COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Exmo. Senhor
Dr. Fernando Negrão
Presidente da Comissão de Assuntos
Constitucionais, Direitos, Liberdades e
Garantias
Assembleia da República
Palácio de São Bento
1249 – 068 LISBOA

N/Ref. 02.02
Proc. n. º 3974/2012
Of. n.º 9331 17/04/2012

Assunto: Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais e à livre circulação desses dados.

Com referência ao assunto em epígrafe, venho comunicar a V. Exa. o Parecer desta CNPD n.º 18/2012, proferido em 16 de Abril p. p., cuja cópia se anexa.

Com os melhores cumprimentos.

A Secretária da CNPD,

(Isabel Cristina Cruz)

ASSEMBLEIA DA REPÚBLICA
Divisão de Apoio às Comissões
CACDLG
N.º Único 428537
Entrada/Saída n.º 454 Data: 17/04/12

RC

Rua de São Bento, 148-3º • 1200-821 LISBOA
Tel: 213 928 400 Fax: 213 976 832
geral@cnpd.pt www.cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Processo n.º 3974 /2012

Parecer 18 /2012

A Assembleia da República, através da Comissão de Assuntos Constitucionais, Liberdades, Direitos e Garantias, solicitou à CNPD para se pronunciar sobre a Proposta de Directiva do Parlamento Europeu e do Conselho, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infracções penais ou de execução de sanções penais, e à livre circulação desses dados.[1]

Esta Proposta de Directiva integra, conjuntamente com a Proposta de Regulamento Geral de Protecção de Dados, o novo quadro jurídico proposto pela Comissão Europeia para a protecção de dados pessoais na União Europeia.

A Carta dos Direitos Fundamentais da UE consagra, no seu artigo 8.º, a protecção de dados pessoais como um direito fundamental.

Com a entrada em vigor do Tratado de Lisboa, o direito à protecção de dados pessoais estendeu-se ao domínio da cooperação policial e da cooperação judiciária em matéria penal, por via do artigo 16.º do Tratado de Funcionamento da União Europeia (TFUE), que estabelece que todas as pessoas têm direito à protecção de dados de carácter pessoal que lhes digam respeito, dando simultaneamente uma base jurídica específica para a adopção de regras em matéria de protecção de dados pessoais também nestas áreas, ficando essas normas sujeitas ao controlo de autoridades independentes.

[1] COM (2012) 10 final de 25.1.2012

Devido à natureza específica do domínio da cooperação policial e judiciária em matéria penal, foi reconhecido na Declaração 21[2] anexa ao TFUE que poderão ser necessárias disposições específicas sobre a protecção de dados pessoais e sobre a livre circulação desses dados nestes domínios, razão pela qual é agora apresentada esta Proposta de Directiva como acto jurídico autónomo do Regulamento Geral de Protecção de Dados.

Todavia, apesar das particularidades inerentes ao tratamento de dados pessoais no âmbito da cooperação policial e judiciária em matéria penal, os princípios aplicáveis são os mesmos, aliás já plasmados na Convenção 108[3] do Conselho da Europa e no seu Protocolo Adicional[4], instrumentos internacionais de referência em matéria de protecção de dados, tanto ao nível da UE como dos seus Estados-Membros, ambos ratificados por Portugal, e que já cobrem todos os sectores.

Nessa medida, é essencial que o novo quadro jurídico de protecção de dados da União venha a reflectir no normativo das duas propostas legislativas a coerência e consistência necessárias para garantir um elevado nível de protecção de dados pessoais na UE, garantindo efectivamente a defesa de um direito fundamental.

Em Portugal, a protecção de dados pessoais e da privacidade tem consagração constitucional desde 1976 e o legislador nacional optou por oferecer, na Lei de Protecção de Dados, um âmbito de protecção mais abrangente do que o prescrito pela Directiva 95/46/CE, e no qual já se inclui o tratamento de dados policiais, com as derrogações necessárias à sua natureza específica, mas dando corpo a um regime legal

[2] Declaração 21 sobre a protecção de dados pessoais no domínio da cooperação judiciária em matéria penal e da cooperação policial (anexa à Acta Final da Conferência Intergovernamental que adoptou o Tratado de Lisboa, de 13.12.2007)

[3] Conv enção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, de 28.1.1981, ratificado pelo Decreto do Presidente da República n.º 21/93, de 9 de Julho

[4] 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 8.11.2001, ratificado pelo Decreto do Presidente da República n.º 56/2006, de 20 de Junho.

coeso, que tem sido referenciado como paradigmático ao nível de várias instâncias da União.

Nessa medida, o alargamento da protecção de dados aos domínios da cooperação policial e judiciária em matéria penal, agora proposto ao nível da UE e destinado aos Estados Membros, não se apresenta como uma novidade para o nosso país, que detém já uma longa experiência jurídica nesta área.

A. Comentários Gerais

1. A adopção de uma Directiva para regular a protecção de dados pessoais tratados pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infracções penais ou de execução das sanções penais no âmbito da UE é uma medida legislativa muito positiva, na medida em que irá permitir alargar o âmbito da protecção a sectores que até agora não estavam abrangidos por um regime jurídico de protecção de dados pessoais.

   O único instrumento da União com um alcance mais generalizado neste domínio é a Decisão-Quadro[5] 2008/977/JAI do Conselho (adiante designada por Decisão-Quadro), mas que tem a grande limitação de não se aplicar aos tratamentos de dados domésticos, mas apenas às transferências de dados. Nessa medida, esta Proposta de Directiva vem possibilitar que o tratamento de dados no contexto da cooperação policial e judiciária em matéria penal, com forte impacto na vida das pessoas, seja feito de forma harmonizada no respeito

[5] Decisão-Quadro 2008/977/JAI do Conselho, de 27 de Novembro de 2008, relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (JO L 350 de 30.12.2008, página 60).

pelo direito fundamental à protecção de dados pessoais em todo o espaço da União.

Para uma maior solidez do novo quadro jurídico, é essencial que, em tudo o que não deriva das especificidades inerentes aos domínios policial e judiciário, haja a maior correspondência possível entre a Proposta de Directiva e a Proposta de Regulamento Geral de Protecção de Dados.
Isso nem sempre acontece, designadamente ao nível dos poderes e competências das autoridades de controlo, encontrando-se um pouco por todo o articulado discrepâncias que deveriam ser suprimidas nesta fase de discussão.
De igual modo, ao nível dos considerandos, deveria ser feito um esforço, no sentido de lhes dar um maior valor interpretativo que faculte uma melhor clarificação de algumas normas, cuja redacção é equívoca e o alcance nem sempre perceptível.

2. Apesar da importância de que esta Proposta de Directiva se reveste, no panorama actual de reforço da cooperação policial e judiciária em matéria penal, considera-se que o nível de protecção de dados previsto está aquém do desejável. Na verdade, representa mesmo nalguns aspectos fundamentais um recuo das garantias, relativamente aos instrumentos de referência do Conselho da Europa, à Decisão-Quadro e a outros actos legislativos da UE que, nesta área, já são cerca de 30.

Por outro lado, a Proposta de Directiva deveria apontar para um elevado patamar de protecção de dados, não fazendo baixar o nível de protecção de alguns Estados-Membros, sobretudo quando está agora consagrado como direito fundamental.

Seria expectável e desejável que esta Proposta reflectisse melhor as novas realidades tecnológicas e as suas potencialidades para o tratamento de dados

pessoais, com vista a poder abordá-las de forma menos tímida no articulado, não só ao nível do tratamento de certos tipos de dados como biométricos, genéticos, voz, imagem, como também no que diz respeito a plataformas *web* de partilha de informação, acessos em linha a bases de dados ou utilização de redes fechadas. A própria utilização dos conceitos de *privacy by design* e *privacy by default* peca claramente por defeito.

3. Apesar dos motivos apresentados para justificar a adopção de um acto legislativo autónomo para o sector policial, e de terem sido introduzidas algumas normas específicas relevantes (distinção das categorias de titulares, registos de *logs*, categorização dos dados em função do seu grau de fiabilidade e de rigor), em muitas situações essa particularidade foi negligenciada.

   Com efeito, no plano dos princípios aplicáveis aos tratamentos de dados, como a limitação da finalidade, o princípio da necessidade e da proporcionalidade, a qualidade dos dados, não foram tidas em conta as especificidades deste sector, com claro prejuízo para a salvaguarda das garantias das pessoas.

