

## Parecer n.º 40 /2012

O Ministério dos Negócios Estrangeiros, através da Direção-Geral dos Assuntos Europeus, solicitou à CNPD que se pronunciasse sobre a Proposta alterada de Regulamento do Parlamento Europeu e do Conselho, relativo à criação do sistema EURODAC de comparação de impressões digitais para efeitos de determinação do Estado-Membro responsável pela análise de um pedido de asilo, e ao acesso pelas entidades policiais competentes dos Estados-Membros e pela Europol aos dados EURODAC<sup>1</sup>.

Em conformidade com o n.º 2 do artigo 22.º e com a alínea a) do n.º 1 do artigo 23.º da Lei n.º 67/98, de 26 de Outubro – Lei de Protecção de Dados (LPD), a CNPD é competente para emitir o respetivo parecer.

A Proposta alterada de Regulamento EURODAC (doravante, designada apenas por «Proposta») insere-se num quadro mais vasto, relativo ao Sistema Europeu Comum de Asilo, e resulta de propostas já apresentadas anteriormente pela Comissão Europeia, em Dezembro de 2008, Setembro de 2009 e Outubro de 2010.

<sup>1</sup> Reformulação da Proposta alterada de Regulamento do Parlamento Europeu e do Conselho relativo à criação do sistema «EURODAC» de comparação de impressões digitais para efeitos da efetiva aplicação do Regulamento (UE) n.º [...] [que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de asilo apresentado num dos Estados-Membros por um nacional de um país terceiro ou um apátrida] e a pedidos de comparação com os dados EURODAC apresentados pelas autoridades responsáveis dos Estados-Membros e pela Europol para fins de aplicação da lei e que altera o Regulamento (UE) n.º 1077/2011 do Parlamento Europeu e do Conselho que cria uma Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça – COM (2012) 254 final, de 30.5.2012.



## I Proposta

Esta Proposta vem revogar os regulamentos em vigor relativos ao sistema EURODAC<sup>2</sup>, juntando-os num único ato legislativo, vem alterar o Regulamento (UE) n.º 1077/2011 do Parlamento Europeu e do Conselho, de 25 de Outubro de 2011, que cria uma Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça, e vem introduzir a possibilidade de acesso aos dados EURODAC por parte das autoridades competentes dos Estados-Membros para a prevenção, deteção e investigação criminal e por parte da Europol (Serviço Europeu de Polícia).

Quanto às alterações ao Regulamento (UE) n.º 1077/2011, de 25 de Outubro de 2011, elas destinam-se tão só a ajustar o texto em conformidade com as novas referências legislativas e a conferir à Europol o estatuto de observador a nível do conselho de administração da Agência sempre que uma questão relacionada com o EURODAC figure na ordem de trabalhos, uma vez que a Europol passará a ter acesso aos dados EURODAC, o que não acontecia anteriormente.

Esta é uma alteração que não suscita qualquer comentário, pelo que não a analisaremos adiante.

No que diz respeito às alterações introduzidas pela Proposta ao atual quadro legal, a mais significativa é o acesso das forças policiais ao sistema EURODAC, que passarão a poder pedir comparações de impressões digitais, incluindo impressões digitais latentes recolhidas em locais de crime, com as armazenadas no sistema central EURODAC, cujo fim é facilitar o procedimento dos processos de asilo.

<sup>2</sup> Regulamento (CE) n.º 2725/2000 do Conselho, de 11 de Dezembro de 2000, relativo à criação do sistema «Eurodac» de comparação de impressões digitais para efeitos da aplicação efetiva da Convenção de Dublin, e Regulamento (CE) n.º 407/2002 do Conselho, de 28 de Fevereiro de 2002, que fixa determinadas regras de execução do Regulamento (CE) n.º 2725/2000 do Conselho, de 11 de Dezembro de 2000, relativo à criação do sistema «Eurodac» de comparação de impressões digitais para efeitos da aplicação efetiva da Convenção de Dublin.



Para habilitar as forças policiais a comparar estes vestígios de impressões digitais, será necessário proceder a alterações técnicas no sistema, adicionando-lhe essa nova funcionalidade, pois neste momento tal não é possível.

A Proposta prevê, no n.º 2 do artigo 1.º, que esses acessos sejam limitados para fins de prevenção, deteção e investigação de «infrações terroristas»<sup>3</sup> e outros «crimes graves»<sup>4</sup>.

Os Estados-Membros deverão designar as autoridades (artigo 5.º) que podem aceder aos dados EURODAC neste contexto, sendo que deverão ser autoridades competentes para os fins acima enunciados. Dentro destas, os Estados-Membros têm ainda de listar as unidades operacionais que estão autorizadas a solicitar comparações de impressões digitais. Será ainda designada por cada Estado-Membro uma entidade nacional (artigo 6.º), com igual competência, que servirá de «autoridade de controlo» para verificação da conformidade dos pedidos que lhe são remetidos pelas outras forças policiais com as condições de acesso.

