Agradecimentos

Agradeço a todos aqueles que sempre estiveram presentes e de alguma forma me deram a força e coragem para alcançar mais esta etapa que chega agora ao fim.

Quero, em primeiro lugar, agradecer aos meus Pais, por me terem dado as "ferramentas" necessárias para a minha vida, aqueles que me ensinaram que todos os sonhos são realizáveis, basta querer.

Um muito obrigada à minha família, amigos e namorado, que sempre me incentivaram a alcançar os meus objetivos.

Em segundo lugar quero agradecer ao Professor Doutor André Ventura por ter aceite orientar esta dissertação, permitindo-me, assim, concluir esta etapa.

O meu sincero obrigada!

Resumo

Com a presente dissertação pretende-se contribuir para aprofundar o estudo e conhecimento quanto à importância que a base de dados *Passenger Name Record* teve, como meio de investigação criminal, na União Europeia.

Para tanto, entendeu-se iniciar o estudo por um breve enquadramento histórico sobre o Espaço de Liberdade, Segurança e Justiça na União Europeia, a fim de compreender em que consiste a luta contra a criminalidade no espaço Europeu, e ainda, como se processa o intercâmbio de informações neste espaço.

De seguida, pretendeu-se proceder à análise minuciosa da base de dados Passenger Name Record – daqui em diante designada por PNR -, recorrendo-se à doutrina nacional e internacional, bem como a jurisprudência internacional e a outras fontes consideradas de grande relevância para o tema.

Por último, concluiu-se pelas vantagens da criação de um sistema europeu de PNR, enunciando-se os vários contributos que este trouxe para a investigação criminal e sugerindo-se aspetos a melhorar, por forma a tornar mais eficiente a utilidade do PNR na luta contra a criminalidade.

Palavras-chave: PNR, Protecção de dados, União Europeia

Abstract

With the present dissertation´s aims to contribute to further study and knowledge about the importance of the Passenger Name Record database was as a means of criminal investigation in the European Union.

Therefore, it was considered to start the study by a brief historical background on the Area of Freedom, Security and Justice in the European Union, in order to understand what is the fight against crime in the European space, and also how they can be exchange of information in this space.

Then it intended to undertake a very careful analysis of the database Passenger Name Record - hereinafter referred to as *PNR* - resorting to national and international doctrine and international jurisprudence and other sources, believed to be of great relevance to the theme.

Finally, it was concluded by the advantages of setting up a European PNR system, the various contributions that this has brought to the criminal investigation and suggesting up aspects to improve if enunciating-in order to make more efficient PNR usefulness in the fight against crime.

Keywords: PNR, Data Protection, European Union

ÍNDICE

Capítulo II – O Passenger Name Record

Capítulo III – A criação de um sistema Europeu de PNR

Capítulo IV

Lista de Siglas e Abreviaturas

ADN	Ácido Desoxirribonucleico
AIRIMP	Reservations Interline Message Procedures Passenger
API	Passenger Advanced Information
ATS	Automated Targeting System
ATS-PIA/ATS-P	Privacy Impact Assessment
ATS SORN	System of Records Notices
CECA	Comunidade Europeia do Carvão e do Aço
CEPOL	Academia Europeia de Polícia
COSI	Comité Permanente para a Cooperação Operacional em matéria de Segurança Interna
C.R.P.	Constituição da República Portuguesa
CRS	Computer Reservation Systems
DCS	Departure Control Systems
DEI	Decisão de Execução e Investigação
EC3	Centro Europeu da Ciber Criminalidade
EUA	Estados Unidos da América
EUROPOL	Serviço Europeu de Polícia
FOIA	Freedom of Information Act
GDS	Global Distribution Systems
iOCTA	Criminalidade Organizada Dinamizada pela Internet
INMLCF, I.P.	Instituto Nacional de Medicina Legal
INTCEN	Centro de Análise de Informações da União Europeia
IATA	Passenger Services Conference Resolutions Manual
JAI	Justiça e Assuntos Internos
MEOP	Mandado Europeu de Obtenção de Provas

ONU	Organização das Nações Unidas
PAXLST	Passenger List Message
PE	Parlamento Europeu
PIU	Passenger Information Units
PNR	Passenger Name Record
SEAE	Serviço Europeu para a Ação Externa
SIS	Sistema de Informação Schengen
TCE	Tratado da Comunidade Europeia
UE	União Europeia
UIP	Unidade de Informações de Passageiros

Nota: A presente dissertação obedece às regras ditadas pelo Acordo Ortográfico da Língua Portuguesa de 8 de dezembro de 1945 e respetivas alterações.

Introdução

1. Importância do Tema: Objetivos da Investigação

Com o fenómeno da globalização abriram-se as "portas" de acesso a todo o Mundo.

Hoje em dia as pessoas viajam, trabalham, estudam e vivem no estrangeiro, ou seja, têm a possibilidade de escolher onde querem fixar a sua vida ou, apenas, onde querem passar as suas férias.

Contudo, nem sempre estas pessoas que escolhem viajar ou ter uma vida "lá fora", são pessoas de boa fé, cujas intenções são de mero enriquecimento pessoal.

Nessas viagens, muitas das vezes, também partem criminosos, facto esse que constitui o propósito desta tese.

Com o fenómeno da globalização, como acima foi referido, a criminalidade tornou-se um fenómeno internacional e de uma sofisticação, muitas vezes, para lá do que a imaginação humana consegue conceber.

Desta forma, esta dissertação pretende auxiliar a investigação criminal, percebendo que é possível alcançar a verdade dos factos de uma forma mais rápida, eficaz sem que, para isso, se lese a integridade física do suspeito.

O objectivo desta dissertação é mostrar a importância do desenvolvimento de um espaço de justiça penal europeu comum, onde predomine a confiança mútua e onde as autoridades policiais nacionais possam cooperar entre si.

Assim, numa primeira fase, será feito um enquadramento do tema, analisando o espaço de Liberdade, Segurança e Justiça da União Europeia de modo a perceber que espaço é este e quais as vantagens que ele traz ao intercâmbio de informações como instrumento de cooperação policial na União Europeia.

De seguida, a análise passará para, aquela que é, a questão essencial da dissertação, o *Passenger Name Record*. É neste segundo capítulo que se irá analisar e perceber detalhadamente em que consiste esta base de dados, quais os seus objetivos e quais são as suas funções.

Ou seja, neste capítulo será demostrada a importância que o PNR terá para a investigação criminal, nomeadamente para a União Europeia, no combate ao terrorismo e à criminalidade organizada transnacional.

Por último, num terceiro capítulo, será estudada a criação de um sistema Europeu de *Passenger Name Record*, dando a conhecer as vantagens da sua utilização no âmbito da investigação criminal.

O objetivo principal desta investigação é perceber as vantagens da criação de uma base de dados, que contém todas as informações necessárias sobre as pessoas que circulam por todo o território da União Europeia, contribuindo para que, de uma forma mais rápida e eficaz, se consiga obter resultados satisfatórios no quadro da pequena, média e alta criminalidade.

Nesta dissertação será, igualmente analisada a problemática da coexistência da Segurança com a Privacidade e a importância e a forma como é garantida a salvaguarda dos dados pessoais das pessoas que circulam por todo o espaço da União Europeia.

O objetivo é chegar à conclusão de que tudo isto só será possível respeitando o princípio do reconhecimento mútuo das decisões judiciais em todos os Estados-Membros da União Europeia.

2. Questões da Investigação

Com a análise deste tema, o objetivo é encontrar novas possibilidades de investigação criminal sem lesar o direito à privacidade de cada pessoa.

No entanto, o PNR europeu deve ser criado tendo sempre em consideração a proteção de dados.

As principais questões deste tema são:

1. Perceber qual o contributo que a base de dados PNR traz para a investigação criminal no âmbito da União Europeia;
2. Como conciliar o aumento da segurança no espaço europeu com a proteção dos direitos fundamentais;
3. Perceber se a União Europeia se encontra devidamente preparada para ter uma base de dados PNR.

3. Metodologia de Investigação

De acordo com os ensinamentos de Adilah Abd Razak, a investigação é um processo sistemático, completo e rigoroso, que aumenta o conhecimento (Collis and Hussey, 2003 *apud* Adilah Abd Razak, 2009: 19).

A investigação jurídica, de acordo com os ensinamentos de Adilah Abd Razak, compreende a análise e posterior explicação de novos estatutos, novos regimes legais ou, apenas, interpretar e criticar situações específicas.

Através da investigação jurídica pretende-se alcançar um padrão legal, que explica ou justifica um conjunto específico de regimes jurídicos.

Como é, por exemplo, o caso desta dissertação, em que são analisados os regimes jurídicos que deram origem ao PNR.

Através da investigação jurídica foi possível interpretar a doutrina jurídica relevante, e, consequentemente, analisar as causas e as consequências.

O resultado da investigação consiste em adquirir um minucioso grau de compreensão do assunto em análise, permitindo alcançar uma elevada capacidade de argumentação sobre o mesmo.

Quanto ao formato da investigação jurídica, esta foi dividida em investigação doutrinária e não doutrinária (McConville and Wing 2007 apud Adilah Abd Razak, 2009: 20).

A investigação não doutrinária pode ser qualitativa ou quantitativa, enquanto que a doutrinária é qualitativa, uma vez que não envolve a análise estatística de dados.

É possível que estes dois tipos de investigação se possam sobrepor.

No entanto, existe um terceiro tipo de investigação que é uma combinação de ambas, que utiliza um método comparativo.

A investigação utilizada para a realização deste trabalho foi a metodologia doutrinária, pois foi a que nos pareceu mais adequada e mais útil para chegar às respostas das perguntas a que nos propusemos responder.

De acordo com Adilah Abd Razak, este tipo de investigação permite a análise da lei em relação a uma questão em particular, sendo este tipo de investigação também designado por investigação teórica pura.

Esta é uma investigação simples, orientada para uma análise mais aprofundada e mais complexa e mais centrada no raciocínio legal. (McConville and Wing, 2007 apud Adilah Abd Razak, 2009: 20).

Assim, para este estudo, partiu-se de várias bases legislativas percebendo o que esteve na origem de uma base de dados como o *Passenger Name Record* na União Europeia.

Por último, temos o terceiro formato de investigação, que é a investigação jurídica comparativa.

"Este é um formato usado para estudar os textos legislativos, em particular, leis estrangeiras, jurisprudência e também doutrina."[1]

Assim, esta pesquisa serve para, através da comparação das legislações de diferentes sistemas jurídicos, fornecer ideias e opiniões para o desenvolvimento legal futuro.

Ora, através dessa análise, foram dadas sugestões, na conclusão final, quanto às questões que devem ser melhoradas a propósito da base de dados que é o cerne deste estudo.

5. O Projeto e o Processo de Investigação

A investigação jurídica pode ser descritiva, explicativa ou exploratória.

Este estudo tem como base a investigação descritiva das leis, estabelecendo os factos, analisando as decisões dos Tribunais em certos casos, sem que, no entanto, se ofereça uma explicação do motivo pelo qual os Tribunais decidiram daquela forma.

Ou seja, neste tipo de investigação estuda-se a lei tal como ela é, o que permite explicar e perceber a razão para uma determinada decisão.

Quanto ao processo de investigação jurídica, este é único.

Em primeiro lugar, começou-se pela investigação do tema que nos pareceu relevante, de seguida, procedeu-se a uma seleção de bases de dados bibliográficas, bem como legislativas.

Foram, ainda, analisados casos concretos, bem como os motivos que levaram o Tribunal a tomar determinada decisão.

No final, respondeu-se às perguntas de pesquisa, as quais, inicialmente, nos propusemos responder, tendo essas respostas produzido um resultado válido.

[1] Tradução livre da autora, *"This format is used to study legislative texts, jurisprudence and also legal doctrines, particularly or foreign laws."* (Adilah Abd Razak, 2009, p. 21)

Capítulo I – A luta contra a criminalidade na União Europeia e o intercâmbio de informações

1. O Espaço de Liberdade, Segurança e Justiça da União Europeia: breve enquadramento

> "A noção de cidadania da União implica uma comunidade de direitos e obrigações que unem os cidadãos da União por um vínculo comum que transcende a nacionalidade de um Estado Membro. A introdução deste conceito foi largamente inspirada pela preocupação de aproximar a União dos seus cidadãos e de exprimir a sua natureza como algo de diverso de uma União puramente económica. Esse intento encontra-se reflectido no abandono da expressão "económica" na denominação da Comunidade e pela progressiva introdução, no Tratado CE, de um amplo conjunto de actividades e de políticas que extravasam do âmbito económico".
>
> (Advogado-geral F. G. Jacobs, conclusões no proc. C-274/96, Bickel e Franz, pág. 7645)[2]

Em 1993, com o Tratado de Maastricht nascia a União Europeia e com ela foram surgindo novas designações como Direito da Integração Europeia; Direito da União Europeia; Direito das Comunidades Europeias; Direito da União e das Comunidades Europeias; Direito Constitucional da União Europeia e Direito Constitucional e Administrativo das Comunidades Europeias.[3]

A expressão *Direito da União Europeia* descreve e abarca todo o conjunto de regras e princípios conformadores do estatuto jurídico da União Europeia.

[2] F. G. Jacobs, conclusões no proc. C-274/96, Bickel e Franz, pág. 7645.
[3] V. Maria Luísa Duarte, *Estática e Dinâmica da Ordem Jurídica Eurocomunitária,* Almedina, 2011, p.18.