   Exemplo evidente disso é a ausência de norma quanto a prazos de conservação dos dados e revisões periódicas quanto à necessidade da sua manutenção, e a sua relação com diferentes categorias de dados e com diferentes categorias de titulares, bem como a separação entre dados de natureza administrativa e dados operacionais.

4. No plano das obrigações, é manifesta a intenção de as reforçar nalguns casos e de atribuir responsabilidades acrescidas ao subcontratante. No entanto, é estabelecido um permanente equívoco entre o papel do responsável pelo tratamento e o papel do subcontratante, ao ponto de se confundirem. Na maior parte das normas, não é claro de quem são as obrigações uma vez que

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

aparecem em alternativa, o que poderá levar à desresponsabilização de ambos.

Atenta a sensibilidade deste tipo de tratamentos de dados, o carácter muitas vezes centralizado dos sistemas de informação e o facto de o responsável ter de ser uma autoridade pública competente, esperar-se-ia que fosse feita uma ponderação sobre a necessidade de definir alguns critérios e limites relativamente à subcontratação.
Devem os subcontratantes ser autoridades públicas? Que tipo de operações de tratamento de dados ou áreas de intervenção são passíveis de ser efectuadas por subcontratantes e quais não são? Podem os custos da subcontratação ser factor determinante na escolha do subcontratante? Devem as operações de tratamento realizadas por subcontratantes ser feitas fora das instalações dos responsáveis? Ou por acesso remoto?

Estas são questões primordiais e às quais a Proposta não dá qualquer resposta, tratando a subcontratação de serviços no domínio policial como uma qualquer prestação de serviços de marketing.

Tendo em conta o crescimento exponencial do recurso a prestadores de serviços externos (*outsourcing*) e a real falta de controlo por parte dos responsáveis dos tratamentos sobre a subcontratação prestada, elevando a sua dependência funcional de empresas privadas, impor-se-ia uma reflexão séria sobre as condições concretas em que seria possível recorrer à subcontratação no contexto policial e judiciário.

5. Num mundo cada vez mais globalizado em que a criminalidade também não tem fronteiras e se encontra organizada de forma transnacional, é indispensável o reforço da cooperação policial e judiciária em matéria penal, o que

necessariamente implica o intercâmbio regular de dados pessoais e a partilha de informações.

Todavia, importa estar ciente que os dados transferidos neste cenário para um universo muito alargado de destinatários são de uma extrema sensibilidade e podem afectar de forma muito negativa e irreparável os direitos e liberdades dos cidadãos, caso não sejam tomadas todas as medidas adequadas para salvaguardar esses direitos.
A informação policial não assenta unicamente em factos verificados, mas baseia-se também em juízos pessoais, avaliações subjectivas e fontes cuja fiabilidade não é totalmente garantida.
A falta de qualidade dos dados, sendo altamente prejudicial para os titulares num contexto nacional, mais o será certamente num contexto internacional de rápida circulação da informação.

Por isso, impõe-se que as regras para a transferência internacional de dados pessoais sejam bem definidas, as condições bem delimitadas e as salvaguardas acauteladas.
Tal não acontece, de maneira nenhuma, no texto desta Proposta de Directiva, do qual ressalta um objectivo de facilitar as transferências de dados, sem cuidar de regular devidamente as garantias das pessoas.

Ao invés de se evoluir nesta matéria, com base nas experiências negativas de que há conhecimento, e adoptar medidas adicionais para protecção dos direitos dos cidadãos, verifica-se haver um claro recuo, relativamente a normas recomendadas pelo Conselho da Europa já em 1987, e mesmo em relação a actos legislativos adoptados pela União Europeia nos últimos anos.

6. O Tratado de Lisboa consagrou a existência de autoridades independentes para controlar a aplicação das normas de protecção de dados. Na Proposta de

Directiva, é patente o propósito de estabelecer condições que assegurem essa independência, também seguindo a jurisprudência recente do Tribunal de Justiça da União[6].

Para uma efectiva independência contribuem vários factores que, no todo, constituem o seu suporte: a forma de constituição das autoridades; os seus meios humanos, técnicos e financeiros; a sua gestão autónoma; as suas funções e poderes. São esses alicerces que garantem o exercício real das competências das autoridades de controlo na defesa do direito fundamental à protecção de dados.

Apesar do claro objectivo em atribuir às autoridades de controlo uma posição de independência que elas não detêm em alguns países, a Proposta resvala nesse intuito em relação ao modo restritivo como quer impor a designação dos seus membros, impedindo por um lado formas de designação que não comprometem o exercício independente de funções, e permitindo por outro que os governos possam sozinhos, em alternativa aos parlamentos, escolher os membros das autoridades de controlo que irão supervisionar as entidades públicas por si tuteladas.

Por outro lado, esta Proposta de Directiva reduz na substância os poderes das autoridades de controlo comparativamente aos poderes atribuídos no âmbito da Proposta de Regulamento, distorcendo a necessária coesão do novo quadro legal de protecção de dados. É basilar que os poderes de investigação e de intervenção das autoridades de controlo sejam fortalecidos para que se alcance uma eficaz acção supervisora para assegurar os direitos, liberdades e garantias dos cidadãos.

[6] Acórdão do Tribunal de Justiça, de 9 de Março de 2010 (Processo C-518/07)

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

B. Apreciação da Proposta de Directiva

1. Disposições gerais (Capítulo I)

1.1 Objecto e Objectivos

A proposta de Directiva estabelece as regras para a protecção de dados pessoais tratados pelas autoridades competentes para efeitos de prevenção, investigação, detecção, repressão de infracções penais ou de execução de sanções penais (artigo 1.º n.º 1).

No memorando explicativo, é afirmado que esta Directiva visa proteger, por um lado, os direitos fundamentais e liberdades das pessoas singulares, em particular o direito à protecção de dados e, por outro, garantir um elevado nível de segurança pública e assegurar o intercâmbio de dados entre autoridades competentes da UE.

Ora é essencial que, à semelhança do que consta actualmente no articulado da Decisão-Quadro (cf. artigo 1.º), esta Directiva consagre também um nível elevado de protecção dos direitos, enquanto garante um nível elevado de segurança pública. É fundamental que o propósito de balanceamento dos direitos seja claramente afirmado.

De igual modo, a referência ao direito à privacidade, expressa na Decisão-Quadro, deveria ser introduzida, na medida em que este direito consta do catálogo de direitos fundamentais da Carta Europeia e está intimamente relacionado com o direito à protecção de dados pessoais.

Ainda quanto ao artigo 1.º n.º 2 alínea b), que prevê que os Estados-Membros assegurem que o intercâmbio de dados pessoais pelas autoridades competentes da União não seja restringido nem proibido por razões relacionadas com a protecção de dados, no seguimento da livre circulação de dados prescrita no artigo 16.º do TFUE, é

de salientar que para os fins previstos nesta Directiva, o Reino Unido e a Irlanda[7] e a Dinamarca[8] não estão vinculados às medidas que vierem a ser adoptadas em aplicação do Título V da Parte III do TFUE, tendo um prazo para optar pela sua participação.

Não é feita qualquer menção a este facto, nem no memorando explicativo nem nos Considerandos da Proposta. O princípio da livre circulação de dados no seio da União exige um nível de protecção de dados equivalente em vários campos, designadamente no reforço dos direitos dos titulares, nas obrigações dos responsáveis pelos tratamentos de dados e nos poderes das autoridades nacionais de supervisão.

Deste modo, uma vez que o prazo para a tomada dessa decisão (3 e 6 meses respectivamente) pelos Estados-Membros em causa termina antes da aprovação da Proposta de Directiva, dependendo da sua opção de ficarem ou não abrangidos pela Directiva, deverá ser acautelado na Proposta que a livre circulação de dados não se aplicará em relação aos EM que não se vincularem a este acto legislativo.

1.2 *Âmbito de aplicação*

O artigo 2.º n.º 3 alínea a) exclui do âmbito de aplicação da Proposta o tratamento de dados «*efectuado no exercício de actividades não sujeitas à aplicação do direito da União, nomeadamente no que se refere à segurança nacional*». Esta é uma excepção compreensível neste quadro legal, mas a clarificação do termo "segurança nacional" deveria ser feita, ao nível dos Considerandos, para evitar que, de acordo com as suas políticas internas, os EM possam dar-lhe um diferente valor interpretativo e, dessa forma, haver o risco de os tratamentos de dados relativos a certos tipos de criminalidade, em particular, o terrorismo, poderem ficar fora do âmbito de aplicação desta Directiva.