A Proposta determina, no artigo 20.º, que só poderão ser comparadas impressões digitais na base de dados central do EURODAC, depois de pesquisadas as bases nacionais de dados dactiloscópicos e as de outros Estados-Membros, ao abrigo da chamada Decisão Prüm<sup>5</sup>, com resultados negativos, e sempre que o acesso seja necessário para fins de prevenção, deteção ou investigação de infrações terroristas ou outros crimes graves, seja necessário «num caso específico», não podendo ser efetuadas comparações sistemáticas, e existam motivos razoáveis para considerar

<sup>3</sup> Definidas pela legislação nacional como equivalentes aos crimes previstos nos artigos 1º a 4º da Decisão-Quadro 2002/475/JAI, de 13 de Junho de 2002, relativa à luta contra o terrorismo (cf. artigo 2.º, n.º 1, alínea j) da Proposta).

<sup>4</sup> Os crimes correspondentes ou equivalentes às infrações previstas no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI, de 13 de Junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros, «se forem puníveis com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos nos termos da legislação nacional» (cf. artigo 2.º, n.º 1, alínea k) da Proposta).

<sup>5</sup> Decisão 2008/615/JAI do Conselho



que o acesso aos dados EURODAC contribuirá significativamente para a prevenção, deteção ou investigação de qualquer dos crimes em causa.

Só a «autoridade de controlo» está autorizada a transmitir os pedidos de comparação de impressões digitais ao ponto nacional de acesso, que comunica com o Sistema Central EURODAC.

A Europol terá igualmente que designar uma «unidade operacional» autorizada a solicitar comparações com os dados EURODAC, e uma «unidade especializada», entre os seus funcionários, para desempenhar o papel de «autoridade de controlo».

As condições de acesso da Europol são diferentes das dos Estados-Membros, prevendo-se que os pedidos de comparação têm lugar se tal for necessário para o exercício das suas funções, nos termos da Decisão Europol, e para efeitos de uma análise específica ou de uma análise de natureza geral e de tipo estratégico.

Os seus pedidos serão reencaminhados para um ponto de acesso de um dos Estados-Membros, uma vez que não haverá ligação direta entre a Europol e o sistema EURODAC (artigo 7.º).

Todas estas comunicações e transmissões de dados se processam por via eletrónica, entre as autoridades de controlo e os pontos nacionais de acesso, sendo utilizada a infraestrutura de comunicação EURODAC. As impressões digitais são tratadas digitalmente e transmitidas num formato adequado que permita a comparação por sistema informatizado de reconhecimento de impressões digitais.

Está ainda previsto, no artigo 33.º da Proposta, que aos tratamentos de dados pessoais para fins policiais por força do presente regulamento se aplica, nos Estados-Membros, a Decisão-Quadro 2008/977/JAI, não podendo os dados ser tratados para outras finalidades. Aos dados pessoais obtidos a partir do EURODAC por um Estado-Membro ou pela Europol que não venham a ser necessários para efeitos de uma investigação criminal específica em curso são apagados dos ficheiros nacionais e dos ficheiros da Europol, após o período de um mês.



O artigo 35.º da Proposta proíbe a transferência ou disponibilização de dados pessoais obtidos por um Estado-Membro ou pela Europol a partir da base de dados central do EURODAC para países terceiros ou organizações internacionais ou entidades privadas estabelecidas na União Europeia ou fora dela, com exceção dos países terceiros que aplicam igualmente o Regulamento de Dublin.

Relativamente a outras alterações introduzidas pela Proposta ao regulamento em vigor, destacam-se a diminuição do prazo de conservação dos dados dos titulares da categoria 2 (nacionais de países terceiro ou apátridas intercetados por ocasião da passagem ilegal de uma fronteira externa) para 1 ano (n.º1 do artigo 16.º); a verificação por um perito em impressões digitais dos resultados da comparação havendo um acerto (n.º 4 do artigo 25.º); a marcação dos dados pessoais relativos a pessoas a quem já foi concedida proteção internacional, em vez do anterior bloqueio dos dados, passando a ser devolvido o resultado da comparação (artigo 18.º); a imposição de um prazo máximo de 72 horas para a transmissão dos dados dactiloscópicos e outros dados ao Sistema Central (n.º 1 do artigo 9.º e n.º 2 do artigo 14.º); a obrigação dos Estados-Membros manterem registos (*logs*) de todas as operações de tratamento para efeitos de auditoria e controlo de proteção de dados.

Foram ainda introduzidas algumas melhorias ao nível da prestação do direito de informação aos titulares dos dados, designadamente através da publicação de um folheto comum, bem como a obrigação do responsável pelo tratamento manter um registo escrito dos pedidos de direito de acesso (artigo 29.º).