O filósofo e economista Stuart Mill defendia a sua ideia de que uma sociedade só podia intervir sobre a liberdade de ação dos seus membros para proteção de si mesma.

É por isso que o tema da cidadania tem constituído um desafio às concepções tradicionais nos espaços de integração, uma vez que, a construção de espaços de cidadanias múltiplas tem vindo a questionar conceitos e quadros sociais e normativos bem estabelecidos[4].

Ligada a esta ideia de cidadania e uma vez que a União Europeia é um espaço com uma grande diversidade cultural e populacional surgiu a preocupação, por razões óbvias, de garantir a eficácia direta e a prioridade aplicativa das respetivas normas nas ordens jurídicas dos Estados-membros.

É por isso mesmo que o Direito da União Europeia tem como principal característica a expansibilidade, uma vez que, ligada à ideia de espaço europeu, existe um vasto leque normativo eurocomunitário capaz de regular os mais variados aspectos da vida jurídica e social da comunidade europeia.

Desta forma, as normas de fonte comunitária evidenciaram-se em praticamente todos os espaços típicos de regulamentação interna.

Assim, feita esta primeira análise, é possível concluir que o Direito da União Europeia designa o conjunto de regras e princípios que regem a existência e o funcionamento da União Europeia.

Foi a 2 de outubro de 1997 através do Tratado de Amesterdão que o acordo de Schengen passou a integrar o quadro institucional e jurídico da União Europeia.[5]

O Tratado de Amesterdão introduziu importantes alterações ao Tratado da União Europeia, no que diz respeito ao reforço da segurança, criando um "espaço de liberdade, segurança e justiça".

Este Tratado instituiu mecanismos de decisão comunitária sobre matérias de cooperação intergovernamental, como por exemplo, vistos, asilos, imigração, bem como

[4] Quanto à questão da cidadania europeia, é importante reproduzir os ensinamentos do Professor Jorge Miranda, "Curso de Direito Internacional Público" 2006, pág. 210 e segs.:*"(...) a "cidadania europeia" é derivada da cidadania perante qualquer Estado-membro; não há um território da União (...)"*.

[5] Cfr. Fichas Técnicas sobre a União Europeia, II. O Tratado de Amesterdão: *"(...) Esta faculdade veio juntar-se aos casos de cooperação reforçada regida por disposições especificas, como a União Económica e Monetária, a criação do espaço de liberdade, segurança e justiça e a integração do acervo de "Schengen""*.

outras políticas relativas à livre circulação de pessoas, tendo, desta forma, alargado o âmbito de limitação da soberania dos Estados, no que diz respeito a estas matérias relacionadas com a livre circulação de pessoas.

Foi, no entanto, com a integração no Tratado do acervo dos acordos intergovernamentais, celebrados no quadro do Acordo de Schengen – 1985 – que se realizou plenamente a livre circulação de pessoas no âmbito de um espaço europeu de liberdade, segurança e justiça.

O acordo de Schengen é uma convenção entre os países europeus signatários que prevê a abertura das fronteiras, bem como, a livre circulação de pessoas.[6]

Assim, essa área em que a circulação de pessoas é livre designa-se por espaço Schengen.

O objetivo primordial da criação deste espaço foi a abolição de fronteiras, de modo a que as viagens realizadas entre os países signatários passassem a ser consideradas viagens domésticas.

As pessoas que residem fora da União Europeia, desde que obtenham um visto de longo prazo ou que ingressem como turistas, podem circular livremente por este espaço.

O espaço Schengen caracteriza-se pela abolição de controlo nas suas fronteiras internas, embora, por razões de ordem pública ou da própria segurança interna, esses controlos possam ser reativados temporariamente.

Mais tarde, a 1 de fevereiro de 2003, entrou em vigor o Tratado de Nice, que concretizou o objetivo de finalizar a reforma institucional assinalada no Tratado de Amesterdão, por se verificar fundamental ao funcionamento de uma "nova" União Europeia, uma vez que, o número de Estados associados como membros aumentou e, ainda, pela abrangência e natureza das matérias integradas na sua esfera de competências, principalmente no que toca à política monetária, à política externa e ao espaço de liberdade, segurança e justiça.[7]

Com o Tratado de Lisboa, assinado a 13 de dezembro de 2007, as regras jurídicas do espaço Schengen sofreram algumas alterações, de modo a reforçar a ideia de que "espaço de

[6] Cfr. Acordo Schengen, 1985
[7] Cfr. Tratado de Nice, 2005

liberdade, segurança e justiça" é mais do que cooperação policial e judiciária, visando a implementação de políticas comuns no que respeita à concessão de vistos, a asilo e imigração, através, já não do método intergovernamental, mas sim, através do método comunitário.[8]

O Tratado de Lisboa veio instituir o novo estatuto jurídico da União Europeia, comportando alterações substanciais sobre diversos pontos, tendo sido no domínio da Política Externa e de Segurança Comum, associada a uma Política Comum de Defesa em formação, e ainda no domínio da Cooperação Judiciária e Policial em Matéria Penal, que se deu o reforço mais significativo dos poderes de decisão da União Europeia.

Assim sendo, apraz fazer uma análise daquele Tratado, que é o responsável pela garantia da Justiça e da Segurança na União Europeia.

2. O Tribunal de Justiça da União Europeia

Com as relações económicas e jurídicas que se foram criando entre os Estados Membros, houve a necessidade de criação de um órgão dotado de características próprias de um verdadeiro tribunal, uma vez que essas relações tinham implicação direta na esfera jurídica e patrimonial dos particulares.[9]

Este Tribunal foi criado com o primeiro tratado comunitário, CECA, em 1950, tendo sido primeiramente designado por Tribunal de Justiça das Comunidades Europeias e entrando em funcionamento em 1952.

A partir da revisão do Tratado de Lisboa, este tribunal ficou reconhecido como o órgão jurisdicional da União, tal como é possível verificar pelo artigo 19º do Tratado da União Europeia, abrangendo o Tribunal de Justiça e o Tribunal Geral, além dos tribunais de competência especializada que vieram a ser criados.

Tal como é possível verificar pelo artigo 225º do Tratado da Comunidade Europeia, com a entrada em vigor do Ato Único Europeu, foi associada ao Tribunal de Justiça, uma

[8] Cfr. Tratado de Lisboa, 2007
[9] Neste sentido, Maria Luísa Duarte, *"Estática e Dinâmica da Ordem Jurídica Eurocomunitária"*, Almedina, 2011, p. 234

"jurisdição encarregada de conhecer, em 1ª instância (...) certas categorias de acções determinadas", denominada por Tribunal de 1ª Instância.[10]

Mais tarde foi rebatizado pelo Tratado de Lisboa como Tribunal Geral, nos termos dos artigos 19º, n.º1 do Tratado da União Europeia e artigo 256º do Tratado sobre o Funcionamento da União Europeia.

Com o Tratado de Nice, foram criadas câmaras jurisdicionais *"encarregadas de conhecer em primeira instância de certas categorias de recursos em matérias específicas"*, de acordo com o artigo 257º do Tratado sobre o Funcionamento da União Europeia.

Atualmente, o último tribunal especializado da União Europeia é o Tribunal da Função Pública, criado em 2004 por decisão do Conselho.

No artigo 13º, n.º1 do Tratado da União Europeia encontra-se consagrada a existência do Tribunal de Justiça da União Europeia, o Tribunal Geral, anteriormente designado por Tribunal de 1ª Instância e pelos tribunais especializados.

Nos termos do artigo 19º, n.º1 do Tratado da União Europeia, ao Tribunal de Justiça é-lhe atribuída a garantia do *"respeito do direito na interpretação e aplicação dos Tratados"*.

Tal como ensina Maria Luísa Duarte, *"o Tribunal de Justiça funciona como verdadeiro tribunal supremo, garante do princípio do duplo grau de jurisdição e da uniformidade da jurisprudência para evitar "lesão na unidade ou na coerência do direito da União""*, tal como consagra o artigo 256º, n.ºs 2 e 3 do Tratado sobre o Funcionamento da União Europeia[11].

Quanto à sua composição, o Tribunal de Justiça é composto por um Juiz por cada Estado Membro, nos termos do disposto no artigo 12º, n.º 2 do Tratado da União Europeia e do artigo 251º e seguintes do Tratado sobre o Funcionamento da União Europeia e por oito Advogados-Gerais, sendo que, tanto os Juízes como os Advogados-Gerais, são designados pelos governos dos Estados-Membros por períodos de seis anos, renovando-se a composição do Tribunal a cada três anos, de modo a permitir a continuidade da jurisprudência.[12]

[10] V. ex-artigo 225.º-A TCE
[11] Cfr. Maria Luísa Duarte,*"Estática e Dinâmica da Ordem Jurídica Eurocomunitária"*, Almedina, 2011, p. 235
[12] V. a este respeito, Miguel Gorjão-Henriques, *"Direito Comunitário",* 5ªEdição, Almedina, 2008

O artigo 19º, n.º 3 do Tratado da União Europeia define as competências do Tribunal de Justiça da União Europeia por referência a três áreas de jurisdição, sendo elas:

a) Recursos interpostos por um Estado-Membro, por uma instituição ou por pessoas singulares ou colectivas;
b) Quanto à interpretação do Direito da União ou sobre a validade dos atos adoptados pelas instituições;
c) E nos de mais casos previstos pelos Tratados.

O Tribunal de Justiça viu serem excluídas das suas competências, as respeitantes aos domínios relativos à Política Externa e de Segurança Comum, e à Cooperação Policial e Judiciária em Matéria Penal, que constituem os pilares da União Europeia, consignados no Tratado de Maastricht.

Posteriormente, *"o Tratado de Amesterdão manteve em relação ao II Pilar a imunidade ao controlo jurisdicional, mas no que respeita às matérias do III Pilar operou uma alteração fundamental no sentido da sua (relativa) jurisdicionalização."*[13]

No entanto, isto só foi possível devido à comunitarização de um conjunto de matérias que anteriormente haviam sido abrangidas pela cooperação intergovernamental, como é o caso dos vistos, asilo, imigração e, ainda, outras políticas relativas à livre circulação de pessoas – artigo 68º do Tratado da Comunidade Europeia; e ainda, porque se reconheceu como competência exclusiva do Tribunal de Justiça os poderes de interpretação e de controlo no âmbito das restantes matérias do III Pilar – artigo 35º do Tratado da União Europeia.

Assim, é possível afirmar que o Tratado de Lisboa alargou o âmbito do controlo jurisdicional a domínios em que não estava previsto em relação às matérias do III Pilar.

Senão, vejamos o artigo 275º do Tratado sobre o Funcionamento da União Europeia, que atribui ao Tribunal de Justiça da União Europeia a competência para controlar a observância do artigo 40º do Tratado da União Europeia, a fim de se poder pronunciar sobre os recursos de anulação que os particulares possam instaurar com fundamento na violação de direitos resultante de medidas restritivas, como por exemplo, o Regulamento do Conselho sobre o congelamento de bens pertencentes a pessoas e entidades suspeitas de terrorismo.

[13] Cfr. Maria Luísa Duarte, *"Estática e Dinâmica da Ordem Jurídica Eurocomunitária"*, Almedina, 2011, p. 247

Relativamente à cooperação judiciária e policial em matéria penal, o Tribunal de Justiça da União Europeia não tem competência quanto às operações policiais nos Estados Membros, nem pode intervir no exercício, pelas autoridades nacionais, das respetivas atribuições em matéria de ordem pública e segurança interna.[14]

2.1. O Tribunal Geral

Com o passar do tempo, foi-se reconhecendo a necessidade de criar um Tribunal que, de alguma maneira, pudesse auxiliar o Tribunal de Justiça, que por volta dos anos 80 *"(...) conheceu um extraordinário incremento do número de processos: de 79 em 1970, passou-se para 279 em 1980 e em 1985 esse número atingiu 433 processos. Este crescente afluxo processual repercutiu-se sobre a duração média dos processos: em 1970, um processo de questões prejudiciais era decidido em seis meses, mas em 1989 já demorava dezoito meses; em 1970, um recurso directo esperava nove meses pelo veredicto final e em 1989 esse período alongou-se para vinte e três meses."*[15]

Facilmente se percebe que tal afluxo processual repercutiu-se sobre a duração média dos processos.

Assim, a solução que pareceu mais apropriada, para evitar um bloqueio da justiça administrada pelo Tribunal de Justiça, seria a criação de um novo tribunal.

Desta forma, foi criado um novo tribunal através da Decisão 88/591/CE, CECA, EURATON, do Conselho, de 24 de outubro de 1988, tendo sido designado, primeiramente, por Tribunal de 1ª Instância.[16]

Este tribunal foi oficialmente instalado a 11 de outubro de 1989, tendo proferido o seu primeiro acórdão em fevereiro de 1990.

O Tratado de Lisboa fez deste tribunal a instância intermédia da estrutura jurisdicional, com competência para julgar a maior parte dos litígios, não só em 1ª instância, como os recursos das decisões proferidas pelos tribunais especializados.

Foi por esta razão que se achou mais apropriado alterar a sua designação para Tribunal Geral, nos termos do artigo 19º, n.º1 do Tratado da União Europeia.