[7] Protocolo relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça (1997)
[8] Protocolo relativo à posição da Dinamarca (1997)

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

1.3 Definições

No artigo 3.º da Proposta, são dadas definições de "dados biométricos" e de "criança", que depois não têm qualquer expressão no restante articulado, o que não é compreensível.

Com efeito, ao tratamento de dados de menores deveriam ser aplicadas especiais garantias, em particular no contexto desta Proposta. O princípio da necessidade, bem como a qualidade dos dados, seja quanto à sua actualização ou fiabilidade, uma vez que os dados de crianças podem alterar-se mais rapidamente (por exemplo, dados biométricos: reconhecimento facial ou impressões digitais), seja quanto a prazos de conservação mais curtos, deveriam merecer no texto uma abordagem específica, com vista a salvaguardar os direitos dos menores.

Quanto à definição de "autoridades competentes", constante do ponto 14, tendo em conta que os tratamentos de dados só podem ser realizados por autoridades competentes para os fins enunciados (artigo 2.º n.º 1 conjugado com o artigo 1.º n.º 1), seria indispensável introduzir no final da definição que esta competência esteja prevista por lei do Estado-Membro.

2. Princípios (Capítulo II)

2.1 Princípio da finalidade

No artigo 4.º alínea b) da Proposta, estipula-se que os dados pessoais devem ser «*recolhidos para finalidades determinadas, explícitas e legítimas e não ser posteriormente tratados de forma incompatível com essas finalidades*». Trata-se aqui do que se designa por princípio da limitação da finalidade.

Embora esta redacção seja idêntica à usada pela Directiva 95/46/CE (Directiva de Protecção de Dados), a experiência tem demonstrado que ela é insuficiente se não estiverem verificadas uma das seguintes condições: que a lei estabeleça o que são fins

incompatíveis ou que a autoridade nacional de supervisão seja chamada a pronunciar-se quando houver alteração da finalidade inicialmente prevista.

Na verdade, no contexto do tratamento de dados policiais, pressupõe-se que as finalidades prosseguidas pelas autoridades competentes estão previstas na lei. Nesse sentido, qualquer utilização dos dados pessoais para uma finalidade diferente, mesmo que compatível, deveria igualmente estar prevista em lei. Só assim se atinge, por um lado, que a finalidade seja legítima, explícita e específica, como se evita que os dados possam ser tratados para fins diferentes e até incompatíveis, pois a norma proposta deixa em aberto como e quem faz a avaliação sobre eventual uso incompatível.

A redacção do articulado deveria assim ser alterada, no sentido de proibir que os dados pessoais possam ser tratados para finalidade diferente (em vez de "incompatível"), a menos que previsto por lei. Aí o legislador nacional fará a devida ponderação sobre a utilização dos dados para fim compatível.

Esta é uma questão crucial, na medida em que da explicitação da finalidade depende a aplicação de um conjunto de outros princípios como o da necessidade, da qualidade dos dados ou o princípio da proporcionalidade, bem como a análise dos fundamentos de legitimidade.

2.2 *Princípio da necessidade e qualidade dos dados*

A Proposta de Directiva não tem qualquer norma relativa a prazos de conservação dos dados, limitando-se na alínea e) do artigo 4.º a prever a possibilidade de anonimização. Tal não é de maneira nenhuma aceitável, devendo ser introduzida a obrigatoriedade de proceder à eliminação dos dados quando deixarem de ser necessários à finalidade para que foram recolhidos e posteriormente tratados[9].

[9] Actualmente, a Decisão-Quadro tem uma disposição específica, no artigo 5.º, relativa aos prazos de conservação dos dados pessoais.

De igual modo, a Proposta deverá conter a obrigação de as autoridades competentes reverem periodicamente a necessidade de manterem os dados conservados.

Por outro lado, no que diz respeito à qualidade dos dados, a alínea d) do mesmo artigo apenas prevê que sejam adoptadas as «*medidas razoáveis*» para garantir que os dados inexactos sejam rectificados ou apagados, o que é manifestamente insuficiente.

O rigor da informação de natureza criminal é indispensável não só para a defesa dos direitos das pessoas, como também para o bom desempenho da actividade policial. Nesse sentido, deveria ser introduzida na Proposta a obrigação de proceder a verificações regulares sobre a qualidade dos dados. Esta prática reveste-se de importância acrescida num contexto de partilha de dados pessoais a nível da União e internacional. Assim, deveria ser eliminada a expressão «*medidas razoáveis*».

O artigo 6.º, sobre níveis diferentes de exactidão e fiabilidade, vem aliás reforçar este entendimento, ao prever que sejam estabelecidas distinções entre dados pessoais em função da sua fiabilidade e distinguindo o que são factos de apreciações pessoais, em linha com a Recomendação R (87) 15 do Conselho da Europa.

Todavia, pelos motivos atrás expostos, a expressão «*na medida do possível*» deve ser suprimida, pois se não fosse possível às autoridades competentes fazerem essa distinção não poderiam realizar a sua missão. Também o termo «*categorias de dados*», no n.º 1 do artigo 6.º, deveria ser substituído apenas por "dados", porquanto a fiabilidade da informação diz respeito aos dados em si e não necessariamente a categorias de dados. Na mesma categoria de dados, poderá haver dados fiáveis e dados não fiáveis, dependendo da fonte de informação e de como as categorias estão organizadas.

Ainda ao nível dos princípios relativos aos tratamentos de dados, previstos no artigo 4.º, seria de introduzir uma nova alínea, na qual se estipulasse que os dados só podem ser acedidos ou disponibilizados a pessoal devidamente autorizado das autoridades competentes que necessitem deles para o cumprimento das suas funções. Este é um princípio relevante de acesso à informação com base na "necessidade de conhecer",

impondo, por isso, a aplicação de uma rigorosa política de gestão de perfis de utilizador.

2.3 *Categorias de titulares*

O artigo 5.º estabelece, à semelhança de outros instrumentos legais da União[10], a distinção entre diferentes categorias de titulares de dados (suspeitos, condenados, vítimas, testemunhas, informadores, contactos, outros). Esta obrigação é importante ao nível das normas de protecção de dados no contexto policial, uma vez que permite aplicar regras diferenciadas de acordo com a categoria em causa.

Contudo, esta diferenciação por si só não traz qualquer valor acrescentado, pois não resulta da Proposta qualquer medida protectora subsequente. É pois imprescindível estabelecer quais são as consequências desta categorização. O texto da Proposta deve impor condições específicas e salvaguardas, em particular, sobre os dados de não-suspeitos para evitar que essas pessoas sejam lesadas nos seus direitos, garantindo uma utilização proporcional desses dados, designadamente períodos de conservação bastante mais limitados e revisões periódicas quanto à necessidade de manter os dados.

Também a expressão «*na medida do possível*» deve ser eliminada, pois as autoridades competentes quando recolhem os dados conseguem determinar, no momento, qual a condição do titular, mesmo que tal venha a sofrer eventuais ajustamentos futuros.

Por outro lado, na alínea a) do mesmo artigo, juntam-se na mesma categoria de titulares "suspeitos" e "potenciais criminosos", o que suscita as maiores reservas. Por um lado, trata-se de situações bem distintas que representam diferentes categorias de titulares, o que é relevante quando se analisa a adequação dos dados tratados e terá naturalmente reflexos ao nível dos prazos de conservação desses dados; por outro lado, porque se prevê que a aferição seja feita com base em «*motivos fundados para crer*»,

[10] cf. Decisão Europol, Decisão Eurojust, Decisão-Quadro

o que é demasiado vago, principalmente no que diz respeito a um crime que não ocorreu. Urge, pois, que tal expressão seja substituída por indicações factuais, o que será mais facilmente verificável e limita a possibilidade de tratamento de dados de forma abusiva.

Por último, a categoria "outros" é demasiado genérica, podendo abranger qualquer pessoa. Impunha-se no mínimo alguma exemplificação ao nível dos Considerandos.

2.4 *Licitude do tratamento*

No artigo 7.º da Proposta, estabelecem-se os fundamentos de legitimidade para o tratamento de dados, sendo que as alíneas a) e b) têm sempre por base disposição legal. Em derrogação, a alínea c) prevê que é lícito tratar dados para protecção dos interesses vitais do titular ou de um terceiro e a alínea d) para prevenção de uma ameaça grave e imediata para a segurança pública.

Considera-se que a alínea d) deveria ser eliminada, na medida em que a *«prevenção de uma ameaça grave e imediata para a segurança pública»* já se inscreve nas funções de "prevenção" das autoridades competentes, determinadas por lei, estando já por isso incluída no âmbito da alínea a).