É ainda proposto um modelo de supervisão coordenada do sistema EURODAC, entre a Autoridade Europeia de Proteção de Dados e as autoridades nacionais de proteção de dados (artigo 32.º).

Em suma, as alterações mais visíveis prendem-se com a passagem das funções de gestão do sistema EURODAC da Comissão Europeia para a Agência europeia para a gestão operacional dos sistemas informáticos de grande escala no espaço de



liberdade, segurança e justiça, que fará igualmente a gestão dos sistemas VIS e SIS II, e com a introdução do acesso pelas forças policiais aos dados EURODAC.

A Proposta agora em análise não regista alterações relevantes em relação ao quadro legal existente, além do alinhamento da terminologia com outros atos jurídicos e da atualização das referências legislativas.

## II Apreciação

O EURODAC é um sistema de informação europeu, em funcionamento desde 2003, criado com o objectivo de ajudar a determinar qual o Estado-Membro responsável pela análise de um pedido de asilo apresentado na União Europeia, sendo possível saber, por comparação com as impressões digitais, se um requerente de asilo ou um estrangeiro encontrado em situação ilegal no território ou a atravessar uma fronteira externa já tinha requerido anteriormente proteção internacional noutro Estado-Membro. Deste modo, é possível acelerar o procedimento de asilo, o qual decorre da aplicação do Regulamento de Dublin<sup>6</sup>.

De acordo com o Regulamento EURODAC, tem de se proceder à recolha das impressões digitais de todos os requerentes de asilo com mais de 14 anos de idade. Essas impressões digitais, de todos os dedos das mãos, são de seguida enviadas em formato digital à base de dados central do EURODAC. O sistema compara automaticamente as impressões digitais com outras já armazenadas, permitindo assim às autoridades controlar se o requerente já apresentou um pedido noutro Estado-Membro.

Além dos 27 Estados-Membros da União, fazem parte atualmente do sistema EURODAC a Noruega, a Islândia, a Suíça e o Liechtenstein, na medida em que também aplicam o Regulamento de Dublin.

<sup>6</sup> Regulamento (CE) n.º 343/2003 do Conselho, de 13 de Fevereiro de 2003, que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de asilo apresentado num dos Estados-Membros por um nacional de um país terceiro.



A Proposta agora em análise mantém como objetivo do sistema a ajuda na determinação do Estado-Membro responsável «*pela análise de um pedido de proteção internacional apresentado num Estado-Membro por um nacional de país terceiro ou apátrida, e em facilitar a aplicação do Regulamento de Dublin nos termos do presente regulamento*» (artigo 1.º, n.º 1).

No entanto, acrescenta como finalidade suplementar o estabelecimento de «*condições em que as autoridades designadas dos Estados-Membros e o Serviço Europeu de Polícia (Europol) podem solicitar a comparação dos dados dactiloscópicos com os dados conservados na base de dados central do EURODAC para fins de prevenção, deteção e investigação de infrações terroristas e outros crimes graves*» (artigo 1.º, n.º 2).

Ora esta nova possibilidade, introduzida pela Proposta, não pode deixar de merecer a total discordância por parte da CNPD, pelos riscos que comporta para os direitos fundamentais das pessoas, incluindo menores, que, por motivos humanitários vários, buscam proteção internacional nos Estados-Membros da União. Pode igualmente vir a pôr em causa o direito de asilo, consagrado no artigo 18.º da Carta Europeia dos Direitos Fundamentais, pelo receio legítimo dos requerentes que o seu exercício possa trazer consequências muito negativas por via deste acesso policial.

O sistema EURODAC foi criado com um propósito muito específico, de facilitação do procedimento de asilo, do qual resulta um benefício para os requerentes, que são assim obrigados a deixar recolher as suas impressões digitais.

O acesso a este sistema para fins policiais representa não só um desvio significativo da finalidade basilar da existência do EURODAC, como se afigura ser desproporcional, atenta a perspetiva de criminalização dos requerentes de asilo que se encontram já numa situação de grande vulnerabilidade, bem como os riscos decorrentes da informação destas pessoas acabar nos seus países de origem, com perigo de vida para as suas famílias aí residentes e para os próprios, caso não venham a ser beneficiários de proteção internacional e tenham de regressar.



Apesar da proibição genérica de transferência dos dados obtidos a partir do EURODAC para países terceiros ou organizações terceiras, no artigo 33.º da Proposta, a verdade é que não são contemplados mecanismos que efetivamente impeçam que, uma vez introduzidos nas bases de dados das polícias nacionais, os dados não sejam disponibilizados a terceiros, ao abrigo dos múltiplos acordos bilaterais ou multilaterais, e acabem tendo como destinatários os países de origem dos requerentes de asilo, seja direta ou indiretamente através de transferências de dados subsequentes.