---

[14] Cfr. artigo 276.º Tratado sobre o Funcionamento da União Europeia

[15] Cfr. Maria Luísa Duarte, *"Estática e Dinâmica da Ordem Jurídica Eurocomunitária"*, Almedina, 2011, p. 249

[16] Cfr. artigo 17.º, n.º 2 da Decisão 88/591/CE, *"O n.º1 do artigo 2.º da Decisão 88/591/CECA//CEE/ Euratom do Conselho passa a ter a seguinte redacção: "O Tribunal de primeira Instância é composto por quinze juízes."*

Quanto às suas competências, rege o artigo 256º do Tratado sobre o Funcionamento da União Europeia, atribuindo a este tribunal a competência para conhecer em 1ª instância dos seguintes recursos:

a) "Recursos de anulação – artigo 263º do Tratado sobre o Funcionamento da União Europeia;
b) Recursos por omissão – artigo 265º do Tratado sobre o Funcionamento da União Europeia;
c) Ações de indemnização – artigo 268º do Tratado sobre o Funcionamento da União Europeia;
   e
d) dos Recursos e ações no âmbito da cláusula compromissória – artigo 272º do Tratado sobre o Funcionamento da União Europeia."[17]

O artigo 256º, n.º 3 do Tratado sobre o Funcionamento da União Europeia remete para o Estatuto relativamente às matérias específicas de que o Tribunal Geral pode conhecer, através de solicitação feita pelos tribunais nacionais.

Tal como refere Maria Luísa Duarte, *"as decisões proferidas pelo Tribunal Geral podem ser objecto de recurso para o Tribunal de Justiça, que incide unicamente sobre as questões de direito (v. artigo 256º, n.º 1, parágrafo segundo, TFUE). Sob a preocupação de harmonizar o princípio do duplo grau de jurisdição com a garantia da uniformidade da jurisprudência, o artigo 256.º TFUE estabelece critérios especiais de intervenção do Tribunal de Justiça sobre decisões proferidas ou a proferir pelo Tribunal Geral:*

- *Se existir risco grave de lesão da unidade ou coerência do direito da União, o Tribunal de Justiça pode, a título excepcional, reapreciar as decisões tomadas pelo Tribunal Geral sobre os recursos instaurados das decisões dos tribunais especializados (triplo grau de jurisdição);*
- *Se estiver em causa uma decisão de princípio susceptível de afectar a unidade ou a coerência do direito da União, o Tribunal Geral pode remeter para o Tribunal de Justiça os pedidos de questões prejudiciais que, no futuro, venham a integrar o âmbito da sua competência;*

[17] Cfr. Maria Luísa Duarte, *"Estática e Dinâmica da Ordem Jurídica Eurocomunitária"*, Almedina, 2011, p. 251

- *Se existir risco grave de lesão da unidade ou da coerência do direito da União, as decisões proferidas pelo Tribunal Geral sobre questões prejudiciais poderão ser reapreciadas, a título excepcional, pelo Tribunal de Justiça."*[18]

2.2. O Tribunal da Função Pública

A par do aumento do contencioso, em virtude da aplicação das normas comunitárias, estava o fenómeno da litigiosidade em domínios específicos, motivo esse que levou à criação de um tribunal dotado de competência especializada, uma vez que já existia o Tribunal de Justiça e o Tribunal Geral, ambos de competência genérica, tal como prevê o artigo 19º, n.º1 do Tratado sobre o Funcionamento da União Europeia.

É da competência deste tribunal, decidir dos litígios entre a União e os seus agentes, tal como prevê o artigo 270º do Tratado sobre o Funcionamento da União Europeia.

Das suas decisões cabe recurso para o tribunal Geral, de acordo com o artigo 257º, parágrafo 3º e a título excepcional, para o Tribunal de Justiça, nos termos do artigo 256º, n.º2, todos do mesmo diploma.

3. A cooperação policial na União Europeia. Objectivos

Como anteriormente se referiu, a União Europeia é um espaço de liberdade, segurança e justiça mas, para que tal funcione na plenitude, e tendo como linha condutora e principal objetivo o respeito pelos direitos fundamentais, é necessária uma cooperação policial eficaz.

Foi em 1976, com o chamado "Grupo de Trevi" que a cooperação policial teve origem, sendo este grupo uma espécie de rede intergovernamental de representantes do Ministério da Justiça e do Ministério do Interior.[19]

Já em 1985, com a criação do Espaço Schengen, a cooperação policial transfronteiriça tornou-se, finalmente, uma realidade, uma vez que com a entrada em vigor do Tratado de Amesterdão, o "acervo de Schengen" passou a fazer parte integrante do Direito da União Europeia, ao abrigo do "terceiro pilar" da cooperação intergovernamental.

---

[18] Cfr. Maria Luísa Duarte, *"Estática e Dinâmica da Ordem Jurídica Eurocomunitária"*, Almedina, 2011, p. 251
[19] V. a este respeito, Fichas Técnicas sobre a União Europeia, www.europarl.europa.eu

A mesma abordagem intergovernamental imperou para as medidas de cooperação policial adoptadas por um pequeno grupo de Estados Membros ao abrigo do Tratado de Prüm, que continha disposições relativas ao intercâmbio de ADN, impressões digitais e informações sobre o registo de veículos.

No entanto, apenas com o Tratado de Maastricht de 1992 foi inserida, pela primeira vez, a cooperação entre os serviços policiais e as autoridades aduaneiras dos Estados Membros, definindo e especificando as questões de interesse comum que justificavam seriamente a cooperação policial, tendo ficado estabelecido que essas questões se prendiam com o terrorismo, drogas e outras formas de criminalidade internacional.[20]

O Tratado de Maastricht estabeleceu, ainda, o princípio da criação de um "serviço europeu de polícia", a ora conhecida Europol.

O objetivo primordial da criação de uma cooperação policial transfronteiriça, foi a prevenção, a detecção e a investigação de crimes em todo o espaço europeu. Ou seja, no fundo, o objetivo foi a realização dos interesses comuns da União, uma vez que, se todos os Estados-Membros cooperassem entre si, esta seria a forma mais eficaz para a concretização desses objetivos.

No entanto, apenas a 1 de maio de 1999, com a entrada em vigor do Tratado da União Europeia, é que se alargaram as possibilidades de cooperação no âmbito da Justiça e dos Assuntos Internos.

Foi com este Tratado que se especificaram os objetivos e as ações a desenvolver no domínio da cooperação policial e aduaneira.

Para além disso, foi com o Tratado da União Europeia que se reforçou o quadro institucional e que se desenvolveu o processo de decisão neste domínio.

O Tratado de Lisboa – Tratado sobre o Funcionamento da União Europeia – prevê no seu artigo 67º, que a União Europeia pretende garantir um nível de segurança, através da prevenção e combate à criminalidade organizada, ou não, através da cooperação entre as forças policiais, autoridades aduaneiras e outras autoridades competentes dos Estados Membros.

[20] V. a este respeito, *"A cooperação Policial e Segurança"*, www.sg.mai.gov.pt

Assim, o Tratado de Lisboa veio facilitar a ação a nível europeu através do "método comunitário", que consistia na tomada de decisão por maioria qualificada com base em propostas da Comissão, estando estas sujeitas ao controlo judicial do Tribunal de Justiça e passando a ação do Parlamento Europeu a ter um destaque maior.

O "método comunitário", introduzido pelo Tratado de Lisboa, consiste num reforço do controlo democrático dos parlamentos nacionais, sob a fiscalização do Tribunal de Justiça.

Esta cooperação policial transfronteiriça, consiste na possibilidade das autoridades policiais dos Estados Membros poderem intervir no território de outro Estado-Membro, em conjunto e em articulação com as autoridades desse mesmo Estado.[21]

A cooperação policial transfronteiriça envolve tanto as alfândegas como a própria policia e as restantes autoridades competentes para a execução das leis, visando essencialmente, os crimes graves como o terrorismo, a criminalidade organizada, o tráfico de drogas, o tráfico de seres humanos e, ainda, a cibercriminalidade.[22]

Em matéria de cooperação policial, não se pode deixar de referir, a previsão de um novo Comité, designado por Comité Permanente para a Cooperação Operacional em matéria de Segurança Interna.

A sua principal preocupação, prende-se com a eficácia no combate às ameaças pan-europeias, com a criminalidade e, principalmente, que esse combate seja feito com respeito e em conformidade com os direitos fundamentais e de acordo com as regras de proteção de dados.

---

[21] Segundo o Professor Manuel Monteiro Guedes Valente, *"A cooperação policial internacional, assim como europeia, depende do objecto, dos sujeitos, das relações estabelecidas, do método e da sua natureza. A cooperação depende, também, do grau e do carácter da reciprocidade em que é desenvolvida.*
Defendemos que só se deve considerar como cooperação quando a actuação policial de cooperação reveste um carácter recíproco ou mútuo, caso contrário, estaremos em uma situação de ajuda na resolução de um caso específico e pontual.
Considera-se que, independentemente dos discursos e patamares de cooperação, esta só existe quando está subordinada ao princípio da reciprocidade em igualdade de acção que pode abranger a reciprocidade na edificação mútua de um espaço comum ou restrito de liberdade, de justiça e de segurança.
Outra posição leva-nos a considerar que estamos no patamar da coadjuvação ou da colaboração, que revestem natureza de cooperação (policial) específica." (Manuel Monteiro Guedes Valente, 2014, p. 622)

[22] De acordo com um comunicado de imprensa do Parlamento Europeu *"Os Estados-Membros devem impedir a circulação de suspeitos terroristas através do reforço dos controlos nas fronteiras externas, de uma verificação mais sistemática e eficaz dos documentos de viagem e do combate ao tráfico de armas e à utilização fraudulenta de documentos de identidade, bem como da identificação de zonas de risco".* Assim, entendemos que deve haver um reforço nas fronteiras externas.

Certo é que, o caminho ainda é longo e que, apesar dos grandes progressos que a União Europeia tem feito, a cooperação policial e as suas políticas encontram-se ainda em desenvolvimento.

3.1. Schengen e a Cooperação Policial

"O Tratado de Amesterdão de 1997 integrou a Convenção de Aplicação do Acordo de Schengen (CAAS), de 1990, no âmbito da União Europeia."[23]

O principal objectivo de Schengen consiste na livre circulação de pessoas, eliminando-se qualquer controlo nas fronteiras comuns, sendo que a cooperação policial tem sido considerada uma das medidas complementares de proteção de segurança interna.

Assim sendo, são exigidas aos Estados Membros determinadas obrigações no que diz respeito à matéria de cooperação policial nas suas fronteiras internas comuns, e nas fronteiras externas tais como fronteiras terrestres, aeroportos internacionais, fronteiras marítimas e no interior do espaço Schengen em geral, de modo a equilibrar possíveis deficiências de segurança derivadas da eliminação dos controlos nas fronteiras internas.

É por isso que Schengen tem uma dupla importância, por um lado proporciona a livre circulação e, por outro lado, prevê um mínimo de medidas necessárias de modo a compensar os défices de segurança, de modo a garantir que o sistema judiciário consiga responder de forma eficaz à mobilidade acrescida.

Para a supressão dos controlos nas fronteiras internas é necessário haver um quadro legislativo eficiente, e por isso, torna-se, igualmente preciso, introduzir controlo nas fronteiras externas com base em normas comuns, bem como, as respetivas regras de aplicação obrigatórias com o objetivo de intensificar a cooperação dos serviços responsáveis pela aplicação da lei.

[23] V. a este respeito, *"Vertente policial na cooperação Schengen"*, www.dgai.mai.gov.pt

3.2. EUROPOL

No âmbito da cooperação policial, criou-se um Serviço Europeu de Polícia (Europol) com o Tratado da União Europeia – Maastricht – no seu artigo K.1, n.º 9 UE, sendo que a Convenção assinada pelos Estados Membros e que deu origem à Europol, só entrou em vigor a 1 de Outubro de 1998.[24]

De acordo com os ensinamentos de Manuel Monteiro Guedes Valente, esta cooperação compreendia dois domínios: *"operacional, desde a investigação, da recolha, armazenamento, tratamento, análise e intercâmbio de informações, até a operações materiais de intervenção e instalação de agentes de ligação - e formação - cursos de aperfeiçoamento e de especialização"* em áreas de grande importância para o bom desempenho da sua atividade, como é o caso da investigação criminal.[25]

A Europol é competente para a coordenação e execução de investigações e de operações entre as várias polícias europeias, de modo a poder reprimir e prevenir a criminalidade organizada, sendo ainda responsável pela criação de uma rede de investigação, de documentação e, ainda, de estatística sobre a criminalidade transfronteiriça.

A Europol possui uma relação estreita com a União, cuja regulação da sua atuação está inserida no título relativo à cooperação policial e judiciária em matéria penal, particularmente nos artigos 29º, § 2 e 30º UE.

A Europol dispõe de mais de 900 funcionários, provenientes de vários tipos de órgãos policiais e têm como função garantir a eficácia das autoridades nacionais de polícia e de outas autoridades, ajudando a colmatar as lacunas em matéria de informação e a minimizar o espaço de atuação dos criminosos. Tem ainda a função de melhorar o intercâmbio de informações entre as autoridades de polícia, cooperando na prevenção e na luta contra o terrorismo, a cibercriminalidade, o tráfico de droga, bem como outros crimes transfronteiriços de elevada gravidade.

