados, incluindo a eliminação dos dados.

De igual modo, quaisquer restrições ao tratamento de dados, por força do direito interno da Parte fornecedora da informação, devem ser comunicadas a todas as entidades às quais vão ser subsequentemente transmitidos os dados.

Estas obrigações devem constar de eventuais acordos, no âmbito do rastreio do terrorismo, que as Partes venham a celebrar com terceiros países.

8. Dos direitos dos titulares

Os direitos dos titulares dos dados, em particular o direito de acesso, de rectificação e de eliminação, não estão de todo consagrados no presente Acordo.

O artigo VIII, nº 2 alínea c) parece, mesmo, pretender derrogar o direito de acesso.

O texto, no seu artigo XI, apenas prevê a possibilidade de se estabelecerem procedimentos para «apresentar queixas relativas ao rastreio», em qualquer dos países, que serão encaminhadas e tratadas após consulta entre as Partes, e das quais poderão resultar rectificações aos dados pela Parte que transmitiu a informação.

A «queixa» deverá ser acompanhada de cópia de um documento de identificação, como o passaporte ou outro documento de identidade emitido pelas autoridades governamentais, que contenha fotografia, nome completo, data de nascimento e nacionalidade.

O titular dos dados não pode receber qualquer informação sobre as diligências tomadas nem que a «queixa» foi reencaminhada para a outra Parte, assim como nem está prevista qualquer resposta a dar ao queixoso.

De acordo com informação disponibilizada pelo TSC, no seu *website*, as queixas das pessoas dizem respeito sobretudo a problemas e demoras em verificações no controlo de fronteiras, o que as autoridades norte-americanas atribuem a coincidências na informação de identificação, sem nunca revelar qual a autoridade responsável pelo tratamento dos dados.

O Acordo prevê ainda que cada Parte deve assegurar que o titular dos dados tem acesso a recurso judicial e à possibilidade de procurar uma compensação legal, no caso de violação dos seus dados pessoais.

Todavia, o direito interno dos EUA só aceita a interposição de acções judiciais nos seus tribunais por parte de cidadãos norte-americanos ou que ali residam em permanência. Desta forma, a menos que o Acordo claramente o preveja, fica excluída a possibilidade de pessoas que se considerem lesadas nos seus direitos conseguirem uma responsabilização do Estado norte-americano – o que se não afigura aceitável.

Anote-se, a propósito, que o teor do artigo XII, nº 2 do Acordo parece introduzir grande ambiguidade a esse respeito.

Por outro lado, apesar das limitações inerentes ao exercício do direito de acesso, rectificação e eliminação, no âmbito do tratamento de dados policiais, e que estão consagradas na LPD (artigo 11.º n.ºs 2 e 4), na Decisão-Quadro 2008/977/JAI do Conselho, de 27.11.2008 (artigo 17.º) e no Princípio 6 da Recomendação do Conselho da Europa já mencionada, tais direitos não podem ser liminarmente excluídos.

Acrece ainda que são direitos fundamentais, consagrados na Constituição da República Portuguesa (n.º do artigo 35.º), não podendo nessa medida Portugal aceitar a supressão de tais direitos e garantias num acordo internacional.

A possibilidade de uma pessoa apresentar uma queixa não substitui o exercício dos direitos que legalmente lhe assistem.

A LPD prevê o exercício do direito de acesso de forma indirecta, através da CNPD, que, como autoridade independente, faz as verificações necessárias, de modo a apurar da conformidade legal do tratamento de dados, designadamente a aferir se houve um erro de facto passível de rectificação ou um erro de direito, passível de eliminação.

Ainda nos termos da LPD, não serão comunicados quaisquer dados aos titulares que possam prejudicar a segurança do Estado, a prevenção ou a investigação criminal.

Neste sentido, o Acordo deve ser reformulado, no sentido de incluir, com as limitações inerentes à finalidade do tratamento, todos os direitos e garantias a que a Constituição obriga.