A legislação dos Estados-Membros, no setor policial, é variável e será de acordo com essas normas que os dados serão tratados. Apesar da aplicabilidade da Decisão-Quadro 2008/977/JAI aos dados EURODAC no intercâmbio de dados entre Estados-Membros, ela admite a transferência posterior de dados a terceiros a partir de um Estado-Membro que foi destinatário da informação.

Por outro lado, os Estados-Membros têm já atualmente muitos mecanismos de cooperação policial ao seu dispor para fins de prevenção, deteção e investigação criminal, os quais assentam sobretudo na partilha de informações sobre suspeitos, mas também condenados, vítimas, associados, contactos ou testemunhas.

A possibilidade de acesso aos dados EURODAC corresponde a uma pesquisa sobre uma base de dados de não suspeitos, de pessoas sem antecedentes criminais, como é aliás admitido no Considerando 9 da Proposta; pelo contrário, trata-se de pessoas refugiadas e fragilizadas que procuram a proteção de um Estado de Direito.

O Considerando 2 da Proposta afirma que é objetivo da União Europeia estabelecer um espaço de liberdade, de segurança e de justiça *«aberto às pessoas que, forçadas pelas circunstâncias procuram legitimamente proteção internacional na União»*.

Por tudo isto, considera a CNPD que o sistema EURODAC deveria apenas cumprir a finalidade para a qual foi criado e que, pela natureza da sua função, implica o tratamento de um vasto conjunto de impressões digitais, não por razões de índole criminal, mas porque muitos dos requerentes não possuem identificação suficiente.

Cumpra agora analisar em concreto as disposições da Proposta mais relevantes, no âmbito das alterações introduzidas.

## 1. Acesso para fins policiais

Na Exposição de Motivos da Proposta, é afirmado que a utilização dos dados EURODAC para fins policiais constitui uma «*ingerência*» no direito à proteção de dados, pelo que «*a legislação que impõe tal restrição deve ser redigida com uma precisão suficiente para permitir às pessoas adaptar a sua conduta e para as proteger contra situações arbitrárias. Deve igualmente indicar com suficiente clareza o grau de discricionariedade conferido às autoridades competentes e as modalidades do seu exercício*».

No entanto, do articulado da Proposta não resulta a clareza pretendida e necessária, havendo mesmo algumas omissões quanto aos procedimentos concretos no que diz respeito à comparação das impressões digitais neste âmbito. Por outro lado, como se verá adiante, não está suficientemente salvaguardada, na prática, a limitação dos acessos com base nas condições impostas.

### a. Catálogo de crimes

A Proposta, no Considerando 9, afirma que as autoridades policiais podem ter acesso ao sistema em «*casos bem definidos*», em que a repreensibilidade do ato criminoso seja suficiente para justificar a pesquisa na base de dados, concluindo que «*o limiar a respeitar pelas autoridades responsáveis pela segurança interna para consultar o EURODAC deve ser, portanto, significativamente superior ao limiar que se deve respeitar para consultar bases de dados criminais*» [sublinhado nosso].

Todavia, o catálogo de crimes que dá acesso aos dados EURODAC remete para as infrações terroristas, previstas na Decisão-Quadro 2002/475/JAI, e que incluem infrações conexas, e para o vasto elenco de crimes abrangidos pelo mandado de

detenção europeu, nos quais se incluem burla, corrupção, falsificação de documentos administrativos, falsificação de meios de pagamento, desde que puníveis com pena de prisão de duração máxima não inferior a três anos, nos termos da legislação nacional.

Se é entendível a remissão para catálogos de crimes já definidos ao nível da União, por questões de segurança jurídica, entende a CNPD não haver nesta opção o estabelecimento do propalado limiar significativamente superior. A adição de um limite na pena em caso de crimes graves não é suficiente, atento o prazo previsto, além de suscitar diferenciações indesejáveis entre os Estados-Membros nos critérios de acesso ao EURODAC, na medida em que as legislações nacionais têm diferentes molduras penais para o mesmo tipo de crime.

Por outro lado, não estando a Europol abrangida sequer pela definição de crimes graves, pois há remissão para a legislação nacional, e estando habilitada a solicitar dados no âmbito das suas competências (artigo 21.º), a Europol poderá assim aceder aos dados EURODAC em situação muito “mais vantajosa” do que os EM, porque pode tratar dados pessoais relativos aos crimes do seu mandato e a todos os crimes conexos, o que lhe confere a possibilidade de aceder a dados de modo quase ilimitado.

Acresce ainda que este acesso pode desvirtuar as restrições impostas aos EM, pelo facto de os dados tratados pela Europol poderem ser partilhados pelos EM em momento posterior.