Para isso, a EUROPOL elabora uma Avaliação da Ameaça da Criminalidade Grave e Organizada, identifica e avalia as ameaças emergentes, descrevendo a estrutura dos grupos de criminalidade organizada e a sua forma de atuação, bem como os principais tipos de crime que afetam a União Europeia, servindo de base às decisões do Conselho.[26]

---

[24] Cfr. Miguel Gorjão-Henriques, "*Direito Comunitário"* 2008, p. 227
[25] Cfr. Manuel Monteiro Guedes Valente, *"Teoria Geral do Direito Policial"*, 2014, p. 616
[26] V. a este respeito, *"O Serviço Europeu de Polícia - Europol"*, www.dgai.mai.gov.pt

Elabora ainda, um relatório sobre a Situação e Tendência do Terrorismo na Europa que fornece uma análise exaustiva e previsível em matéria de criminalidade e terrorismo na União Europeia.

Muito embora, a EUROPOL possua todas estas competências, são-lhe vedados poderes de ação coerciva, querendo isto dizer que a EUROPOL não pode proceder a detenções ou a buscas.

Com o passar do tempo as competências operacionais da EUROPOL foram aumentando gradualmente e, exemplo disso, é o Ato do Conselho de 28 de novembro de 2002, que passou a autorizar a participação da EUROPOL em equipas de investigação conjuntas, permitindo-lhe ainda, que esta solicite aos Estados Membros que iniciem investigações em matéria penal.

A EUROPOL viu as suas capacidades analíticas reforçadas quando em janeiro de 2013 foi instituído o Centro Europeu da Cibercriminalidade (EC3), responsável pela avaliação da ameaça da criminalidade organizada dinamizada pela internet (iOCTA).

A EUROPOL tem tido um papel bastante eficaz no que respeita às novas ameaças terroristas, uma vez que, o Conselho de Justiça e dos Assuntos Internos, na sequência dos ataques terroristas de Paris e Copenhaga de 2015, mandatou a EUROPOL criar uma Unidade de Sinalização de Conteúdos na Internet de modo a combater a propaganda terrorista e outras atividades extremistas.

Desta forma, a 1 de julho de 2015, a Unidade de Sinalização de Conteúdos na Internet iniciou as suas funções.

A 1 de janeiro de 2016, o Conselho alargou o mandato da EUROPOL no que respeita à luta contra o terrorismo, na sequência dos atentados de Paris de novembro de 2015, criando o Centro Europeu de Luta contra o Terrorismo, no qual participam peritos dos Estados-Membros com o objetivo de reforçar a capacidade de investigação transfronteiriça.

Acresce ainda, que com a enorme afluência de migrantes irregulares que têm chegado à Europa, a EUROPOL iniciou a Operação Conjunta MARE em março de 2015, de forma a combater o tráfico de seres humanos.

Cabe ainda referir que, por decisão do Conselho Europeu da Cibercriminalidade, de 27 de março de 2000, a EUROPOL está habilitada para negociar acordos com instâncias e Estados terceiros, como foi com o caso dos Estados Unidos, em que a EUROPOL celebrou acordos de cooperação com a Interpol e os Estados Unidos.

De acordo com a Ficha Técnica sobre a União Europeia, *"em 27 de março de 2013, a Comissão apresentou ao Parlamento Europeu e ao Conselho uma proposta legislativa para*

alterar a atual decisão relativa ao Europol, que incluía uma proposta relativa à fusão entre o Europol e a Academia Europeia de Polícia (CEPOL). Tendo sido rejeitada pelo Conselho e pelo Parlamento, a hipótese de uma fusão foi posta de parte. O Parlamento chegou recentemente a acordo com o Conselho sobre o novo regulamento nas negociações no âmbito do trilogo – sob reserva de aprovação na sessão plenária. O novo regulamento tomará mais fácil para o Europol criar unidades especializadas para dar resposta às ameaças emergentes, estabelecerá regras para as unidades existentes (tais como as unidades de luta contra o terrorismo antes descritas) e proporcionará um regime de proteção de dados mais sólido, uma melhor governação e uma maior responsabilização da agência, o que deverá ser alcançado através de um grupo de controlo parlamentar conjunto que reúna o Parlamento Europeu e os parlamentos nacionais."[27]

3.3. CEPOL

A CEPOL foi criada pela Decisão 2000/820/JAI do Conselho, com o objetivo de contribuir para a formação dos agentes e, assim, auxiliar a cooperação policial. Para isso ela foi constituída, inicialmente, em rede, agrupando os institutos nacionais de formação de altos funcionários dos serviços de polícia dos Estados-membros, que para o efeito deverão manter uma estreita cooperação e, subsequentemente, sob a forma de uma agência da União Europeia, através da Decisão 2005/681/JAI do Conselho, de 20 de Setembro de 2005.[28]

A CEPOL executa os programas e as iniciativas decididas pelo Conselho de Administração, constituído pelos diretores dos institutos nacionais de formação de altos funcionários dos serviços de polícia.

Os objetivos prosseguidos pela CEPOL prendem-se com o *"aprofundar o conhecimento mútuo dos sistemas e estruturas nacionais de polícia dos outros Estados-Membros, da EUROPOL e da cooperação policial transfronteiras na União Europeia;*

[27] V. a este respeito, *"O Serviço Europeu de Polícia - Europol"*, www.europarl.europa.eu
[28] V. a estes respeito, *"A Academia Europeia de Polícia – Cepol"*, Fichas Técnicas sobre a União Europeia, www.europarl.europa.eu

melhorar o conhecimento dos instrumentos internacionais, nomeadamente dos que já existem a nível da União Europeia em matéria de cooperação na luta contra a criminalidade(...).”[29]

É, ainda, objetivo da CEPOL *“(...) assegurar uma formação adequada quanto ao respeito das garantias democráticas, designadamente dos direitos de defesa, e favorecer a cooperação entre a AEP e os demais institutos de formação policial.”*[30]

De modo a prosseguir os seus objectivos e a ter sucesso com a concretização dos mesmos, a CEPOL participa na elaboração dos programas harmonizados de formação de agentes de patente intermédia, de agentes operacionais, contribuindo para a elaboração dos programas adequados de formação avançada, desenvolvendo e assegurando a formação dos próprios formadores.

A CEPOL é responsável pela formação especializada dos agentes de polícia com postos-chave na luta contra a criminalidade transfronteiriça, dando especial importância à criminalidade organizada.

Cabe-lhe, ainda, a divulgação das práticas mais eficazes e os resultados da investigação; desenvolver e assegurar uma formação destinada a preparar as forças policiais dos Estados-Membros da União Europeia para a sua participação na gestão não militar de crises; tem como função facilitar o intercâmbio e destacamentos pertinentes de agentes de polícia no quadro da formação; tem, ainda, a seu cargo a criação de uma rede eletrónica destinada a prestar apoio à CEPOL no desempenho das suas funções, garantindo que sejam tomadas as medidas de segurança necessárias.

Por último, é da sua responsabilidade garantir que os agentes de polícia de alto nível dos Estados-Membros adquiram conhecimentos linguísticos adequados.

[29] Cfr. *“Cooperação Policial”*, p.4, www.dgai.mai.gov.pt
[30] Cfr. *“Cooperação Policial”*, p.4, www.dgai.mai.gov.pt

3.4. COSI

O Comité Permanente para a Cooperação Operacional em matéria de Segurança Interna – COSI – tem como objetivo assegurar a promoção e o reforço da cooperação operacional em matéria de segurança interna na União.

Até porque, de acordo com as Fichas Técnicas da União Europeia, *"a cooperação operacional constitui, desde o início, a pedra angular do desenvolvimento da cooperação policial."*

A criação de um Comité Permanente vem regulada no artigo 71º do Tratado sobre o Funcionamento da União Europeia e, de acordo, com este artigo o Comité deve promover a coordenação da ação das autoridades competentes dos Estados-Membros, sendo que os representantes, quer dos órgãos, como dos organismos da União, podem ser associados aos trabalhos do próprio Comité.

Este Comité foi criado pela Decisão do Conselho 2010/131 de 25 de fevereiro de 2010, estabelecendo os objetivos e fixando as regras do seu funcionamento.

O COSI tem como funções, facilitar e garantir uma cooperação operacional e coordenar eficazmente a cooperação policial e aduaneira entre as autoridades responsáveis pelo controlo e proteção das fronteiras externas e cooperação judiciária no âmbito penal, nos casos relevantes e fundamentais para a cooperação operacional no domínio da segurança interna e, ainda, na cooperação no combate ao terrorismo.

É da sua competência avaliar e dirigir eficazmente a cooperação operacional, recomendando medidas ao Conselho, no quadro da "cláusula de solidariedade", tal como prevê o artigo 222º do Tratado sobre o Funcionamento da União Europeia.

Por último, é ainda da sua competência o desenvolvimento, a monitorização e a implementação da Estratégia Europeia de Segurança Interna.

No entanto, é de ter em conta que o COSI não tem competência para conduzir as operações, pois esta é uma tarefa que cabe aos Estados-Membros e nem é da sua competência participar na preparação dos atos legislativos, uma vez que não se trata de um "FBI" europeu com autonomia para conduzir operações.[31]

[31] A este propósito, *"(...) o COSI não é um "FBI" europeu com autonomia para conduzir operações, nem intervém no processo legislativo. As suas atividades estão sediadas nas diferentes capitais mas os representantes dos Estados-Membros reúnem-se em Bruxelas, onde são apoiados pelos conselheiros da Justiça e dos Assuntos Internos das representações permanentes. Os representantes de outros organismos envolvidos na segurança interna – tais como o EUROPOL, a EUROJUST – participam com frequência nas reuniões do COSI."*

Os representantes dos outros organismos pertencentes à segurança interna, como a Europol e a Eurojust, participam nas reuniões do COSI.

3.5. INTCEN

O INTCEN – abreviatura para Centro de Análise de Informações da União Europeia não é um órgão de cooperação policial, uma vez que pertence ao Serviço Europeu para a Ação Externa – SEAE.

O que importa referir é que o INTCEN avalia as ameaças, com base nas fontes que lhe são fornecidas pelos serviços de informação, pelas entidades militares, pelos diplomatas e pelos serviços de polícia.

Ou seja, o INTCEN acaba por dar o seu contributo, numa perspectiva operacional, uma vez que é útil a informação prestada a nível da União Europeia sobre os destinos, as razões e os principais circuitos de deslocação dos terroristas.

4. A cooperação Judicial em matéria Penal na União Europeia

Com a supressão dos controlos nas fronteiras da União Europeia, a circulação dos cidadãos europeus tornou-se mais simples. No entanto, foi inevitável o aparecimento de aspectos negativos, como é o caso da criminalidade internacional que viu a sua atividade facilitada através da eliminação dos controlos nas fronteiras, usufruindo, assim, das potencialidade de um mercado global ou transnacional.

É o que acontece, desde logo, com as organizações criminosas, bastando reparar na sua constituição para perceber que são verdadeiras detentoras de instrumentos de controlo dos mercados de droga, de armas, de corrupção, de branqueamento de capitais, do trafico de pessoas e, até mesmo, de órgãos.

Para além disso, são características destas organizações, a versatilidade, a invisibilidade e a capacidade de influência e domínio de pontos mais sensíveis dos vários sistemas, como o económico, o político e financeiro mundial e, são ainda suas características, a mobilidade e a capacidade de regeneração.

Pela crescente instalação destas fenomenologias criminosas à escala global, é que a União Europeia se viu obrigada a enfrentar o desafio do combate à criminalidade internacional, uma vez que, existindo um espaço único de justiça penal, é necessário que na base esteja o princípio do reconhecimento mútuo, constituindo a base de uma verdadeira cidadania, o combate à criminalidade e a garantia da proteção do direito das vítimas, dos suspeitos e dos reclusos na União, mesmo que atravessem fronteiras nacionais.

Com o Tratado de Lisboa, o espaço de Liberdade, Segurança e Justiça conheceu uma legitimidade maior, ou seja, com este Tratado o espaço de Liberdade, Segurança e Justiça viu o seu papel reforçado.

A Convenção relativa ao Auxílio Judiciário Mútuo em Matéria Penal foi aprovada pelo Conselho de Ministros da União Europeia a 29 de maio de 2009.

Esta Convenção pretende incentivar a cooperação entre autoridades judiciárias, policiais e aduaneiras da União, servindo de complemento às disposições contidas em instrumentos jurídicos existentes e, ao mesmo tempo, tendo em conta a Convenção Europeia para a Proteção dos Direitos do Homem de 1950.

Simultaneamente, foram aprovados, através de organizações internacionais, acordos como a Convenção do Conselho da Europa sobre o Auxílio Mútuo em Matéria Penal de 1959.

Como inicialmente se referiu, para que a cooperação judicial em matéria penal resulte eficaz, é necessário o reconhecimento mútuo de decisões judiciais em matéria penal, tal como declarou o Conselho Europeu de Tampere e posteriormente confirmado nos programas de Haia e de Estocolmo.

Este reconhecimento mútuo de decisões judiciais em matéria penal é essencial, uma vez que só através deste reconhecimento é que é possível ultrapassar as dificuldades que possam surgir pelas diferenças que existem entre os sistemas judiciais nacionais.

O cumprimento deste princípio só é possível se houver um elevado nível de confiança entre os Estados-Membros.

Um dos pontos mais importantes relativos a esta matéria prende-se com o Mandado de Detenção Europeu.

Foi com a Decisão-Quadro do Conselho, de 13 de junho de 2002, que o sistema de extradição tradicional sofreu alterações através da adoção de regras inovadoras, como é o caso da delimitação dos fundamentos para a recusa da execução, ou a transferência da decisão das autoridades políticas para as autoridades judiciárias, ou a possibilidade de entrega de nacionais do Estado de execução e os prazos claros para a execução de cada Mandado de Detenção Europeu.