Não se entende pois o objectivo de isolar esta finalidade como fundamento autónomo de licitude do tratamento, podendo sim abrir a porta a uma legitimidade menos escrutinável.

2.5 *Dados sensíveis*

No artigo 8.º n.º 1 são elencados os dados sensíveis que têm uma proibição genérica de tratamento e no n.º 2 as situações em que tal proibição não se aplica.

Com efeito, esta disposição é mais aberta do que a constante da Decisão-Quadro e de outros actos legislativos da União, não só porque não faz depender o tratamento destas categorias especiais de dados da condição cumulativa da estrita necessidade[11], como as derrogações são muito amplas, permitindo na prática que todos os dados sejam tratados sem qualquer limitação, pelo que não se vislumbra o alcance da proibição geral.

Acresce ainda que não é definido o que se entende por garantias adequadas, o que pode resultar numa aplicação muito diferenciada entre Estados-Membros.

O Considerando 26 não é de todo esclarecedor, pois limita-se a repetir as derrogações para o tratamento de dados.

Também relativamente aos dados genéticos, que foram aduzidos à lista de dados sensíveis constante da Directiva 95/46/CE, não há qualquer orientação nem nos Considerandos nem no articulado sobre a utilização destes dados no contexto policial.

Deste modo, sugere-se que a redacção do artigo 8.º seja alterada num sentido mais restritivo e clarificador quanto à adopção de garantias adequadas ao tratamento deste tipo de dados. Também quanto à alínea c) do n.º 2, que prevê a possibilidade de tratar dados sensíveis quando estes tiverem sido *«manifestamente tornados públicos pelo seu titular»*, deverá ser aditado "desde que sejam relevantes e estritamente necessários à finalidade em causa". Será, no entanto, de ponderar se será sempre possível de forma inequívoca distinguir quando é o próprio titular a tornar os dados públicos ou um terceiro, principalmente no ambiente da Internet.

Por último, não se poderá deixar de referir que o elenco fechado de dados do artigo 8.º da Proposta de Directiva contende com o artigo 35.º da Constituição da República Portuguesa, que inclui no catálogo de dados sensíveis os dados relativos à *«vida*

[11] Também a Recomendação R (87) 15 do Conselho do Europa, sobre o tratamento de dados no sector policial, no seu Princípio 2.4, só admite a recolha de dados sensíveis se for *«absolutamente necessário para as finalidades de um inquérito concreto»*.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

privada». Nessa medida, a Proposta de Directiva deveria ter uma formulação mais flexível, que permitisse aos Estados-Membros compatibilizar com o seu direito interno.

3. Direitos do titular dos dados (Capítulo III)

3.1 Modalidades do exercício dos direitos

Relativamente aos direitos dos titulares, previstos nos artigos 10.º a 17.º, reconhece-se haver de, uma maneira geral, importantes melhoramentos por comparação com o actual regime, mormente quanto a uma melhor clarificação das obrigações do responsável pelo tratamento, a uma maior transparência perante o titular dos dados e aos mecanismos propostos para um melhor exercício dos direitos.

Todavia, tais avanços são enfraquecidos por expressões limitativas como *«medidas razoáveis»* (cf. artigo 10.º n.ºs 1 e 3). Tendo em conta a natureza sensível da informação aqui em causa e o impacto negativo que pode ter na vida das pessoas, é essencial que as modalidades para o exercício dos direitos sejam claras e transparentes. Neste sentido, é imperioso que a redacção seja alterada para "medidas adequadas". Por outro lado, também no nº4 do artigo 10.º, deverá ser fixado um prazo máximo de resposta ao cidadão, pois prever fornecer a informação apenas *«sem demora injustificada»* permite que na prática o titular dos dados encontre dificuldades no exercício dos seus direitos.

Sugere-se ainda que a expressão *«interesses legítimos dos titulares»*, que é usada em vários artigos em casos de ponderação de valores com vista à restrição de direitos, seja substituída por "direitos e garantias" dos titulares, pois não se está aqui no contexto contratual ou de mero interesse individual.

Relativamente ao exercício do direito de acesso (artigo 12.º), prevê-se na alínea g) que sejam comunicados ao titular, os dados objecto de tratamento e quaisquer

informações *«disponíveis»* sobre a origem desses dados. Ora, no âmbito do tratamento de dados policiais, as autoridades competentes têm sempre de saber a origem dos dados, até porque a fonte da informação tem de estar devidamente registada e documentada, pelo que a palavra *«disponíveis»* deve ser apagada.

3.2 *Restrições aos direitos*

Quanto às restrições de informação, acesso, rectificação e apagamento, compreensíveis no âmbito do tratamento de dados policiais e jdiciários, elas devem ser, por princípio, avaliadas pelo responsável do tratamento caso-a-caso, com base nas derrogações já previstas na Proposta de Directiva.

A possibilidade de os EM determinarem por lei categorias de dados sobre as quais venham a recair limitações ao exercício dos direitos (artigos 11.º n.º 5 e 13.º n.º 2) deve ser melhor clarificada, acautelando-se que tal só poderá ser feito em situações especiais plenamente justificáveis, nas quais seja evidente que a derrogação diz respeito a todos os dados naquelas circunstâncias (por exemplo, quando estiver em causa o segredo de justiça).

O n.º 4 do artigo 13.º deveria ser alterado no sentido de garantir que os responsáveis pelo tratamento documentam cada decisão individualmente, se houver recusa de comunicação dos dados aos titulares, a qual deverá estar disponível para as autoridades nacionais de supervisão em caso de queixa.

3.3 *Direito de rectificação e de apagamento*

É ainda de salientar que, à semelhança do que acontece com o direito de informação e o direito de acesso, em que os fundamentos para a limitação do exercício de direitos vêm prescritos na Proposta de Directiva, também o mesmo deveria ser feito

relativamente aos direitos de rectificação e de apagamento, a fim de conseguir uma melhor harmonização de critérios e procedimentos.

Também deveria ser introduzido, em número autónomo, no final do artigo 15.º (direito de rectificação) e do artigo 16.º (direito de apagamento), que "os Estados-Membros devem prever que o responsável pelo tratamento notifica os terceiros a quem tenha transmitido dados da rectificação/apagamento ou restrição realizadas em conformidade com o n.º 1".

3.4 Intervenção das autoridades nacionais de controlo

As autoridades nacionais de controlo têm um papel importante a desempenhar na recepção de queixas ou de pedidos de verificação da legitimidade do tratamento de dados, decorrentes do exercício dos direitos por parte dos titulares, tendo os responsáveis a obrigação de informar os titulares de que podem recorrer para a autoridade de controlo.

Contudo, não estando previsto nos poderes destas autoridades, elencados no artigo 46.º da Proposta de Directiva, a possibilidade de ordenar ao responsável pelo tratamento o cumprimento dos pedidos relativos ao exercício dos direitos, a intervenção da autoridade de controlo não tem qualquer eficácia.

É pois crucial atribuir os devidos poderes às autoridades de controlo de protecção de dados para que possam efectivamente ser um garante do exercício dos direitos dos titulares.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

4. Responsável pelo tratamento e subcontratante (Capítulo IV)

4.1 Protecção de dados desde a concepção e por defeito

O artigo 19.º da Proposta introduz, pela epígrafe, os conceitos de *privacy by design* e *privacy by default*, embora convertendo a "privacy" em protecção de dados. No entanto, o articulado não reflecte tais noções, resultando numa norma confusa e insuficiente. Os Considerandos também não contêm qualquer elucidação sobre a aplicação destes conceitos à especificidade do tratamento de dados policiais.

A "protecção de dados desde a concepção", prevista no n.º 1 do artigo 19.º, não vai além do princípio geral relativo à adopção de medidas de segurança, o qual é desenvolvido mais adiante no artigo 27.º sobre segurança dos dados. Ora, este conceito pressupõe que, na fase de concepção dos sistemas de informação, as condições gerais e específicas aplicáveis aos tratamentos de dados sejam consideradas ao nível do desenho e programação/configuração prévios desses sistemas (separação lógica de dados ou categorias, alertas de consulta, encriptação de determinados campos, gestão de identidades, notificações automáticas de prazos limites de conservação, etc.).

De igual modo, a privacidade por defeito, no n.º 2 do artigo, é limitada apenas a garantir o princípio da minimização dos dados, quando o conceito é em si mesmo muito mais abrangente, devendo neste contexto incluir procedimentos, perfis de acesso dos utilizadores, entre muitos outros aspectos.