Nesse sentido, deveria pois ser substancialmente reduzida a lista de infrações penais que dariam acesso ao sistema EURODAC, igualmente aplicável aos EM e à Europol, de modo a alcançar a proporcionalidade desejada e desejável.

#### b. Papel da autoridade de controlo

O artigo 6.º da Proposta prevê a designação pelos EM de uma única entidade nacional, que seja competente para a prevenção, deteção ou investigação de

infrações terroristas ou outros crimes graves, para funcionar como a «autoridade de controlo», incumbida de receber os pedidos de acesso ao EURODAC das várias autoridades policiais nacionais, verificar a sua observância com as condições impostas para o acesso, transmitir os pedidos de comparação de impressões digitais ao ponto nacional de acesso (autoridade competente para aceder diretamente ao sistema EURODAC para os fins da aplicação do Regulamento de Dublin) e receber as respostas do sistema pelo percurso inverso.

Em primeiro lugar, uma nota relativamente ao termo «autoridade de controlo», habitualmente usado para identificar as autoridades de protecção de dados e inclusive usado nesse sentido no texto da própria Proposta, pelo que pode criar uma confusão indesejável, sugerindo-se por isso uma outra designação.

Em segundo lugar, considera-se que a atribuição a uma autoridade policial da tarefa de verificar a legalidade dos pedidos de pesquisa no sistema EURODAC, feitos por outras autoridades policiais, é claramente desajustada e de eficácia duvidosa.

Todo o quadro de garantias previsto para admitir a excecionalidade do acesso ao EURODAC pelas polícias assenta no cumprimento das condições impostas pelo regulamento, que são cumulativas, designadamente a aferição da necessidade da consulta num caso específico e dos *«motivos razoáveis para considerar que a comparação com os dados EURODAC contribuirá significativamente para a prevenção, deteção ou investigação de qualquer dos crimes em causa»*.

É evidente que colocar uma autoridade policial, parte interessada no acesso – a autoridade de controlo poderá mesmo ter de verificar pedidos provenientes de unidades operacionais que integram a sua própria entidade – a realizar um juízo imparcial sobre o cumprimento dos requisitos para aceder não se afigura razoável nem assegura, à partida, o correto desempenho dessa função.

A verificação da legalidade do acesso aos dados EURODAC, através da apreciação da observância das condições determinadas pelo artigo 20.º da Proposta deveria ser atribuída às autoridades judiciais.



### c. Condições de acesso da Europol

A situação é ainda mais questionável no que diz respeito à Europol, que terá de designar no seu seio uma unidade operacional para solicitar os dados EURODAC e uma outra unidade especializada, constituída igualmente por funcionários, para controlar a legalidade dos pedidos da primeira (artigo 7.º).

Por outro lado, as condições para a Europol aceder ao sistema EURODAC são substancialmente menos exigentes do que as impostas aos EM. Além de não existir o mecanismo de pesquisa Prüm, etapa prévia obrigatória para os EM, a Europol poderá pedir a comparação de impressões digitais para efeitos de *«uma análise específica»* ou de *«uma análise de natureza geral e de tipo estratégico»* (artigo 21.º).

Ora, a aplicação do princípio da necessidade, com vista a excluir a comparação sistemática de grandes volumes de dados, consagrado no Considerando 26 da Proposta, que afirma dever o pedido de comparação de impressões digitais estar associado *«a uma situação específica e concreta ou a um perigo específico e concreto»* e se *«existirem motivos razoáveis para considerar que essa comparação permitirá obter informações que contribuirão efetivamente para a prevenção, deteção ou investigação (...)»*, não está devidamente acautelada na redação do articulado.

Com efeito, tendo em conta a natureza do trabalho desenvolvido pela Europol, o desenvolvimento de análise criminal muito raramente terá equivalência no «caso específico» investigado pelos EM. Ademais, as análises de natureza geral e de tipo estratégico, como a própria designação indica, estão longe de reunir os critérios de perigo específico e concreto, em que a Proposta se sustenta para permitir o acesso ao sistema EURODAC para fins policiais.

Assim sendo, considera-se que as condições de acesso aos dados EURODAC pela Europol não respeitam de todo os princípios de necessidade e proporcionalidade aplicáveis. Na verdade, a própria fundamentação para o acesso da Europol é genérica e frágil, pois assenta tão só na declaração do seu *«papel primordial na cooperação*

entre as autoridades dos EM responsáveis pelas investigações sobre atividades criminosas transfronteiras» (Considerando 10).

#### d. Comparação e transmissão do resultado

A Proposta descreve com pormenor os procedimentos relativos aos pedidos de comparação de impressões digitais com os dados dactiloscópicos armazenados no Sistema Central. Determina ainda que as consultas feitas para fins policiais fazem comparação com todos os dados EURODAC, ou seja, com os dados dos titulares de categoria 1 e 2. Todavia, não explicita como se processa a transmissão do resultado.