A Europol, a Eurojust e a Rede Judiciária Europeia podem dar um importante contributo no domínio do auxílio judiciário mútuo e dos pedidos de Mandado de Detenção Europeu.

Como facilmente se percebe, o principal problema que tudo isto acarreta, prende-se com as diferenças entres as legislações penais nacionais.

Por isso mesmo, existe uma aproximação do direito penal na União Europeia, ou seja, existe um ajustamento a uma norma mínima comum e não uma unificação total.

Para certo tipo de crimes foram adotados determinados textos jurídicos e outros encontram-se a ser negociados, com vista à harmonização das sanções e de definições comuns.

Importa, ainda, referir que a Eurojust é um organismo da União Europeia criado em 2002, por uma decisão do Conselho, tendo essa mesma decisão sido alterada posteriormente em dezembro de 2008.

Cabe, por isso, à Eurojust, incentivar e melhorar as investigações e as acções penais entre as autoridades competentes dos Estados-Membros, prestando auxílio judiciário mútuo transfronteiriço e executando pedidos de extradição e de mandados de detenção europeus.

O Tratado de Lisboa permite que o Conselho possa instituir uma Procuradoria Europeia a partir da Eurojust, de modo a combater as infracções lesivas dos interesses financeiros da União, permitindo igualmente a possibilidade de aumentar os poderes da Procuradoria Europeia, numa fase posterior, de modo a que se possa abarcar a criminalidade com dimensão transfronteiriça.

Em 1998 foi criada a Rede Judiciária Europeia em matéria penal, com o objetivo de melhorar a cooperação judicial entre os Estados-Membros.

Esta Rede tem como função ajudar os juízes e procuradores nacionais a procederem a investigações e ações penais transfronteiriças.

Como forma de combater o tráfico de droga, o tráfico de seres humanos e, ainda, o próprio terrorismo, o Conselho Europeu de Tampere propôs a criação de equipas de investigação conjuntas.

No entanto, também a Convenção de Auxílio Judiciário em Matéria Penal de maio de 2000, prevê a criação destas equipas de investigação conjuntas.

Quanto aos direitos processuais, é reconhecido aos arguidos e acusados como, direito fundamental, o direito a um julgamento justo.

Foi em novembro de 2009 que o Conselho adotou um roteiro que reforçava os direitos processuais dos suspeitos ou acusados em processos penais, sendo que eram seis as áreas que o roteiro identificava como sendo as que mais iniciativas legislativas necessitavam.

Essas seis áreas prendem-se com os direitos dos arguidos e são elas:

a) A tradução e a interpretação;
b) A informação sobre os direitos e sobre a acusação;
c) Direito a apoio e a aconselhamento jurídico;
d) Possibilidade de comunicação com a família, empregadores e autoridades consulares;
e) Concessão de garantias especiais a suspeitos ou acusados vulneráveis; bem como,
f) Possibilidade de elaborar um Livro Verde sobre a prisão preventiva.

Quanto ao direito à interpretação e à tradução, no âmbito do processo penal, o Parlamento e o Conselho adoptaram a Directiva 2010/64/EU e em maio de 2012 adotaram a Directiva 2012/13/EU, a que chamaram "Declaração de Direitos", relativa ao direito à informação em processo penal.

Mais tarde, em outubro de 2013, foi adotada a Directiva 2013/48/EU, que garante o direito de acesso a um advogado em processo penal, bem como o direito de comunicação após a detenção.

Cada vez mais se tem seguido rumo a uma política da União Europeia em matéria penal e tanto assim é que, em setembro de 2011 foi publicada, pela Comissão Europeia, uma comunicação intitulada *"Rumo a uma política da União Europeia em matéria Penal: assegurar o recurso ao direito penal para uma aplicação efectiva das políticas da União Europeia"*, cujo objetivo é esclarecer a forma como o cidadão pode ser protegido contra a criminalidade, através da aplicação de normas mínimas de direito penal em toda a União Europeia.

Para além disso, procura definir certos princípios que contribuirão para garantir a homogeneidade e coerência da legislação da União Europeia em matéria de Direito Penal.

Com o Tratado de Lisboa, a justiça penal na União Europeia tornou-se mais eficaz e com uma maior responsabilidade, o que levou o Parlamento a adotar resoluções sobre diversas questões relativas à cooperação judicial em matéria penal, como é o caso da "*prevenção e resolução de conflitos de competência em acções penais, as medidas de controlo como alternativa à prisão preventiva, as medidas de controlo após o processo, a transferência de processos, o mandado de detenção europeu e o mandado europeu de obtenção de provas, a Eurojust, a Rede Judiciária Europeia, as decisões tomadas na ausência do acusado, os crimes ambientais, o terrorismo, o crime organizado, a justiça electrónica, o tráfico de seres humanos, a exploração sexual de crianças e a pornografia infantil, a decisão europeia de protecção, as normas mínimas sobre os direitos e o apoio e a protecção das vítimas da criminalidade".*[32]

Mais recentemente foram aprovados pelo Parlamento resoluções que aprovam as propostas de diretivas relativas ao congelamento e ao confisco de produtos do crime, sobre o abuso de informação privilegiada e a manipulação de mercado, e sobre a proteção do euro contra a falsificação.

Por último, cabe ainda referir que o Parlamento Europeu deve intervir na avaliação e supervisão do espaço de Liberdade, Segurança e Justiça, nomeadamente no que ao domínio da justiça penal diz respeito.

Assim, é possível verificar que o *"Parlamento Europeu e os Parlamentos nacionais são informados do teor e dos resultados dessa avaliação"* da *"execução, por parte das*

[32] Cfr. Fichas Técnicas sobre a União Europeia 2016: Cooperação Judiciária em Matéria Penal, pág. 4, www.europarl.europa.eu

autoridades dos Estados-Membros, das políticas da União referidas no presente título, especialmente para incentivar a aplicação plena do princípio do reconhecimento", nos termos do artigo 70º do Tratado sobre o Funcionamento da União Europeia.

Na mesma linha segue a redação do artigo 80º do mesmo diploma, ao afirmar que o Parlamento Europeu e os Parlamentos nacionais devem estar associados à *"avaliação das actividades da Eurojust"*; sendo estes mecanismos determinados por meio de novos regulamentos adoptados, tanto pelo Parlamento como pelo Conselho, segundo o processo legislativo ordinário.

Hoje em dia, as obrigações jurídicas e os compromissos políticos respeitantes à cooperação policial e aduaneira em matéria penal na União Europeia são enunciados no Tratado de Lisboa, na Convenção de Aplicação do Acordo de Schengen e nas conclusões do Conselho Europeu de Estocolmo de 2009.

5. O intercâmbio de informações como instrumento de cooperação policial na União Europeia

A troca de informações policiais na União Europeia é essencial para que haja uma cooperação policial eficaz.

No que diz respeito à troca de informações policias, existem dois instrumentos jurídicos fundamentais:

O primeiro é a Decisão-Quadro 2006/960/JAI do Conselho, de 18 de dezembro de 2006, que permitiu a simplificação da troca de dados e informações entre as autoridades de aplicação das leis dos Estados-Membros da União Europeia.

Esta Diretiva foi adotada no seguimento dos atentados de Madrid e veio instituir um novo regime jurídico que permite melhorar a transmissão das informações.

Um outro instrumento de igual importância foi a "Decisão Prüm", como é assim conhecida a Decisão 2008/615/JAI do Conselho, de 23 de junho de 2008.

Esta decisão visou aprofundar a cooperação transfronteiriça, principalmente no que diz respeito à luta contra o terrorismo e contra a criminalidade transfronteiras.

A Decisão Prüm pretende reforçar a cooperação policial ou judicial entre os Estados-Membros, no que respeita à matéria Penal, melhorando o próprio sistema de troca de informações entre autoridades encarregues de proceder à prevenção e investigação criminais.

A Decisão é constituída por disposições respeitantes ao acesso a ficheiros automatizados de análise de dados de ADN, de sistemas automatizados, de identificação dactiloscópica, a dados relativos a grandes acontecimentos e informação destinada a evitar atos terroristas e a outras medidas para reforçar a cooperação policial.

O artigo 18º da referida Diretiva, prevê, em caso de manifestações de massa ou quaisquer outros eventos de grande dimensão ou até de catástrofes ou acidentes graves, as possíveis formas de assistência policial entre Estados-Membros.

Esta Decisão prevê formas de assistência policial entre Estados-Membros através de unidades especiais de intervenção em situação de crise que sejam provocadas pela ação humana, que representem uma ameaça física grave e direta para as pessoas, bens patrimoniais, infraestruturas ou instituições, como por exemplo, a tomada de reféns, ou o desvio de aviões.

A Decisão 2008/617 prevê as regras e as condições gerais que permitem às unidades especiais de intervenção de um Estado-Membro prestar assistência ou atuar no território de outro Estado-Membro a pedido deste.

No entanto, esta Diretiva não abrangeu manifestações de massa, as catástrofes naturais nem os acidentes graves, tendo sido a referida Decisão Prüm que veio completar esta Decisão no que diz respeito à assistência policial entre os Estados-Membros numa destas situações.

5.1. O Modelo de Intercâmbio de Informações da União Europeia

5.1.1. A Decisão Prüm

"O Acordo de Prüm é um Acordo Internacional de tipo clássico, celebrado na cidade alemã de Prüm, a 27 de maio de 2005, entre o Reino da Bélgica, a Alemanha, a Espanha, a França, o Luxemburgo, os Países Baixos e a Áustria, que visa aprofundar a cooperação policial transfronteiras nomeadamente nos domínios da luta contra o terrorismo, a criminalidade organizada e a imigração ilegal e lança as bases para uma cooperação

avançada entre os Estados-Membros da União Europeia que desejam intensificar certos aspectos maiores da cooperação policial."[33]

A Decisão Prüm constitui um dos instrumentos jurídicos fundamentais no que respeita à troca de informações policiais.[34]

Esta Decisão estabelece regras mínimas que deverão ser cumpridas por todos os Estados-Membros, dizendo respeito à prova genética, aos dados dactiloscópicos e ao registo de matrículas de veículos, bem como, de outros meios de cooperação respeitantes a "Eventos importantes", "Prevenção de atentados terroristas", "Operações conjuntas", "Manifestações de massa, calamidades e acidentes graves", "utilização de armas de serviço, munições e equipamento", não deixando de lado as outras disposições do Tratado entre os Estados aderentes.[35]

Esta Decisão prevê a possibilidade dos Estados-Membros concederem reciprocamente direitos de acesso aos ficheiros de análise automatizada de ADN, aos sistemas automatizados de identificação dactiloscópica e aos dados de registo de matrícula de veículos.[36]

O Estado-Membro que analisa os dados provenientes de ficheiros nacionais de análise de ADN e dos sistemas automatizados de identificação dactiloscópica, pode, numa segunda fase, solicitar dados pessoais específicos ao Estado-Membro que administra o ficheiro e, se for o caso, solicitar informações adicionais mediante procedimentos de assistência mútua, incluindo os que foram adotados no âmbito da Decisão-Quadro 2006/960/JAI.

---

[33] V. a este respeito, *"Tratado de Prüm"*, www.dgai.mai.gov.pt

[34] Cfr. *"Tratado de Prüm"*, www.dgai.mai.gov.pt: *"Nos termos do Acordo de Prüm, o intercâmbio de informações abrange, para efeitos de prevenção e investigação de infracções penais e de manutenção da ordem e segurança públicas, as matérias relativas, nomeadamente, aos perfis de ADN, aos dados dactiloscópicos, a outros dados pessoais com aqueles relacionados, e aos dados relativos aos registos de matrícula de veículos".*

[35] Cfr. *"Tratado de Prüm"*, www.dgai.mai.gov.pt: *"O Acordo prevê, especificamente, medidas destinadas à prevenção de atentados terroristas, entre as quais se destaca a possibilidade de intervenção de agentes armados a bordo de aeronaves. No campo relativo à luta contra a imigração ilegal, o Acordo consagra medidas como as relativas ao destacamento de peritos em documentos falsos e à assistência em matéria de afastamento de nacionais de países terceiros."*

[36] Cfr. *"Tratado de Prüm"*, www.dgai.mai.gov.pt: *"Este Acordo contempla ainda normas relativas à proteção de dados que têm como objetivos regular o nível de proteção de dados, as finalidades da sua utilização, os aspectos relativos à sua conservação e transmissão, entre outros aspectos."*

Capítulo II – O Passenger Name Record (PNR)

1. O Passenger Name Record

A massificação das tecnologias da comunicação e informação, as migrações, bem como a desterritorialização do crime são fenómenos que têm suscitado acrescida preocupação por parte dos Estados, uma vez que, a par dar suas vantagens, estas acarretam uma série de desvantagens, as quais se pretende reduzir o seu impacto.

Ou seja, a intensificação dos fenómenos globais, levou a uma *"Globalização do Crime"*, o que faz com que a criminalidade já não seja apenas de cariz nacional, passando esta a ser um problema transfronteiriço.

A designação "*Passenger Name Record"* refere-se à base de dados utilizada pelas companhias aéreas e agências de viagens, através do registo das viagens feitas por uma pessoa.