Sugere-se, pois, que este artigo seja bastante mais substanciado, tendo em conta designadamente muitas das obrigações impostas por este instrumento quanto ao tratamento de dados pessoais, bem como seja estabelecido o momento para a implementação destes princípios.

4.2 Responsáveis conjuntos e subcontratante

O artigo 20.º da Proposta prevê a possibilidade da existência de responsáveis conjuntos pelo tratamento, situação em que deverão est es, por acordo, definir as respectivas obrigações.

Esta é uma previsão importante, porquanto há circunstâncias em que o modelo que melhor reflecte o caso concreto é o da responsabilidade conjunta. Todavia, é essencial clarificar que todos os responsáveis envolvidos devem ser autoridades competentes na acepção do artigo 3.º da Proposta.

De igual modo, e tendo em conta os fundamentos de legitimidade do artigo 7.º, deverá, sempre que possível, ser a lei a determinar estas situações.

Nos casos em que tal não aconteça, a norma deverá dispor que entre os responsáveis conjuntos seja obrigatoriamente feito um acordo escrito de carácter vinculativo, de modo a que fique claramente atribuída a repartição de responsabilidades e, subsequente, assumpção. Além disso, esse acordo deverá ser submetido a parecer da autoridade de controlo para verificação do cumprimento das disposições adoptadas em conformidade com a Proposta de Directiva.

Além dos mecanismos para o exercício dos direitos pelos titulares dos dados (mencionado no texto), há um vasto conjunto de outras obrigações dos responsáveis que tem de estar reflectido nesse acordo escrito.

Em relação à posição e obrigações do subcontratante, o artigo 21.º não tem de todo em consideração a natureza e a especificidade dos tratamentos de dados para efeitos de prevenção, investigação, detecção e repressão de infracções penais ou execução de sanções penais.

Com efeito, o texto não reflecte as exigências inerentes ao contexto em causa nem tão pouco a evolução da realidade quanto ao recurso a serviços de subcontratação, havendo até um certo recuo relativamente a exigências actualmente em vigor na Directiva 95/46/CE e que se imporiam aqui com mais acuidade.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Assim, no n.º 1 do artigo 21.º, que prevê que o responsável pelo tratamento «*escolha um subcontratante que apresente garantias suficientes de execução das medidas e procedimentos técnicos e organizativos apropriados*», desapareceu a obrigação, constante do artigo 17.º n.º 2 da mencionada Directiva, de o responsável pelo tratamento zelar pelo cumprimento dessas medidas.

Além disso, não são definidos quaisquer critérios para aferir o que pode ser entendido como garantias suficientes e como podem ser mensuráveis. Não se pode ignorar, por exemplo, o recurso cada vez maior ao *cloud computing*, por motivos de custos, com as inerentes desvantagens que tal pode acarretar ao nível da segurança da informação e ao nível da protecção de dados pessoais da sensibilidade dos que estão aqui em causa.

Deste modo, seria indispensável que a Proposta de Directiva estabelecesse alguns critérios e desenvolvesse o que podem ser consideradas garantias suficientes, além de introduzir a obrigação do responsável velar pelo cumprimento de tais medidas.

O n.º 2 do artigo 21.º, que prevê que as operações de tratamento de dados em subcontratação sejam reguladas por um acto jurídico vinculativo, deveria igualmente ser mais detalhado, no sentido de fazer verter para esse contrato quais são à partida as instruções do responsável pelo tratamento e o que se espera que o subcontratante faça. Desta forma, ficariam bem delineados os papéis e obrigações de cada um e permitiria ao responsável do tratamento ter um maior controlo sobre a actividade do subcontratante.

Quanto ao nº 3 do artigo 21.º, considera-se estar-se perante uma norma legitimadora de uma violação assumida das disposições da Proposta, pelo que não é aceitável, devendo ser eliminada. Na verdade, não se entende como é admissível que um subcontratante trate dados pessoais fora das instruções do responsável pelo tratamento – às quais está vinculado – e, em vez de ser sancionado, seja "promovido" a responsável conjunto. Ademais, não se vislumbra como se compatibilizaria esta situação na prática com as exigências do artigo 20.º.

A situação não é menos que caricata, pois abre a porta a que uma empresa privada que desrespeite os termos para o tratamento de dados a que está legalmente vinculada se transforme em responsável pelo tratamento, a par de uma autoridade pública competente, que apenas pode tratar os dados pessoais no cumprimento das suas funções atribuídas por lei.

Por último, é fundamental que seja introduzida no artigo 21.º ou no artigo 22.º (cujo alcance real não se entende), a obrigação de sigilo profissional às pessoas que, actuando sob a direcção do subcontratante, tenham conhecimento de dados pessoais.

4.3 Documentação

O artigo 23.º vem introduzir a obrigação do responsável e do subcontratante manterem documentação sobre todos os sistemas e procedimentos de tratamento sob a sua responsabilidade e disponibilizá-la à autoridade de controlo de protecção de dados, quando solicitados.

Esta norma vem substituir a actual obrigação de notificação à autoridade de controlo e tem por objectivo, de acordo com o Considerando 40, permitir o controlo de todas as operações de tratamento.

Assim sendo, o elenco de informações que devem constar da documentação é escasso para dar cumprimento ao propósito da norma. Devem pois ser aditadas, como patamar mínimo, as seguintes informações: categorias de dados tratados; prazos de conservação; fundamentos de legitimidade do tratamento; identificação e contactos do delegado de protecção de dados (*data protection officer*); regras internas para o exercício dos direitos dos titulares nos termos do artigo 10.º;

Deveria ainda ser prevista a existência de um catálogo de informações mais alargado, onde seria relevante que constassem: acordo escrito em caso de responsáveis conjuntos pelo tratamento; lista de subcontratantes e actividades objecto da subcontratação,

bem como os actos jurídicos previstos no artigo n.º 21 n.º 2; política de segurança da informação e correspondente avaliação de riscos prevista no artigo 27.º.

Tudo isto corresponde a documentação que os responsáveis já têm de deter em cumprimento das disposições da presente Proposta, não representando por isso um encargo ou esforço adicional.

4.4 Registo das operações de tratamento

O artigo 24.º prevê o registo de operações de tratamento e a sua conservação, obrigando à existência dos designados *logs* de auditoria. Esta é uma previsão muito positiva, em particular no contexto do tratamento de dados de grande sensibilidade e de grande partilha e intercâmbio de informação.

No entanto, o texto da norma não está correctamente formulado do ponto de vista técnico nem permite cumprir o objectivo a que se propõe. Na verdade, a identificação da pessoa que realizou uma operação é essencial para detectar acessos não autorizados ou abusivos, pelo que deverá ser eliminada a expressão *«na medida do possível»*. Aliás, tendo o utilizador que se autenticar, é registada naturalmente essa informação.

O nº 1 deve, pois, ser reescrito, no sentido de prever o registo de todas as operações de tratamento de dados, incluindo todas as transmissões de dados, bem como da data e hora em todas elas, devendo ser incluído no *log* o conteúdo da informação acedida. A conservação destes registos deveria ficar sujeita a um prazo máximo.

Quanto ao n.º 2 do artigo, deveria estar explícito que estes registos podem ser usados para fins de auditoria, quer por parte do delegado de protecção de dados, quer por parte da autoridade de protecção de dados. Deveria ainda ser clarificada a finalidade de *«autocontrolo»*, impondo-se a análise periódica destes registos a fim de detectar qualquer desvio, em conformidade com as boas práticas de segurança.

4.5 Cooperação e consulta prévia com a autoridade de controlo

O artigo 25.º estabelece as condições de cooperação dos responsáveis pelos tratamentos ou subcontratantes com a autoridade nacional de protecção de dados.

Independentemente dos comentários feitos mais adiante sobre os poderes das autoridades de controlo, considera-se fundamental introduzir, num ponto autónomo deste artigo, que o dever de cooperação também deve ser assegurado quando a autoridade de controlo tiver necessidade de examinar os sistemas de informação e os tratamentos de dados pessoais, sendo-lhe garantido o acesso às instalações do responsável ou subcontratante, à semelhança do que está previsto noutros actos legislativos da União, designadamente em relação à Europol e à Eurojust.

No que diz respeito às situações de consulta prévia à autoridade de controlo, previstas no artigo 26.º, afigura-se serem demasiadamente limitadas, na medida em que se resumem ao tratamento de dados sensíveis – sendo que estes resultarão na maioria das vezes de disposição legal específica – e a tratamentos que apresentem riscos específicos para os direitos, liberdades e garantias dos titulares, o que é sobremaneira vago e impreciso.