A Exposição de Motivos refere haver uma resposta do sistema tipo *hit/no hit* (acerto/não acerto), mas no articulado a modalidade de resposta não está expressa, como também nada é dito sobre quais os dados transmitidos.

Por outro lado, também não está previsto como são referenciadas as comparações feitas com base em pedidos das polícias. Uma vez que o número de referência atribuído pelo EM nas comparações habituais tem de indicar a categoria de titulares a que se refere, presume-se que os pedidos para fins policiais venham a ter uma referência diferenciada.

Nenhum destes aspetos está regulado na Proposta e é essencial que assim seja, a bem da transparência e da segurança jurídica, tornando igualmente possível auditar os pedidos realizados neste âmbito.

#### e. Impressões digitais latentes

No que diz respeito à transmissão de impressões digitais latentes, uma possibilidade inexistente neste momento, em que são comparadas as impressões digitais de todos os dedos das mãos, também nada é particularmente regulado, a não ser que as normas técnicas serão posteriormente desenvolvidas pela Agência.



Contudo, esta é uma questão relevante, pois pode suscitar problemas de qualidade dos dados ao nível do aumento de falsos positivos, o que poderia ter um impacto muito negativo sobre os requerentes ou beneficiários de protecção internacional.

A este propósito, além da obrigação geral de os EM transmitirem dados com qualidade, deveriam ser introduzidas salvaguardas específicas para o tratamento dos resultados positivos obtidos quando a consulta tiver tido na sua origem o envio de impressões digitais latentes.

## 2. Estatísticas

A Proposta prevê, no artigo 8.º, que a Agência elabore estatísticas mensais sobre o trabalho desenvolvido pelo Sistema Central. Essas estatísticas deverão conter um conjunto de dados, designadamente o número de acertos por categoria de titulares de dados.

Considera-se que a Proposta deveria igualmente conter a exigência da realização de estatísticas, por EM, sobre o número de pedidos de comparação feitos para fins policiais e do número de acertos conseguidos, por categorias dos titulares dos dados, com distinção dos pedidos e acertos que foram realizados com base em impressões digitais latentes.

Apesar de estar prevista na Proposta a elaboração de estatísticas a nível nacional, considera-se que a produção de estatísticas de forma automática ao nível do Sistema Central será mais adequada e inequívoca.

A existência de estatísticas corretas sobre a utilização do EURODAC para fins policiais é imprescindível para avaliar o cumprimento das disposições do regulamento.

Ainda no plano estatístico, deveria estar prevista a elaboração de estatísticas quanto ao número de consultas realizadas ao sistema, no âmbito do exercício do direito de acesso.

### 3. Direitos dos titulares dos dados

O artigo 29.º da Proposta retoma, em grande parte, o texto atual do Regulamento EURODAC quanto aos direitos dos titulares dos dados, tendo apenas introduzido como novidade a publicação de um folheto comum com a prestação do direito de informação, redigido de forma clara e simples e numa língua que a pessoa compreenda, e na necessidade de fornecer aos menores as informações necessárias de forma adaptada à sua idade.

A CNPD entende que seria de aproveitar a oportunidade de alteração do Regulamento EURODAC para clarificar no texto os direitos dos titulares, bem como junto de que Estado-Membro podem exercer os seus direitos. O texto da Proposta ao reproduzir quase na totalidade o texto atual do Regulamento afigura-se confuso, pelo que se recomenda o seu aperfeiçoamento.

Sugere-se ainda que, no n.º2 do artigo, a remissão para o artigo 12.º da Diretiva 95/46/CE, de 25 de Outubro, seja substituída pela afirmação expressa de que os titulares dos dados têm o direito de aceder aos dados pessoais que lhe dizem respeito, não só porque explicita o exercício do direito de acesso como evita uma referência legislativa que ficará desatualizada no futuro próximo, com a revisão do quadro legal de proteção de dados em curso.

Além disso, é essencial que a Proposta introduza a obrigação expressa de o responsável pelo tratamento de dados informar o titular dos dados da possibilidade de recorrer para a autoridade nacional de proteção de dados, para o assistir no exercício dos seus direitos, em particular quando um EM se recusar a retificar ou apagar os dados no seguimento de um pedido de retificação ou eliminação.

### 4. Supervisão do sistema

A Proposta introduz um figurino de supervisão «*coordenada*» do sistema EURODAC entre a Autoridade Europeia de Proteção de Dados (AEPD) e as autoridades nacionais



de protecção de dados, tendo em conta que atribui à AEPD a supervisão do Sistema Central e às autoridades nacionais a supervisão nos respetivos Estados-Membros (artigo 32.º).

Para o efeito, é criado um grupo específico, com regulamento interno de funcionamento, reuniões pelo menos duas vezes por ano, a expensas da AEPD e utilizando o seu apoio de secretariado, e que fará um relatório conjunto de atividades.