Os dados são recolhidos de diversas formas, como por exemplo, através de reservas que podem ser criadas por organizações internacionais de vendas – *global distribution systems (GDS)*, ou através de *Computer reservation systems (CRS)*, isto é, através de um sistema informatizado de reservas com detalhes importantes do PNR, sendo que, de seguida são transmitidos à respetiva transportadora aérea.

No momento em que os dados estão a ser recolhidos, o/os passageiro/s deve/m ser informado/s que, por lei, o operador que estiver a recolher os dados, pode ser obrigado a facultá-los às autoridades públicas de um Estado que os solicitem – de acordo com os anexos II e III, que constam na folha de Anexos - essa informação deve ser ainda acompanhada de uma outra, que dá a conhecer ao passageiro a forma que ele tem para aceder aos seus próprios dados.

No entanto, os Estados devem ter em conta que não é possível verificar com exatidão se os dados PNR, recolhidos por operadores de aeronaves, estão corretos ou, até mesmo, completos.

Por isso, é que não devem ser tomadas medidas, em termos de sanções, contra uma operadora, não podendo esta ser considerada legal ou financeiramente responsável pela transferência dos dados PNR que tenha recolhido de Boa Fé e que, por qualquer meio, venha

a ser descoberto que essas informações que lhe foram fornecidas são falsas, enganosas ou incorretas.

Assim, existem mecanismos legalmente previstos para que, caso o passageiro, solicite o acesso aos seus dados pessoais e pretenda fazer alguma alteração ou correção aos mesmos, tal seja possível.

No entanto, existem, ainda, mecanismos que podem ser ativados pelos passageiros, caso verifiquem um uso abusivo dos seus dados pessoais PNR por parte das autoridades públicas estatais.

Estes dados respeitam ao nome completo do passageiro; à sua data de nascimento; à morada de casa e do trabalho; ao seu número de telefone; ao seu endereço de e-mail; à informação que consta do passaporte; bem como do seu cartão de crédito ou à forma como irá proceder ao pagamento da compra do bilhete; aos nomes e à informação pessoal dos contactos de emergência e, ainda, quanto à data da viagem, o itinerário da mesma, a agência de viagens através da qual o voo foi reservado e, também, quanto à preferência por uma outra refeição que não aquela que será servida durante a viagem, ou até mesmo, quanto à preferência do lugar no avião e também informações respeitantes à bagagem.

Para além destas, existem outras informações, também definidas no manual IATA, que podem ser incluídas no PNR, como é o caso dos "serviços solicitados", isto é, das necessidades alimentares e médicas especiais, de informações relativas a menor não acompanhado e, até, quanto a pedidos de assistência.

Existem, ainda, informações que podem ser acrescentadas pelos agentes das companhias aéreas, no campo *"Observações Gerais"* e que podem ser, igualmente, armazenadas na base de dados PNR.

Essas observações podem incluir comentários diversos e taquigrafia.

No entanto, o conteúdo exato das informações do PNR irá depender dos dados fornecidos pelo titular, uma vez que nem todos os campos são de preenchimento obrigatório.

Além disso, tanto o número como a natureza dessas informações num PNR varia, consoante se o sistema de reservas for o utilizado durante a reserva inicial ou, caso seja utilizado outro o mecanismo de recolha de dados, como é, por exemplo, o caso do – *DCS – Departure Control Systems.*

No *DCS,* as informações sobre os passageiros e sobre os próprios voos ficam apenas disponíveis a partir do momento em que o voo é "aberto" para o *check-in*, isto é, até 48 horas antes da partida, sendo que, as informações de controlo da partida para um voo serão finalizadas somente após o encerramento desse voo e podem permanecer disponíveis entre 12 a 24 horas, após a chegada do voo ao seu destino.

Os padrões de criação de PNR são detalhados no manual - *IATA´s Passenger Services Conference Resolutions Manual* e no *ATA/IATA Reservations Interline Message Procedures – Passenger (AIRIMP).*

Cabe, ainda, referir que a base de dados PNR não inclui informações que indicam, diretamente, a origem racial ou étnica, as opiniões políticas, as crenças religiosas ou filosóficas do indivíduo, a sua filiação sindical, informações quanto à sua saúde ou, até mesmo, informações respeitantes à sua vida sexual.

Quer isto dizer que o PNR não inclui termos que revelam informações pessoais, sendo que o Departamento de Segurança Interna utiliza um sistema automatizado que filtra alguns desses termos e apenas utiliza essas informações em circunstâncias excepcionais, como por exemplo, se a vida do indivíduo estivesse ameaçada ou em risco de vir a ser seriamente prejudicada.

As informações do PNR são recolhidas em sistemas de reserva, dias, meses ou mesmo um ano antes da data do voo.

Desta forma, as informações dos sistemas de reserva são dinâmicas, uma vez que a sua alteração se pode verificar a qualquer momento e continuadamente, a partir do momento em que o voo está aberto para reserva.

As informações da base de dados PNR ajudam os oficiais da Alfândega e Proteção de Fronteiras a determinar quais os passageiros que representam risco e que, por isso, devem ser sujeitos a uma inspeção adicional no local de partida ou de chegada e são eles os principais utilizadores dessas informações.

Estas informações recolhidas pelas companhias aéreas podem ser disponibilizadas a outras agências governamentais independentes do Departamento de Segurança Interna, unicamente com o objectivo de se fazer cumprir e aplicar a lei, se necessário.

De resto, por outro qualquer motivo, estas informações não podem ser compartilhadas fora do Departamento de Segurança Interna, a menos que a entidade requerida tenha necessariamente que saber alguma informação sobre determinado indivíduo, no entanto, estão obrigadas a proteger, devidamente, essas informações.

É, por isso, particularmente importante que as informações sejam protegidas, especialmente quando um Estado obtém informações PNR, devendo limitar ao máximo a utilização desses dados, para o efeito para o qual foram recolhidos; deve, igualmente, restringir o acesso a tais dados; limitar o período de armazenamento dos mesmos, de acordo com os fins para os quais os mesmos são transferidos; garantir que as pessoas possam solicitar correções ou anotações quanto aos seus dados, caso seja necessário e, por último, assegurar que os protocolos de transferência de dados e sistemas automatizados se encontram no local apropriado para aceder ou receber os dados de acordo com as diretrizes próprias.

Devem, ainda, ser tomadas precauções contra o mau uso dos dados ou contra o abuso na sua utilização por parte das autoridades estatais.

Para se evitar a divulgação não autorizada, cópia ou, até mesmo, utilização ou alteração dos dados fornecidos a um Estado, o Estado receptor deve restringir o acesso a essa informação e utilizar mecanismos de segurança reconhecidos, como por exemplo, através de senhas de acesso, criptografia, entre outras, de modo a impedir o acesso não autorizado aos dados PNR contidos nos seus sistemas de computadores e redes.

Atualmente encontram-se disponíveis dois sistemas possíveis de transferência de dados PNR e são eles:

1. O sistema de importação *"pull"*, segundo o qual as autoridades públicas estatais, que solicitam os dados, podem aceder ao sistema de operador de aeronaves e extrair – *"pull"*- uma cópia dos dados necessários através do banco de dados.
2. O sistema de exportação *"push"*, de acordo com o qual os operadores de aeronaves transmitem - *"push"* –, os dados de PNR solicitados, para o banco de dados da autoridade requerente.

Os Estados devem ter em conta, em cada um dos métodos, as opções de proteção de dados e de avaliação de risco, bem como, o impacto económico que cada método comporta

em relação a cada Estado e a cada operador, relativamente ao suporte dos sistemas e, ainda, relativamente à transferência de dados em curso.

Muito embora, seja recomendável que os Estados adotem o sistema *"push"*, tendo em conta que a posição que os operadores ocupam, neste método, é uma posição de guardiões e controladores dos dados PNR, não significa que não devam considerar cuidadosamente os custos das várias opções para a recolha de dados PNR.

Ou seja, existem custos diferentes conforme seja o sistema *"pull"* ou *"push"*, sendo que, antes de tomar uma opção sobre qual dos métodos adotar, o Estado deve consultar os operadores, de modo a perceber qual o método mais vantajoso, a fim de minimizar os custos, para si.

Até porque, quando os Estados exigem a transferência de dados PNR, eles devem ter em conta os custos que irão comportar ao acolherem operadores de outros Estados, devendo, igualmente, perceber qual o impacto que as infraestruturas, que são necessárias para tal, irão ter no seu território.

Além disso, convém referir que os Estados não devem armazenar os dados PNR para além do tempo considerado necessário para os fins que estiveram na base da sua recolha.

As informações pessoais são mantidas de uma forma segura e confidencial e não podem ser divulgadas a qualquer pessoa dentro ou fora da Alfândega e Proteção de Fronteiras, a menos que, como acima foi dito, estejam de acordo com a lei, com os regulamentos e com as políticas de uso do Sistema de Identificação Automático, designado nos EUA por ATS – *Automated Targeting System* e, ainda, que estejam no exercício das suas funções oficiais.

Esta proteção e salvaguarda cuidadosa dos dados pessoais, engloba controles adequados de segurança, através de auditorias adequadas e acordos escritos com agências independentes do Departamento de Segurança Interna, por forma a garantir que os dados pessoais não são usados ou acedidos de forma indevida.

Além disso, um Estado deve assegurar que cada autoridade pública com acesso aos dados PNR é detentora de um nível adequado de gestão e proteção desses dados.

Outra forma de salvaguardar estes dados, passa pelos próprios funcionários do Departamento de Segurança Interna, que gerem o acesso a estas informações junto da ATS –

Automated Targeting System, bem como, através do sistema de empresários e gerentes, que zelam pela aplicação das leis, regulamentos e seguem as políticas e os procedimentos aplicáveis à ATS – *Automated Targeting System* e ao Departamento de Segurança Interna no desenvolvimento, implementação e operação de sistemas de informação sob o seu controlo.

O sistema de empresários e gerentes estabelecem e mantêm medidas de segurança administrativas, técnicas e físicas apropriadas para proteger as informações pessoais, realizando, para isso, uma avaliação de risco de modo a poder identificar os riscos da violação da privacidade dos dados, determinando quais os controlos de segurança adequados por forma a protegê-los desses riscos.

Certificam, também, que o acesso a essas informações pessoais só é permitido se em causa estiver uma necessidade relevante para um fim que seja legalmente tutelado ou autorizado, e que essas informações, quando recolhidas, são utilizadas para o fim solicitado, garantindo, igualmente, que a destruição dessas informações é feita de acordo com as leis, regulamentos, políticas e procedimentos do Departamento de Segurança Interna e com a ATS – *Automated Targeting System*.

Outras entidades independentes dos serviços de tráfego aéreo, que possam ter acesso às informações pessoais, devem cumprir com os requisitos dos acordos escritos existentes.

Acresce, ainda, que, caso haja um Estado que não tenha regulação especial para a proteção de dados pessoais, os outros Estados dispõem de procedimentos para proteger os dados PNR, devendo, para isso, desenvolver leis e regulamentos de proteção desses dados relativos à sua transferência e ao seu processamento.

Uma questão que pode surgir quando se pensa em dados pessoais, prende-se com o consentimento do indivíduo a quem esses dados são recolhidos.

Ora bem, em primeiro lugar, quem informa o público relativamente a esta recolha de informação é a ATS SORN – *System of Records Notices* – em conjunto com a ATS – *Automated Targeting System*.

ATS SORN é um conjunto de fichas onde se encontram registados os tais dados pessoais dos indivíduos e que estão sob o controlo de um órgão, a partir do qual essa informação é recuperada através de um identificador atribuído ao indivíduo.

A *Privacy Act* exige que cada agência de viagens coloque as suas informações no Registo Federal.

Ora, como a ATS – *Automated Targeting System*, em português, Sistema de Identificação Automático não recolhe PNR diretamente aos indivíduos, estes não têm oportunidade de consentir quanto à sua recolha.

Também não faria sentido, pedir o consentimento na recolha desses dados pessoais aos indivíduos afectados, tendo em conta que, esses dados PNR são recolhidos pelas companhias aéreas, para efeitos de reserva de bilhetes de avião, as quais encaminham esses dados PNR para a Alfândega e Proteção das Fronteiras, com o propósito de a auxiliar, impedindo assim, o indivíduo de poder exercer controlo sobre eles.

A ATS-P – *Privacy Impact Assessment* – está ligada a registos de vigia da aplicação da lei, já a Alfândega e Proteção de Fronteiras corresponde às atividades de execução e de investigação, como é o caso de ameaças específicas e credíveis, ou os próprios voos, os indivíduos e, ainda, as rotas de interesse e, por isso, é que ambas se complementam, uma vez que, o facto de essas informações permanecerem acessíveis, ajuda na prossecução dessas atividades e, consequentemente, na aplicação da lei.

Qualquer pessoa com residência legal permanente, independentemente da sua cidadania, que pretenda solicitar o acesso ao seu PNR, através do Departamento de Segurança Interna, pode fazê-lo, de acordo com a Lei da Liberdade de Informação – FOIA – *Freedom of Information Act*.

A Lei da Privacidade de 1974 protege a informação pessoal e regula o modo como o Governo pode divulgar, compartilhar ou consentir o acesso a essa informação e como mantém as informações pessoais que recolhe.

O Departamento de Segurança Interna alarga a aplicação da Lei da Privacidade à capacidade de aceder e alterar os registos, a todas as pessoas, qualquer que seja a sua cidadania, através de um sistema misto, isto é, através de um sistema de informação relativamente a cidadãos, quer americanos, quer de outra qualquer nacionalidade, residentes nos Estados Unidos.