Caberia aos EUA definir, no âmbito do seu direito interno, que entidade independente poderia, nesta matéria, desempenhar papel correspondente ao da CNPD.

9. Da segurança das informações

O artigo IX do Acordo é muito vago e contido no tocante às medidas de segurança das informações.

As mais importantes medidas deveriam ser concretizadas no próprio Acordo, para não conceder aos Estados demasiada margem de decisão nesta área.

Sugere-se a transposição para o Acordo das exigências, em matéria de segurança, previstas nos artigos 14.º e 15.º da LPD.

10. Cessação do Acordo

Não é evidente a correlação entre o artigo X nº 5 e o artigo XVI nº 3, relativamente à cessação do Acordo e das obrigações dele decorrentes.

À primeira vista – salvo melhor explicitação – essas normas parecem algo contraditórias. Com efeito, por um lado prevê-se a destruição dos dados pessoais após a cessação do Acordo, por outro, a sua manutenção.

Esta é uma questão essencial, pelo que deve estar claramente regulada no artigo sobre as disposições aplicáveis à cessação do Acordo.

Após o termo do Acordo, as informações através dele obtidas deverão ser eliminadas, com salvaguarda dos dados necessários no âmbito de eventual procedimento criminal pendente.

Conclusão

O texto do Acordo deve ser reformulado, de modo a dar satisfação às seguintes questões:

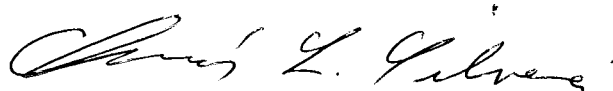
1. Introdução de todas as garantias para o tratamento de dados pessoais, de forma a suprir a ausência de um nível de protecção adequado nos EUA e a criar a indispensável transparência e segurança jurídica;
2. Introdução da noção de terrorismo/actividade terrorista para entendimento cabal das Partes dos crimes e das práticas que lhe estão associados, designadamente por referência à Decisão-Quadro 2002/475/JAI do Conselho, de 13.6.2002;

3. Escolha de uma autoridade portuguesa como responsável pelo tratamento de dados que tenha competência na investigação e repressão de infracções penais;
4. Especificação da finalidade do tratamento de dados realizado no âmbito do Acordo, restrição da utilização dos dados para outras finalidades e inclusão da obrigação de solicitar consentimento prévio escrito antes dessa utilização;
5. Elencar exhaustivamente as categorias de dados tratados no texto do Acordo e não do Instrumento;
6. Descrição de forma completa as categorias dos titulares dos dados no texto do Acordo e não no Instrumento;
7. Previsão da diferenciação dos dados em função da sua natureza factual ou subjectiva, designadamente através de códigos de fiabilidade da informação;
8. Fixação de um prazo máximo de conservação dos dados, sem prejuízo de eventuais prorrogações em função de uma avaliação efectiva da necessidade da sua manutenção;
9. Previsão de uma disposição que obrigue as Partes a eliminar os dados, por força do seu direito nacional;
10. Introdução de mecanismos que obriguem as Partes a informar os destinatários dos dados, em caso de transmissões subsequentes de dados, da actualização da informação anteriormente disponibilizada, de modo a manter os dados rigorosos e actuais;
11. Comunicação aos destinatários subsequentes dos dados de quaisquer restrições impostas ao tratamento de dados pela Parte autora da informação, por força do seu direito interno;

12. Inclusão de regras para o exercício efectivo dos direitos de acesso, rectificação e eliminação, constitucionalmente consagrados;
13. Previsão de mecanismos para o recurso efectivo à via judicial em caso de violação dos direitos das pessoas e consequente responsabilização da Parte em causa;
14. Concretização das medidas de segurança a adoptar;
15. Precisão do regime de cessação do Acordo.

Lisboa, 11 de Outubro de 2010

Ana Roque, Carlos Campos Lobo, Helena Delgado António, Luís Paiva de Andrade e Vasco Almeida



Luís Lingnau da Silveira (Presidente, que relatou)