A cooperação prevista assenta na troca de informações relevantes, na análise das dificuldades de interpretação ou aplicação do regulamento, nos problemas do exercício dos direitos dos titulares, na elaboração de propostas harmonizadas para encontrar soluções comuns, sensibilização para os direitos em matéria de protecção de dados e, por último, na assistência mútua para a realização de auditorias e inspeções.

A este propósito, é de salientar que a revisão do quadro legal de protecção de dados na União, bem como as alterações a vários atos legislativos que criam sistemas de informação europeus, resultantes do Tratado de Lisboa, vão trazer certamente modificações profundas ao nível da supervisão destes sistemas.

Nessa medida, estão em curso vários debates entre a comunidade de protecção de dados e outros intervenientes quanto à escolha de um modelo de supervisão mais adequado, mais eficaz, através do aproveitamento de sinergias, menos dispendioso, mais consolidado e mais consentâneo com a natureza dos próprios sistemas de informação europeus, na perspetiva de protecção de dados. Nesse sentido, não se pode ignorar que a maioria dos sistemas europeus, incluindo o EURODAC, é alimentada exclusivamente pelos dados introduzidos pelos EM, sendo estes os únicos responsáveis pela qualidade dos dados, pela sua retificação ou apagamento. Também é junto das autoridades competentes dos EM que são exercidos os direitos dos titulares dos dados, tendo como eventuais mediadoras as autoridades de protecção de dados.



A maioria dos sistemas centrais corresponde a um repositório de informação dos vários EM que, por se encontrar centralizada, facilita a sua partilha entre os EM. Aliás, a Comissão Europeia ou agora a Agência limitam-se a gerir as plataformas eletrónicas que suportam os sistemas, fazendo-o em nome dos EM.

Aliás, é também nas autoridades nacionais de protecção de dados que existe a experiência e a *expertise* técnica para a realização de auditorias e inspeções, o que têm vindo a fazer há cerca de quinze anos, ao criar uma bolsa de peritos com a disponibilização dos seus técnicos de informática para as ações de inspeção dos sistemas centrais europeus.

Neste quadro atual de mudança, em que se pretende, por um lado, uma aproximação horizontal ao nível da supervisão dos vários sistemas europeus, por outro, que o modelo futuro de supervisão reflecta a realidade do funcionamento dos sistemas que assenta no tratamento de dados da responsabilidade de cada EM, não faz sentido que se esteja a criar mais um grupo, pulverizando ainda mais o universo de entidades de supervisão de protecção de dados.

Com efeito, as formas de cooperação previstas no n.º 2 do artigo 32.º são facilmente alcançáveis no âmbito do atual Grupo do Artigo 29.º (instituído pela Diretiva de Protecção de Dados e que congrega todas as autoridades de protecção de dados), como o poderá ser ainda melhor no futuro *Data Protection Board* (DPB), previsto na Proposta de Regulamento e de Diretiva de Protecção de Dados, com fortes competências de coordenação e cooperação entre as autoridades nacionais de protecção de dados.

A natureza e estrutura do DPB estão ainda em fase de discussão e de desenvolvimento, encontrando-se em aberto a possibilidade de poder vir a adquirir mesmo uma componente de supervisão conjunta (e não só coordenada) dos sistemas europeus.

Nessa medida, e tendo em consideração as alterações que se irão produzir num futuro muito próximo, a Proposta deveria abster-se de criar mais um grupo ou um

determinado figurino de supervisão, limitando-se a remeter a necessária cooperação para a plataforma de proteção de dados, que reúne todas as autoridades de proteção de dados, incluindo as dos quatro países que neste momento aplicam o Regulamento de Dublin.

#### 5. Segurança dos dados

○ Quanto à segurança dos dados, constante do artigo 34.º da Proposta, as obrigações impostas aos EM parecem adequadas.

Suscita-se, no entanto, a questão de não estar devidamente clarificado a quem incumbe garantir a segurança dos dados durante a sua transmissão para o Sistema Central. Se o artigo 34.º atribui essa responsabilidade ao Estado-Membro, o artigo 4.º, sobre a gestão operacional do EURODAC, atribui à Agência a responsabilidade da segurança da infraestrutura de comunicação (alínea b) do n.º 2 do artigo 4.º), que é o canal de transmissão dos dados.

#### 6. Questões ausentes da Proposta

○ A reformulação do Regulamento EURODAC seria uma excelente oportunidade para introduzir no texto legislativo, de forma mais harmonizada, algumas garantias dos direitos dos requerentes de proteção internacional que a prática na aplicação do regulamento tem demonstrado não existirem ao nível dos Estados-Membros.

Em primeiro lugar, o limite mínimo de 14 anos para a recolha de impressões digitais tem colocado alguns problemas aos EM na determinação da idade dos requerentes menores, sempre que estes não detêm documentos de identificação que comprovem a sua idade.