O Departamento de Segurança Interna considera a ATS-P – *Privacy Impact Assessment* – um sistema misto na medida em que permite que os cidadãos estrangeiros

possam, também, solicitar, tanto o acesso, como a alteração dos dados, nos termos da Lei da Privacidade.

No entanto, está vedado o acesso a informações relativas às operações e às atividades do Governo Federal dos Estados Unidos, de acordo com *"DHS Privacy Memorandum Number: 2007 – 1 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons"*.

Os pedidos de acesso a informações pessoais contidas na ATS-P – *Privacy Impact Assessment* – incluindo os dados PNR podem ser submetidos ao Escritório Sede FOIA. Esses pedidos de acesso deverão estar conformes com certos requisitos que prevêm as regras para o pedido de acesso a essas informações, mantidas pelo Departamento de Segurança Interna.

Tanto na carta como no envelope deve ser aposta, de uma forma visível, *"Privacy Act Access Request",* devendo o pedido incluir uma descrição geral dos registos procurados e deve incluir o nome completo do solicitante, o seu endereço atual, bem como a data e o local de nascimento.

Por fim, o pedido deverá ser devidamente assinado e reconhecida a assinatura, sob pena de se considerar perjúrio.

2. Funções do Passenger Name Record (PNR) no domínio da luta contra a criminalidade

Tal como acima foi dito, o terrorismo e o crime organizado envolvem, muitas das vezes, viagens internacionais.

Por isso é que as informações reunidas pelas transportadoras aéreas, sobre viagens se torna um instrumento tão importante para as autoridades, no que respeita à aplicação da lei, de modo a prevenir, detectar e investigar o crime e punir os criminosos.

Como já foi anteriormente explicado, o PNR é um conjunto de informações pessoais dos passageiros recolhidas pelas companhias aéreas, no momento da reserva dos bilhetes de avião, e que ficam armazenadas nos bancos de dados de reserva das companhias aéreas e de controlo de partidas.

Muitos Estados, quer dentro e fora da União Europeia, utilizam os dados PNR para fins de combate ao terrorismo e à criminalidade organizada, considerando os mesmos que

esses dados são de extrema importância no momento de avaliar as possíveis ameaças por parte do terrorismo e da criminalidade organizada.

A análise dos dados PNR, fornece aos Estados a identificação de potenciais passageiros considerados de alto risco, dando-lhes capacidade para:

1. Melhorar a segurança da aviação;
2. Melhorar a segurança nacional e da própria fronteira;
3. Prevenir e combater os atos terroristas e crimes relacionados e, ainda, outros crimes de natureza transnacional, incluindo o crime organizado, fazendo cumprir mandados e impedir fugas da prisão;
4. Proteger os interesses vitais, não só dos passageiros, mas de todos em geral, incluindo a saúde;
5. Melhorar o controlo das fronteiras nos aeroportos; e
6. Facilitar e salvaguardar o tráfego de passageiros.

A transferência de dados entre os Estados deve ser feita de uma forma harmonizada, de modo a que não prejudique a capacidade de cada Estado aplicar a sua lei e preservar a sua segurança nacional e a sua segurança pública.

Se a transferência for feita de forma harmonizada, permite-se que todos os Estados possam beneficiar da análise dos dados compartilhados para fins de segurança; permite-se, ainda, que todos os operadores de aeronaves beneficiem de requisitos comuns para a transferência de dados PNR e, por último, que todos os passageiros possam beneficiar da proteção dos seus dados PNR.

Por esta razão é que a transferência de dados entre os Estados se torna tão importante, e para isso importa estabelecer medidas uniformes, de acordo com as seguintes regras:

1. Minimizar o custo para a indústria;
2. Exatidão das informações;
3. Indicar de forma exaustiva e completa dos dados;
4. Garantir a proteção dos dados pessoais;
5. Oportunidade e eficiência na gestão/gestão de risco dos dados.

Durante quase 60 anos, os dados PNR foram utilizados manualmente, por autoridades alfandegárias e aplicadoras da lei em todo o Mundo.

No entanto, como em causa estava a boa aplicação da lei, o desenvolvimento tecnológico tornou possível o uso desses dados de forma mais sistemática e rápida, o que permitiu melhorar essa tarefa.

A análise dos dados PNR permite identificar os viajantes de alto risco no contexto da luta contra o terrorismo, no crime de tráfico de drogas, no crime de tráfico de seres humanos, crime de exploração sexual de crianças, entre outros crimes.

Isto é, com a recolha desta informação pretende-se que a Alfândega e Proteção de Fronteiras possa tomar decisões precisas sobre os passageiros que necessitam de uma inspeção adicional no porto de entrada, de acordo com a lei ou com outras informações.

O Departamento de Segurança Interna e a Alfândega e Proteção de Dados utiliza a base de dados *"Passenger Name Record"* apenas para prevenir, detectar, investigar os crimes de terrorismo e os relacionados, incluindo condutas que envolvam atos violentos ou um qualquer ato perigoso para a vida humana.

Servem, também, para prevenir as atividades que constituem perigo e que estão devidamente definidas nas convenções e protocolos internacionais aplicáveis em matéria de terrorismo, e ainda, crimes que são punidos com pena de prisão igual ou superior a três anos e que têm natureza transnacional.

Para o efeito, são considerados crimes transnacionais os que são cometidos em mais do que um país; os que são cometidos num país mas a sua preparação é maioritariamente planeada, direcionada ou controlada noutro país; os que são cometidos num país mas envolve uma organização criminal que atua em mais do que um país; os que são cometidos num país mas com efeitos substanciais noutro país ou, por último, os que são cometidos num determinado país, e o autor do crime encontra-se nesse mesmo país ou pretende viajar para outro.

Considera-se estar perante uma organização criminal, *"desde que reportada a uma dada tipologia penal – cujo catálogo é cada vez mais uniforme, dado o processo de integração europeia (e mesmo de outros processos de integração regionais) e de cooperação internacional nos domínios do crime organizado e do terrorismo -, e não a específicos tipos de crime."* (Jorge dos Reis Bravo, 2014, p. 3).

Foi no ano de 2000, mais concretamente a 15 de novembro, no âmbito dos trabalhos da Convenção da ONU sobre o Crime Organizado Transnacional, que se acordou quanto ao

conceito de Criminalidade Organizada, definindo, para isso, o seu artigo 2º, alínea a) *"grupo criminoso organizado"* como *"um grupo estruturado de três ou mais pessoas, existindo durante um período de tempo e actuando concertadamente com a finalidade de cometer um ou mais crimes graves ou infracções estabelecidas na presente Convenção, com a intenção de obter, directa ou indirectamente, um beneficio económico ou outro beneficio material"*[37].

O Departamento de Segurança Interna e a Alfândega e Proteção de Dados utiliza a base de dados *"Passenger Name Record"* para, sempre que haja suspeita de uma ameaça grave, possa proteger os interesses vitais de uma pessoa ou grupos de pessoas.

Além disso, esta base de dados contém as informações necessárias, para saber que passageiros estão sujeitos a um exame mais detalhado à entrada ou à saída dos Estados Unidos.

Qualquer pessoa que viaja para ou a partir dos Estados Unidos, está abrangida por este programa.

2.1. A Retenção de Dados

Outra questão relevante, é perceber durante quanto tempo essa informação é retida.

O período de retenção dos dados pessoais não é superior a quinze anos, o que, ultrapassado esse período de tempo, os dados serão apagados.

No entanto, existem algumas nuances quanto a este período de retenção dos dados pessoais.

A primeira, é que os usuários da ATS-PIA – *Privacy Impact Assessment* - têm acesso geral aos dados PNR, por um período de cinco anos, o que, após esse período, os dados passarão para um estado cuja designação é *"não operacional"*.

Logo após os primeiros seis meses, o PNR é como que "despersonalizado", isto é, informações como o nome do indivíduo, as suas informações de contato e outras informações

[37] Cfr. o texto oficial da Convenção em versão portuguesa, no site http://www.gddc.pt/cooperacao/materia-penal/textos-mpenal/onu/ConvCrimOrganiz.pdf.

pessoais não ficam abertamente identificáveis, isto é, o registo do indivíduo já não fornece diretamente estes dados.

O estado *"não operacional"* dos dados PNR, é mantido por mais dez anos e o acesso a estes dados, só é permitido com autorização prévia de supervisão e apenas como resposta a um caso que esteja identificado como sendo de ameaça ou de risco.

Desta forma, através deste acesso limitado ao PNR mais antigo, consegue-se um equilíbrio razoável, por um lado, entre a proteção dessas informações e, por outro, que a Alfândega e Proteção de Fronteiras continue a identificar potenciais viajantes de alto risco.

2.2. O intercâmbio de prova genética e a cooperação transnacional

Foi na década de 90 do séc. XX que surgiram, na Europa, nos EUA, no Canadá e na Austrália, as bases de ficheiros contendo dados pessoais, bem como perfis de ADN de cidadãos e que, desde logo, começaram a suscitar questões de natureza quer ética quer jurídica.

Cedo se percebeu que a recolha de informações, resultantes das bases de dados dactiloscópicos ou de perfis de ADN, constituíam instrumentos importantes no campo da investigação e repressão criminal, uma vez que contribuíam para a cooperação inter-policial e entre as autoridades judiciárias, quer no que respeita à sua dimensão territorial, quer quanto à sua incidência material e objetiva.

Segundo Jorge dos Reis Bravo as análises de ADN constituem um meio probatório bastante seguro e cientificamente confirmado, *"sendo o seu estatuto epistemológico que lhe tem permitido a afirmação generalizada e reconhecimento nos mais variados domínios, ao nível de decisores nacionais, supra-nacionais e mundiais"*.

Ora, por aqui se percebe que os contributos da genética forense em matéria de ADN, são a maior expressão do avanço científico na área da Medicina Legal e das Ciências Forenses.

Apesar disso, o valor do meio probatório dos perfis de ADN, ainda levanta alguns problemas, quer a nível nacional, quer a nível da cooperação transnacional, uma vez que, dada a sua expansão para vários sistemas jurídicos, tornou-se difícil encontrar entendimentos, práticas e regimes rigorosamente semelhantes.

Outro problema que o valor probatório dos perfis de ADN tem levantado é a dicotomia entre as questões éticas, jusfundamentais, questões profissionais e, ainda, as estritamente profissionais, uma vez que esses perfis de ADN têm uma importância fundamental no que respeita à perseguição e à responsabilização dos culpados. Mas por outro lado, tem de haver, ao mesmo tempo, a proteção da integridade pessoal, da liberdade, da intimidade e da autodeterminação informacional e genética.

Ou seja, no fundo, tudo isto leva a uma ponderação da prevalência dos valores em causa, mas sem que nunca constitua um entrave à atuação do legislador.

Tanto o Conselho da Europa, como a própria União Europeia têm mostrado uma grande preocupação no que respeita a esta questão, sendo que, para isso, têm incentivado os Estados-Membros a aprovar e a adotar regulamentação interna e a aderir a vários mecanismos e instrumentos capazes de atingir um estado de cooperação policial e judiciária, de modo a reforçar a eficiência na prevenção e repressão do crime, principalmente, do crime organizado transnacional.

Desta forma, as questões de auxílio judiciário mútuo em matéria penal foram objeto de regulamentação, e aprofundamento por Decisões-Quadro e Decisões Adotadas pelo Conselho da União Europeia.

Como acima se referiu, estas Decisões-Quadro têm por base o princípio do reconhecimento mútuo, instituído pelo Conselho de Tampere, como sendo o pilar da cooperação judiciária civil e penal da União Europeia[38].

A questão que apraz colocar é a de perceber porque são as bases de dados de perfis de ADN, uma forma de identificação automática que importa às autoridades estaduais da UE, na execução das suas tarefas e, ainda assim, este método não foi completamente integrado, não permitindo, por isso, o acesso e a consulta dessas bases pelas autoridades.

Certo é que, atualmente, existe alguma desorganização nesta matéria, uma vez que a coexistência de várias bases de dados de perfis de ADN autónomas faz com que *"...o mesmo*

[38] Cfr. § 33 das Conclusões e Conclusões 40.ª e 43.ª da Declaração Final do Conselho Europeu de Tampere, de 15 e 16 de outubro de 1999: "C. LUTA CONTRA A CRIMINALIDADE A NÍVEL DA UNIÃO 40.ª O Conselho Europeu está profundamente empenhado em reforçar a luta contra as formas graves de criminalidade organizada e transnacional. Para se alcançar um elevado nível de segurança no espaço de liberdade, de segurança e de justiça, é necessária uma abordagem eficaz e abrangente da luta contra todas as formas de criminalidade. Deverá desenvolver-se a nível da União um conjunto equilibrado de medidas contra a criminalidade, protegendo simultaneamente a liberdade e os direitos legais dos indivíduos e dos operadores económicos"; "43.ª A cooperação entre autoridades dos Estados-Membros deverá traduzir-se num máximo de benefícios, pelo que o Conselho Europeu apela à criação, como primeira medida e o mais rapidamente possível, de equipas de investigação conjuntas, tal como previsto no Tratado, para combater o tráfico de drogas e de seres humanos e o terrorismo. As regras a estabelecer neste contexto devem permitir a participação, como reforço dessas equipas, de representantes da Europol, quando adequado."

indivíduo possa ter o seu perfil de ADN inserido em ficheiros de várias bases, numa(s) a título de mero suspeito ou de arguido, noutra(s) de condenado." (Jorge dos Reis Bravo, 2014, p. 8)

Por outro lado, a existência de um perfil da mesma pessoa em várias bases pode consubstanciar num acréscimo de segurança.