Acresce a isto que a consulta só se efectuará quando houver lugar a tratamentos de dados que farão parte de *«um novo ficheiro»*. Ora, hoje em dia, a maioria dos sistemas de informação são integrados, não sendo pois nada claro quando se está perante a constituição de um novo ficheiro.

Deste modo, o n.º 1 do artigo deveria ser reformulado no sentido de dispor que a consulta prévia se deve realizar sempre que os sistemas de informação são alargados, cobrindo-se assim todas as situações.

Por outro lado, a obrigação de consulta deve ser exclusiva do responsável do tratamento e não do subcontratante, em alternativa, pelo que a referência ao subcontratante deve ser eliminada.

Se se atender às responsabilidades específicas do responsável pelo tratamento (determinar as finalidades, condições e meios do tratamento de dados) e às do subcontratante (agir segundo as instruções do responsável), a obrigação de consulta prévia deve recair apenas sobre o responsável do tratamento, até porque a posição do subcontratante não lhe permite seguir, sem a intervenção do responsável, os resultados da consulta à autoridade de protecção de dados. A manter-se, este seria mais um caso em que as responsabilidades de um e outro seriam equívocas e nebulosas.

Quanto às situações em que deveria haver consulta prévia à autoridade de controlo, o seu leque deveria ser obviamente alargado ao nível da Proposta de Directiva e não ser deixado à discricionariedade dos Estados-Membros, até por motivos óbvios de maior harmonização.

Desde logo, deveriam ser incluídos os tratamentos de dados previstos no artigo 9.º (definição de perfis e decisões automáticas), os acordos firmados entre responsáveis conjuntos para repartição de responsabilidades, as transferências de dados com base no artigo 35.º, bem como o desenvolvimento de novos projectos tecnológicos com incidência no tratamento dos dados.

4.6 Segurança dos dados e notificação de violações de segurança

As matérias relativas à segurança dos dados vêm prescritas nos artigos 27.º a 29.º e trazem algumas novidades. O artigo 27.º baseia-se sobretudo nas medidas de segurança constantes da Decisão-Quadro e também da Directiva 95/46/CE, e apenas diz respeito aos tratamentos de dados automatizados.

Quanto ao tratamento de dados manuais, abrangidos pela Proposta de Directiva, e que são ainda bastante frequentes no contexto policial e judiciário, não estão previstas quaisquer medidas de segurança específicas, o que é uma falha grave que importa colmatar.

Ainda no universo das medidas de segurança, é de saudar a extensão da obrigação de resultado aos subcontratantes, independentemente do que tiver sido acordado com o responsável.

Todavia, considera-se que a redacção do artigo 27.º é algo confusa e nalguns pontos parece ser redundante, o que não beneficia a adopção das medidas e o cumprimento das obrigações. Sugere-se, por isso, que haja uma reformulação genérica da redacção, que traga mais clareza ao que se pretende, que distinga de forma evidente as medidas de segurança física das medidas de segurança lógica e que utilize uma terminologia mais correcta. Falta igualmente uma referência à perda ou destruição de dados acidental ou ilegal.

Esta é sem dúvida uma área em que se pode melhorar substancialmente, tendo em conta a experiência já adquirida, a necessidade de ir ao encontro dos novos desenvolvimentos tecnológicos e a forma como estão desenhadas *grosso modo* as trocas de informações entre Estados-Membros da União e entre os EM e os sistemas de informação europeus.

No que diz respeito à criação de uma nova obrigação do responsável do tratamento, relativa à notificação à autoridade de controlo (e eventualmente aos titulares dos dados) de violações de segurança dos dados pessoais, em linha com a Proposta de Regulamento e com as alterações introduzidas na Directiva 2002/58/CE (Directiva da privacidade nas comunicações electrónicas), considera-se que o prazo para notificar é demasiado curto, não permitindo em rigor ao responsável cumprir todos os requisitos da notificação.

Nesse sentido, sugere-se que o prazo de 24 horas seja alargado para 72 horas, que parece ser um período mais razoável. Quanto ao conteúdo da notificação, apenas se sugere que seja acrescentada a informação sobre se o responsável do tratamento pretende notificar os titulares dos dados, se aplicável, ou se essa comunicação é derrogada pelos motivos referidos no n.º 4 do artigo 11.º.

O artigo 28.º n.º 5 confere à Comissão Europeia competência para adoptar actos delegados *«a fim de especificar mais concretamente os critérios e requisitos aplicáveis à determinação da violação de dados referida nos nºs 1 e 2, e às circunstâncias particulares em que um responsável pelo tratamento e um subcontratante são obrigados a notificar a violação de dados pessoais»*.

Ora, é entendimento da CNPD que as circunstâncias e os critérios aplicáveis à determinação de uma obrigação são elementos essenciais, pelo que não se enquadram no figurino de um acto delegado que, por força do artigo 290.º do TFUE, é um acto não legislativo. Deste modo, considera-se que se trata aqui de matéria substantiva, reservada ao acto legislativo, que não pode ser objecto de delegação de poderes.

Nessa medida, deve a Proposta de Directiva definir à partida quais as situações concretas em que se considera haver uma violação de segurança e quando impende sobre o responsável pelo tratamento a obrigação de a notificar.

4.7 Delegado de protecção de dados

A introdução da figura do delegado de protecção de dados na Proposta de Directiva é indubitavelmente bem-vinda, pela função crucial de apoio ao cumprimento interno das regras de protecção de dados, além da vantagem de ser um interlocutor privilegiado da autoridade de controlo.

Daí que a obrigação de designar um delegado de protecção de dados seja um passo muito importante. Contudo, os termos da sua designação surgem algo confusos no texto do artigo 30.º n.º 1, em que se prevê que seja o responsável ou, em alternativa, o subcontratante a proceder a essa designação.

No âmbito da cooperação policial e judiciária em matéria penal, não é crível que o responsável pelo tratamento não proceda a quaisquer operações de tratamentos de dados. Assim, na hipótese de apenas algumas operações de tratamento terem sido subcontratadas, efectuando ambos tratamentos de dados, não resulta claro a quem

incumbe a obrigação de designar. Considera-se que esta obrigação deve ser, em primeiro lugar, do responsável pelo tratamento, e eventualmente alargada aos subcontratantes nos casos em que a sua intervenção seja de molde a justificar a designação de um delegado de protecção de dados.

Também a redacção do n.º 3 se apresenta equívoca, e o memorando explicativo e o Considerando 44 não trazem esclarecimento adicional sobre a possibilidade de um delegado de protecção de dados «*ser designado para várias entidades, tendo em conta a estrutura organizativa da autoridade competente*».

Com efeito, nos termos da Proposta de Directiva, o responsável pelo tratamento só pode ser a autoridade competente; logo, será sempre ela e não entidades que a possam constituir a ter a obrigação de designar o delegado de protecção de dados. Sugere-se assim que este n.º 3 seja eliminado por não produzir qualquer efeito prático no regime, prestando-se, pelo contrário, a incertezas.

Deveria ainda ser incluída a obrigação de os responsáveis pelo tratamento e os subcontratantes notificarem a autoridade de controlo da identificação e contactos do delegado de protecção de dados, após a sua designação, bem como de quaisquer alterações que venham a ocorrer.

Sobre os artigos 31.º e 32.º, que determinam a posição do delegado de protecção de dados e as suas competências, é de sublinhar que, atendendo ao papel relevante que se pretende que desempenhe, através das funções que lhe estão atribuídas, não estão reunidas as garantias suficientes para o poder fazer com a necessária independência.

Em primeiro lugar, deverão estar salvaguardados eventuais conflitos de interesse; em segundo lugar, deverá ser garantido um vínculo laboral adequado, por um período razoável de tempo, que evite um desajustado desequilíbrio nas relações com o responsável pelo tratamento (autoridades públicas) e garanta, simultaneamente, as condições necessárias ao exercício independente das suas competências. Só neste quadro é útil a designação de um delegado de protecção de dados.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

5. Transferência de dados pessoais para países terceiros ou organizações internacionais (Capítulo V)

Neste capítulo da Proposta, determinam-se os princípios e as condições em que podem ser realizadas transferências internacionais de dados pessoais, isto é, para países ou organizações fora da União Europeia.

Atendendo a que a generalidade dos países de destino não oferece aquilo que para os padrões europeus é considerado um nível de protecção adequado, é indispensável que sejam adoptadas todas as garantias e medidas de salvaguarda ao nível da protecção dos dados pessoais transferidos, num instrumento vinculativo para os destinatários, de modo a garantir a defesa dos direitos das pessoas.