Para esse fim, alguns EM utilizam vários métodos, o que se traduz numa grande diversidade de resultados, com implicações óbvias na equidade de tratamento das

peças em causa. Por outro lado, alguns dos métodos usados, incluindo a submissão dos menores a testes médicos invasivos, levanta um conjunto de problemas éticos e de fiabilidade.

Por conseguinte, a Proposta deveria conter obrigações para os EM, no sentido de assegurar uniformização e fiabilidade dos métodos escolhidos, de não permitir que a recusa em se submeter a um exame médico para determinação da idade possa prejudicar o requerente de asilo, de salvaguardar que as autoridades competentes tenham em conta a margem de erro de alguns testes ao tomarem decisões que afetem o estatuto jurídico dos requerentes menores.

Em segundo lugar, coloca-se a questão dos requerentes de proteção internacional, cujas impressões digitais não conseguem ser recolhidas por se encontrarem danificadas, seja por motivos de trabalho, guerra ou razões de saúde, seja porque foram adulteradas intencionalmente.

A Proposta introduz um prazo máximo de 72 horas para a transmissão de impressões digitais desde a sua recolha. Se houver impossibilidade em recolher impressões digitais, por estarem corrompidas, não é possível fazer a verificação no sistema EURODAC, o que poderá levar nalguns EM à recusa liminar da concessão do asilo.

Seria pois essencial que a Proposta contivesse algumas salvaguardas quanto a esta situação, semelhantes às constantes das Instruções Consulares Comuns, designadamente que o simples facto de o requerente ter impressões digitais danificadas não deve ter efeitos adversos no seu pedido. Deveria ainda ser prevista a aplicação pelos EM de um procedimento uniforme para lidar com estes casos.

### III Conclusões

1. A CNPD considera que o acesso ao sistema EURODAC pelas forças policiais é desproporcional, porque põe em causa os direitos fundamentais dos requerentes de proteção internacional, tratando como suspeitas pessoas sem

antecedentes criminais e em estado de grande vulnerabilidade, além de comportar riscos de a informação ser transmitida ao seu país de origem, o que pode fazer perigar a vida das suas famílias e a deles próprios, caso tenham de regressar.

2. A proibição genérica de transferência de dados para países ou organizações terceiras não tem os mecanismos de salvaguarda suficientes para evitar que, na prática, os dados depois de inseridos nas bases de dados nacionais não possam ser disponibilizados a terceiros.
3. A CNPD entende que o catálogo de crimes que permitem o acesso para fins policiais deveria ser mais restrito, e igualmente aplicável aos EM e à Europol, de modo a poder cumprir o limiar superior de justificação da consulta aos dados EURODAC relativamente às bases de dados criminais.
4. As autoridades de controlo, incumbidas para verificar a legalidade dos pedidos de acesso ao sistema, sendo autoridades policiais, não reúnem os requisitos necessários para ajuizar do cumprimento das condições para o acesso. Tal verificação deveria estar a cargo de autoridades judiciárias.
5. A modalidade e o conteúdo da resposta do sistema EURODAC aos pedidos das autoridades policiais deveriam estar devidamente regulados, bem como as garantias quanto ao tratamento de dados de resultados positivos, retornados de pesquisas feitas com base em impressões digitais latentes.
6. A elaboração de estatísticas do Sistema Central deveria ser mais completa, tendo em vista englobar o número de pedidos e acertos para fins policiais, com distinção dos pedidos com impressões digitais latentes, por categorias de titulares e por EM.

7. A CNPD considera que o texto sobre os direitos dos titulares dos dados deveria ser aperfeiçoado e clarificado, incluindo a prestação de informação aos requerentes sobre as autoridades nacionais de protecção de dados e respetivos contactos para assistência no exercício dos direitos.
8. A CNPD considera que é inoportuna, em vésperas de revisão do quadro legal de protecção de dados e de vários atos legislativos relativos a sistemas de informação europeus, a criação de mais um grupo específico para facilitar a cooperação entre a AEPD e as autoridades nacionais de protecção de dados, quando está em discussão um novo modelo de supervisão. A cooperação necessária poderá ser facilmente assegurada na plataforma já existente e que reúne todas as autoridades de protecção de dados.
9. A Proposta deveria conter normas harmonizadas e garantias quanto aos métodos a que são submetidos os menores para determinação da sua idade, com vista à recolha de impressões digitais.
10. A Proposta deveria conter igualmente regras harmonizadas para o tratamento dos casos em que as impressões digitais dos requerentes estão danificadas e não podem, por isso, ser recolhidas para comparação com o sistema EURODAC, não devendo daí resultar efeito adverso para os requerentes de protecção internacional.

Lisboa, 9 de julho de 2012

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



Filipa Calvão (Presidente)