Os princípios gerais para a transferência internacional de dados limitam-se a duas condições genéricas cumulativas: a transferência ser necessária para fins de prevenção, investigação, detecção ou repressão de infracções penais ou ainda para a execução de sanções penais; e serem cumpridas pelo responsável (e pelo subcontratante?) as condições estabelecidas no presente capítulo, que como se verá adiante são praticamente inexistentes.

Em síntese, os dados pessoais podem ser transferidos sempre que: houver uma decisão de adequação quanto ao nível de protecção de dados emitida pela Comissão Europeia (artigo 34.º); houver um instrumento juridicamente vinculativo com garantias adequadas no que diz respeito à protecção de dados pessoais ou o responsável (ou o subcontratante), através de pessoal devidamente autorizado, após uma avaliação, tiver concluído existirem garantias (artigo 35.º); forem realizadas no âmbito das derrogações previstas (artigo 36.º).

Como se pode verificar, não há nenhuma situação em que os dados pessoais não possam ser transferidos para países terceiros ou organizações internacionais, nem

mesmo caso venha a haver uma decisão de não-adequação da Comissão Europeia (artigo 34.º), por motivos de não estarem assegurados os direitos das pessoas. Nestas circunstâncias, a transferência seria em princípio proibida, mas os dados continuam a poder ser transferidos ao abrigo do n.º 1 do artigo 35.º ou do artigo 36.º.

Quanto a condições específicas aplicáveis às transferências, o artigo 37.º limita-se a dispor que o responsável pelo tratamento deverá informar o destinatário de qualquer limitação do tratamento, o que, de acordo com o articulado da Proposta de Directiva, apenas se verifica no âmbito do exercício do direito de apagamento (artigo 16.º n.º 3).

Em suma, falta quase tudo ao nível das condições e das salvaguardas, permitindo-se inclusivamente que sejam efectuadas transferências ulteriores de dados de um país destinatário para outro, sem qualquer conhecimento, controlo ou restrição por parte do responsável pelo tratamento, contornando ainda de forma mais evidente as já de si exíguas salvaguardas.

Este é, assim, um quadro legal inaceitável, impondo-se profundas alterações no capítulo das transferências, devendo ser introduzidas importantes salvaguardas no articulado, de modo a garantir o respeito pelos direitos fundamentais, incluindo o da protecção de dados pessoais.

Em primeiro lugar, deve ser requisito para a transferência de dados que o responsável no país terceiro ou na organização internacional seja uma autoridade competente na acepção da Proposta de Directiva: prevenção, investigação, detecção e repressão de infracções penais ou execução de sanções penais. Tal condição deve ser introduzida no artigo 33.º.

Em segundo lugar, tendo em conta as finalidades genéricas da Proposta, a transferência de dados deve respeitar o princípio da finalidade legítima, explícita e determinada para a qual os dados são tratados no país de origem, não sendo admissível, por princípio, que possam ser tratados para finalidades diferentes. Qualquer utilização dos dados para uma finalidade diferente, embora no âmbito da

Directiva, deve ser autorizada pelo país de origem e apenas desde que não contrarie a sua legislação nacional. Este será outro requisito a ser introduzido no artigo 33.º.

Em terceiro lugar, as transferências ulteriores para outros países ou organizações só poderão ocorrer se o Estado de origem dos dados der a sua autorização expressa, a qual deve ser baseada na avaliação do nível de protecção de dados do segundo país de destino, bem como na garantia efectiva da aplicação de todas as condições exigíveis para a primeira transferência.

Estas autorizações do Estado de origem deverão ser documentadas.

Em quarto lugar, tal como prescrito no Princípio 5.5.i. da Recomendação R(87)15 do Conselho da Europa, os pedidos de transferência de dados devem conter as razões do pedido e o seu objectivo.

Quanto às condições específicas para a transferência de dados, urge reformular o artigo 37.º, introduzindo um conjunto de requisitos adicionais, designadamente a obrigação de o responsável pelo tratamento notificar o destinatário dos dados de qualquer actualização, rectificação ou apagamento dos dados e de este, por sua vez, caso tenha ocorrido transferência subsequente, proceder também a esta notificação, de modo a garantir que todo o circuito de circulação da informação mantém a qualidade dos dados.

Deveria ainda ser introduzida a obrigação de, na medida do possível, antes de se realizarem as transferências de dados, o responsável pelo tratamento verificar a qualidade dos dados e a classificação da informação em função do seu grau de fiabilidade, na linha das recomendações do Conselho da Europa[12].

De igual modo, a Proposta deveria conter uma norma específica que garantisse que o acesso directo ou acesso em linha a tratamentos de dados só poderia ser efectuado se respeitar a legislação nacional e com garantias, em particular a avaliação do princípio da proporcionalidade e a adopção de medidas de controlo dos dados consultados,

[12] Recomendação R(87)15 sobre o tratamento de dados no sector policial

bem como das pesquisas realizadas. Esta é uma tendência crescente, que comporta riscos acrescidos, pois franqueia as bases de dados pessoais a países terceiros.

A aplicação do princípio da necessidade de conhecer (*need-to-know basis*) por parte do destinatário dos dados deveria também constar das condições específicas do artigo 37.º.

Todas as transferências de dados devem ser documentadas.

No que diz respeito aos fundamentos de legitimidade para os fluxos de dados para países ou organizações terceiras, previstos nos artigos 34.º a 36.º da Proposta, considera-se ser de reformular a lógica do articulado, aproveitando simultaneamente para eliminar contradições e clarificar alguns aspectos.

Desde logo, independentemente do fundamento legal usado, as condições gerais e específicas devem ser aplicadas a todas as transferências de dados.

Por outro lado, a admissão das transferências de dados deveria ser preferencialmente baseada em disposição legal do Estado-Membro, da União ou lei internacional.

Quando não houver disposição habilitadora, as transferências de dados para autoridades policiais ou judiciárias devem ser reguladas por instrumento que vincule as partes, mesmo nas situações em que haja decisão de adequação da Comissão Europeia, uma vez que o facto de um país oferecer um nível de protecção de dados adequado não inviabiliza que as condições particulares da transferência tenham de ser regidas por acto que obrigue o país de origem e o país ou organização de destino dos dados pessoais. Quanto mais elevado for o nível de adequação, menor terá de ser a regulação em concreto. Todavia, a legislação nacional terá sempre de ser respeitada.

Quanto aos critérios gerais para a Comissão Europeia avaliar a adequação de um país terceiro ou organização internacional, previstos no n.º 2 do artigo 34.º parecem ajustados e deverão ser mantidos. Aliás, esses mesmos critérios gerais deveriam ser adoptados pelos Estados-Membros no âmbito da negociação de acordos bilaterais para a transferência de dados pessoais.

Porém, prevê-se que esta avaliação só seja feita *«na falta de uma decisão»* adoptada ao abrigo do que será o Regulamento de Protecção de Dados. Ora, este Regulamento tem um âmbito de aplicação distinto desta Proposta de Directiva e, embora esteja previsto que a Comissão Europeia avalie a legislação relevante em vigor no país terceiro, incluindo a que respeita à segurança pública, à segurança nacional e ao direito penal, o aproveitamento de uma decisão de adequação tomada por força do Regulamento em transferências internacionais para fins de cooperação policial e judiciária em matéria penal só poderá ser feito se a Comissão Europeia concluir pela existência de nível adequado de protecção de dados também nestes domínios, e não apenas nos sectores abrangidos pelo objecto do Regulamento.

Com efeito, um país terceiro poderá oferecer um nível de protecção adequado para os sectores abrangidos pelo Regulamento, o que não constituirá obstáculo à emissão de uma decisão de adequação nesse âmbito, mas não oferecer uma protecção equivalente no sector policial.

Quanto às derrogações previstas no artigo 36.º, elas devem ser interpretadas de forma restritiva, não permitindo transferências massivas e frequentes de dados, e ser limitadas ao estritamente necessário. Nesse sentido, sugere-se que isto seja clarificado ao nível dos Considerandos. Acresce ainda que as transferências decididas com base em derrogações devem estar devidamente documentadas, sugerindo-se a introdução desta medida adicional no artigo 36.º.

Relativamente à possibilidade de serem os próprios responsáveis pelo tratamento (autoridades policiais ou judiciárias competentes) ou subcontratantes a avaliar as garantias de protecção de dados num país terceiro, tal é inaceitável, pelo que a alínea b) do artigo 35.º deve ser eliminada. Com efeito, o responsável pelo tratamento não está obviamente em posição de fazer esse juízo, muito menos o subcontratante.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

6. Autoridades de controlo independentes e cooperação (Capítulo VI e VII)

O estatuto, competências, funções e poderes das autoridades nacionais de controlo de protecção de dados e a assistência mútua estão regulados nos artigos 39.º a 48.º da Proposta de Directiva.

É de salientar, antes de mais, que o artigo 16.º do TFUE dispõe que o controlo da aplicação das normas de protecção de dados pessoais é assegurado por *«autoridades independentes»*.

Com efeito, o artigo 40.º da Proposta enumera um conjunto de condições essenciais, com vista a garantir um estatuto de independência à autoridade de controlo de protecção de dados nos Estados-Membros, incluindo o dever de assegurar de que dispõe de *«recursos humanos, técnicos e financeiros apropriados, bem como de instalações e infra-estruturas, necessários à execução eficaz das suas funções e poderes»* (cf n.º 5).

O fornecimento de todos os meios necessários é uma questão crucial, assim como a existência de um quadro de pessoal próprio (n.º 6) e de um orçamento anual próprio (n.º 7). No entanto, a fim de garantir uma total independência de acção, deveria ser feito um aditamento que clarificasse que a autoridade de controlo deveria fazer a gestão do seu orçamento de forma integralmente autónoma. Por outro lado, também se deveria privilegiar a opção de o orçamento ser dotado por via dos parlamentos nacionais, de modo a diminuir o mais possível qualquer influência directa dos governos.

O artigo 41.º, que determina as condições aplicáveis aos membros da autoridade de controlo, suscita-nos duas reservas.

Uma primeira, relativa à forma de designação dos membros da autoridade (n.º 1), afigura-se ser desnecessariamente limitadora das possibilidades dos Estados-Membros, na medida em que prevê que os membros apenas possam ser designados pelo parlamento ou pelo governo, não admitindo sequer outras modalidades de designação (como por exemplo uma designação mista) que assegurem a

independência do exercício de funções e sejam mais conformes às tradições dos Estados-Membros.

Ademais, não parece ser o mais adequado que a designação dos membros da autoridade de controlo possa ser feita exclusivamente pelo governo, quando é ele que tutela as autoridades competentes aqui objecto de supervisão.

Uma segunda questão prende-se com a norma prevista no n.º 4, quanto à possibilidade de os membros perderem o *«seu direito à pensão ou a outros benefícios equivalentes por decisão de um tribunal nacional competente se deixar de preencher os requisitos necessários ao exercício das suas funções ou tiver cometido uma falta grave»*, o que não tem qualquer paralelo no ordenamento jurídico português e contraria a Constituição Portuguesa.

Na verdade, admite-se que o incumprimento ou violação de dever possam resultar em perda de mandato ou eventual procedimento criminal, mas nunca na perda de pensão ou benefício equivalente.

Assim sendo, o n.º 4 do artigo 41.º deveria ser reformulado, no sentido de deixar aos Estados-Membros, de acordo com o seu direito nacional, a escolha das sanções mais apropriadas, por remissão para a alínea g) do artigo 42.º.

Quanto às funções e poderes da autoridade de controlo (artigos 45.º e 46.º), ressalta desde logo que há uma diferença substancial entre os poderes atribuídos no âmbito da Proposta de Regulamento e da Proposta de Directiva, o que, na opinião da CNPD, não é aceitável.

Com efeito, os poderes conferidos às autoridades de controlo são bastante mais limitados na Proposta de Directiva, o que não se justifica, atendendo em particular à natureza sensível dos tratamentos de dados pessoais em causa, donde se evidencia até a necessidade de uma supervisão forte.

Nesse sentido, relativamente aos poderes da autoridade de controlo, deverá ser acrescentado no artigo 46.º o poder de ordenar ao responsável pelo tratamento (ou

subcontratante) que assegure o cumprimento do exercício dos direitos dos titulares; de ordenar ao responsável pelo tratamento (ou subcontratante) que supra, com medidas específicas, qualquer violação das disposições da presente Directiva; de ordenar ao responsável que forneça à autoridade de controlo qualquer informação considerada relevante para o desempenho das suas funções; de assegurar o cumprimento da consulta prévia prevista no artigo 26.º; o de suspender transferências de dados em violação das disposições da presente Directiva; o poder de aplicar sanções.

Ainda no que diz respeito aos poderes das autoridades, é indispensável que, à semelhança do que consta da Proposta de Regulamento Geral de Protecção de Dados[13] e de outros actos legislativos da União[14], fique expresso no texto desta Proposta de Directiva, que as autoridades de controlo, no uso dos seus poderes de investigação, podem aceder livremente às instalações do responsável pelo tratamento ou do subcontratante, e aos seus sistemas informáticos e dados pessoais neles contidos, bem como a qualquer documentação considerada relevante para o desempenho das suas funções.

A possibilidade de proceder a verificações no local, sem restrições de qualquer ordem, é crucial para o cumprimento das competências das autoridades de controlo. A redacção da alínea a) do artigo 46.º não é clara quanto a esta possibilidade, pelo que se impõe que o articulado reflicta inequivocamente esta prerrogativa.

Em suma, os poderes de investigação atribuídos às autoridades de controlo devem ser reforçados, no que diz respeito à possibilidade de inspeccionar *in situ* os sistemas de informação onde são tratados os dados pessoais, e os poderes de intervenção claramente fortalecidos, no sentido de abrangerem todos os aspectos da protecção de dados.

[13] No entanto, discorda-se igualmente da limitação existente na Proposta de Regulamento quanto a restringir as inspecções *in situ* apenas às situações em que exista um motivo razoável para presumir que é exercida uma actividade contrária às disposições do Regulamento.
[14] cf. Decisão Europol, Decisão Eurojust, Decisão Aduaneira, Regulamento 45/2001.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

O Considerando 56 da Proposta afirma a importância de as autoridades de controlo dos Estados-Membros terem os mesmos deveres e poderes efectivos, incluindo *«os poderes de investigação, de intervenção juridicamente vinculativa, de deliberação e de sanção»*. Contudo, tal declaração não foi plenamente transposta para o articulado. Por exemplo, apenas se prevê decisões vinculativas em situações extremas (como o apagamento ou a destruição dos dados ou a proibição temporária ou definitiva de um tratamento), quando na maioria dos casos não será necessário recorrer a medidas tão drásticas para fazer suprir eventuais violações das normas de protecção de dados.

C. Conclusões

1. A CNPD não pode deixar de se congratular com a iniciativa da Comissão Europeia de, com esta Proposta de Directiva, alargar o direito fundamental à protecção de dados pessoais aos domínios da cooperação policial e judiciária em matéria penal em todos os Estados-Membros, em cumprimento do Tratado de Lisboa.

2. A CNPD considera que, apesar da introdução de algumas normas positivas, o conjunto da Proposta apresenta um nível de protecção de dados inferior ao existente noutros instrumentos da União e do Conselho da Europa, do qual poderá resultar uma diminuição geral dos direitos e garantias das pessoas nalguns Estados-Membros, como é, entre outros, o caso de Portugal.

3. A CNPD sublinha que a Proposta de Directiva deve apontar para um elevado nível de protecção de dados, ao mesmo tempo que garante um elevado nível de segurança pública, reflectindo um normativo equilibrado conciliador de direitos.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

4. A CNPD reitera que a Proposta de Directiva, tendo em devida conta as especificidades inerentes aos tratamentos de dados relativos à cooperação policial e judiciária em matéria penal, deve almejar à maior consistência possível com a Proposta de Regulamento Geral de Protecção de Dados, dando solidez jurídica ao novo quadro legal de protecção de dados da União Europeia, num espaço que se pretende de livre circulação de dados.

5. A CNPD considera que o texto da Proposta de Directiva necessita de bastante aperfeiçoamento, quer ao nível da clarificação do articulado e dos Considerandos; quer ao nível da introdução de salvaguardas adicionais e de normas específicas mais ajustadas ao contexto da prevenção, investigação, detecção e repressão de infracções penais e da execução de sanções penais.

6. A CNPD, com base na sua longa experiência sobre o tratamento de dados pessoais no âmbito policial, no conhecimento profundo dos textos legais europeus e nas boas práticas europeias, fez uma análise detalhada da Proposta e apresenta recomendações concretas, contribuindo para uma melhoria substantiva do articulado.

É este o nosso Parecer.

Lisboa, 16 de Abril de 2012

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

Luís Lingnau da Silveira (Presidente, que relatou)