Atualmente, o modelo vigente, prende-se com a autonomia de cada ordenamento nacional para definir internamente quais os critérios de preenchimento e administração das bases de dados genéticas que pretende adotar, bem como o intercâmbio da informação com os restantes Estados-Membros, de acordo com o princípio da disponibilidade[39].

A opção política atual e o modelo que prevalece é o da "colocação em rede das bases de dados nacionais dos Estados-Membros".

No que diz respeito à cooperação relativa à partilha e intercâmbio de prova genética, importa perceber e enquadrar a cooperação que existe entre Portugal e os Estados Unidos da América.

Tal cooperação foi admitida pelo Acordo celebrado entre a República Portuguesa e os Estados Unidos da América, assinado em Lisboa em 30 de junho de 2009, de modo a Reforçar a Cooperação no Domínio da Prevenção e do Combate ao Crime, aprovado pela Resolução da AR n.º 128/2011, de 31-08-2011[40], abrangendo, também, a troca de informações sobre dados dactiloscópicos.

De modo a reforçar a cooperação na luta contra o crime, em especial, contra o terrorismo, o referido Acordo deve *"abranger apenas os crimes que constituem uma infracção punível nos termos do direito interno das partes com pena privativa de liberdade de duração máxima superior a um ano ou com uma pena mais grave"* (artigo 2º, n.º3).

O Conselho Europeu foi o motor de arranque da cooperação judiciária europeia em matéria de prova genética, tendo incentivado os Estados-Membros a institucionalizar o uso de análises de ADN para diversos fins e, ainda, a adotar sistemas de armazenamento de amostras biológicas, bem como, dos perfis genéticos obtidos.

A Recomendação n.º R (92) 1, é o instrumento referencial no contexto da cooperação judicial em matéria de prova genética, tendo sido adotada pelo Comité de Ministros do Conselho da Europa a 10 de fevereiro de 1992. Esta Recomendação, referenciava a

[39] Ou seja, "(...) um funcionário responsável pela aplicação da lei de um Estado-Membro da União que necessite de informações para poder cumprir as suas obrigações pode obtê-las de outro Estado-Membro, e que as autoridades de aplicação da lei do Estado-Membro que detém essas informações as disponibilizarão para os efeitos pretendidos, tendo em conta a necessidade dessas informações para as investigações em curso nesse Estado" (ponto 4 do Preâmbulo da Decisão 2008/615/JAI do Conselho, de 23 de Junho).
[40] Pub. DR 1.ª Série, n.º 199, de 17-10-2011.

possibilidade de armazenamento desses perfis genéticos em relação aos condenados por crimes contra a vida, contra a integridade física e, até mesmo, quanto à segurança das pessoas.

A União Europeia procurou, em todos os sentidos, harmonizar os ordenamentos jurídicos nacionais em relação a alguns aspectos essenciais, como os de âmbito técnico-científico, nomeadamente quanto à uniformização e certificação de *kits* de marcadores de ADN, credenciação de entidades laboratoriais e procedimentos analíticos – e também a nível jurídico, definindo as condições para a implementação desses métodos, e seus pressupostos de admissibilidade e competência.

Para que a recolha de dados de ADN seja útil, é necessário que haja intercâmbio dessas informações entre os Estados-Membros e, como tal, é necessário referir a esse respeito a Resolução 97/C 193/02, do Conselho, de 9 de junho de 1997, relativa ao intercâmbio de resultados de análises de ADN e que incentivou os Estados-Membros à criação de bases nacionais de dados de ADN, de modo a garantir o intercâmbio desses resultados.

Esta Resolução sugere aos Estados a estruturação desses resultados, de acordo com os mesmos marcadores, e que possibilitassem o tratamento informático desses mesmos resultados.

A par da necessidade de haver intercâmbio de resultados de análises de ADN, surgiu a Resolução 2001/C 187/01, do Conselho, de 25 de junho de 2001, que reforçou o convite para que os Estados adotassem uma série de marcadores de ADN, aquando da análise e tratamento de ADN para fins judiciais, assim designados de *Sete Marcadores ESS: European Standard Set*, por forma a facilitar o intercâmbio desses resultados.

Assim, foi aprovada a Resolução 2009/C 296/01 do Conselho, de 30 de novembro de 2009, que veio alterar o número de marcadores de ADN[41], da Série Uniformizada Europeia (ou ESS), passando de sete para doze, sendo a Portaria n.º 270/2009, de 17 de março que fixa, nos termos do art. 12.º da Lei n.º 5/2008[42], os marcadores de ADN que integram os ficheiros da base de perfis de ADN, contemplando apenas seis dos doze marcadores indicados na Resolução como de "inserção obrigatória".

---

[41] De acordo com a Resolução 2009/C 296/01 do Conselho, de 30 de Novembro de 2009 – *"Marcador de ADN consiste numa molécula de ADN que, tipicamente, contém informações diferentes para indivíduos diferentes. Um marcador genético é uma região variável do genoma, ou seja, um sistema de variantes normais (polimorfismos), que se apresenta de forma diferente em cada pessoa. A utilidade de um polimorfismo genético enquanto "marcador" é tanto maior quanto maior for o número de variantes possíveis e quanto mais aproximadas forem as frequências repetitivas de cada uma delas, i.e., quanto mais frequentes forem as suas formas mais raras e individualizáveis. Os polimorfismos podem conter-se na região codificante (exões) ou na região não-codificante (intrões) dos genes, ou fora deles, podendo até ser simples substituição de uma base (Adenida, Citosina, Guanina e Timina) ou a variação numa sequência repetitiva de duas ou mais bases (nesse caso, o polimorfismo será o número de repetições, muito variável, dessa sequência)".*

[42] A versão atual da Lei n.º 5/2008, de 12 de fevereiro, é a Lei n.º 40/2013, de 25 de junho

Outro instrumento de grande relevância ao nível da cooperação de fornecimento de informações, foi a já mencionada Decisão Prüm.[43]

Esta Decisão tornou-se fundamental no que respeita ao fornecimento de informações como os dados dactiloscópicos, bem como quanto aos registos de veículos.

A Decisão Prüm tem por objetivo aprofundar a cooperação transfronteiras, entre as partes contratantes, através da:

1. *"Consulta e comparação automatizadas de perfis de ADN e dados dactiloscópicos em bases de dados de outra ou outras Partes Contratantes, e subsequente troca de informações em caso de comparação positiva no quadro de um caso concreto (artigos 2.º a 11.º), de prevenção em geral (artigos 13.º a 15.º) ou de prevenção de actos terroristas (art. 16.º);*
2. *Consulta automatizada mútua das bases de dados de matriculas de veículos automóveis, nos outros Estados (art. 12.º);*
3. *Troca de informações de natureza pessoal ou não pessoal, para prevenir a ocorrência de acções terroristas, e para a manutenção da ordem e segurança públicas em caso de grandes eventos, catástrofes ou acidentes graves (artigos 16.º a 19.º);*
4. *Coordenação e apoio mútuo em caso de agentes de segurança armados em voos dos Estados Contratantes (artigos 17.º e 18.º);*
5. *Coordenação e apoio mútuo na luta contra a imigração ilegal, nomeadamente pelo uso de consultores em documentação falsa e aquando da expulsão (artigos 20.º e 21.º);*
6. *Reforço da cooperação policial transfronteiras ao nível operacional, nomeadamente pela implementação de operações conjuntas e de intervenções transfronteiriças a pedido, ou por iniciativa própria em caso de urgência (artigos 24.º, 25.º e 27.º).* (Jorge dos Reis Bravo, 2014, p. 12)

Portugal não se vinculou ao Tratado de Prüm, no entanto, tal como todos os Estados-Membros não subscritores, veio a ser abrangido pela Decisão-Quadro 2008/615/JAI, que prevê aspectos essenciais relativos à cooperação transacional em matéria de prova genética.

---

[43] *"Tratado de Prüm"*, www.dgai.mai.gov.pt: *"As matérias reguladas no Acordo que não foram integradas no ordenamento jurídico da União Europeia, (...), são as matérias relativas à intervenção de agentes armados a bordo de aeronaves (Artigo 17.º do Acordo), ao porte de armas de serviço, munições e equipamento daqueles agentes (artigo 18.º, idem), bem como as medidas atinentes à luta contra a imigração ilegal (artigos 20.º e seguintes, idem), as medidas em caso de perigo iminente (artigo 25.º, idem) e as obrigações de prestação de assistência a pedido (artigo 27.º, idem)."*

No entanto, em matéria de intercâmbio de prova genética, Portugal está abrangido pelos seguintes instrumentos jurídicos em vigor na União Europeia:

- Decisão-Quadro 2006/960/JAI do Conselho, de 18 de dezembro de 2006, que respeita à simplificação do intercâmbio de dados e informações entre as autoridades de aplicação da lei dos Estados-Membros da União Europeia;

- Decisão 2008/615/JAI do Conselho, de 23 de junho de 2008, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras. Esta Decisão contém disposições baseadas nas principais disposições do Tratado de Prüm, que têm em vista melhorar o intercâmbio de informações, nos termos das quais os Estados-Membros se concedem reciprocamente direitos de acesso aos ficheiros de análise automatizada de ADN, aos sistemas automatizados de identificação dactiloscópica e aos dados de registo de matrícula de veículos.

  A Decisão prevê a possibilidade de acesso recíproco aos ficheiros de análise automatizada de ADN, aos sistemas automatizados de identificação dactiloscópica e aos dados de registo de matrícula de veículos.

  Ou seja, dever-se-á permitir ao Estado-Membro que efetua a consulta de dados provenientes de ficheiros nacionais de análise de ADN, solicitar, numa segunda fase, dados pessoais específicos ao Estado-Membro que administra o ficheiro e, caso seja necessário, solicitar informações adicionais de acordo com procedimentos de assistência mútua, incluindo os que foram adotados no âmbito da Decisão-Quadro 2006/960/JAI;

- A Decisão 2008/616/JAI do Conselho, de 23 de junho de 2008, que fixa os detalhes e pormenores técnicos de execução da Decisão 2008/615/JAI, de 23 de junho de 2008;

- A Decisão-Quadro 2009/905/JAI do Conselho, de 30 de novembro de 2009, respeitante à creditação de prestadores de serviços forenses que desenvolvem atividades laborais, nomeadamente, relativas a perfis de ADN e de dados

dactiloscópicos e de reconhecimento de resultados de acordo com a EN ISO/IEC 17025[44].

Os Laboratórios previstos no n.º 2 do artigo 5.º da Lei n.º 5/2008 adotarão as condições que forem necessárias para satisfazer os requisitos internacionalmente fixados para a acreditação da área laboratorial de análises de ADN em sede de controlo de procedimentos, validação de análises, padronização de metodologias e certificação de equipamentos (art. 40.º da Lei n.º 5/2008).

- A Decisão-Quadro 2009/948/JAI do Conselho, de 30 de novembro de 2009, trata da prevenção e resolução de conflitos de exercício de competência em processo penal. Esta Decisão prevê a obrigação de contacto entre as autoridades competentes dos Estados-Membros, de forma a poder confirmar a existência de processos penais paralelos que digam respeito aos mesmos factos e à mesma pessoa, permitindo a existência de um mecanismo de intercâmbio de informações, através de consultas entre aquelas autoridades para definir uma solução que seja desejável e que poderá levar à concentração dos processos conduzidos em paralelo num único Estado-Membro.

- Decisão-Quadro 2008/978/JAI do Conselho, de 18 de dezembro, referente ao mandado europeu de obtenção de provas destinado à obtenção de objetos, documentos e dados para utilização no âmbito de processos penais. A importância deste instrumento deve-se ao facto de ter introduzido, no quadro jurídico da União Europeia, o Mandado Europeu de Obtenção de Provas (MEOP), permitindo a obtenção e transferência de objetos, documentos e dados em determinadas condições.

  No entanto, a Decisão MEOP veio a ser ultrapassada pela Diretiva DEI (Decisão de Execução e Investigação), aprovada pelo Parlamento Europeu em 27 de fevereiro de 2014.

Em relação à Decisão-Quadro 2008/978/JAI do Conselho, de 18-12-2008 (MEOP), o seu artigo 4.º, n.º2, alínea b) exclui expressamente do seu âmbito os *"exames físicos ou*

[44] *Todavia, chama-se a atenção para a aprovação de uma Norma Internacional mais avançada, a ISO 15189 (MARIA ADELINA C. AMARAL GOMES, "Relevância da Qualidade na Actividade dos Laboratórios de Genética Forense", Genética Forense – Perspectivas de Identificação Genética (MARIA DE FÁTIMA PINHEIRO Coord.), Ed. Universidade Fernando Pessoa, Porto, 2010, p. 328.* (Jorge dos Reis Bravo, 2014, p.15).

recolha de elementos materiais ou dados biométricos directamente de um corpo humano, incluindo amostras de ADN ou impressões digitais".

A recolha de amostra biológica, diretamente do corpo humano através, por exemplo, de uma zaragatoa bucal não é possível ser objecto de pedido de execução/obtenção ao abrigo de tal instrumento, muito menos é possível que recolha de sangue, urina, tecidos, ou outro tipo de colheita, constituam amostras biológicas.

No entanto, esta matéria foi incluída, no que respeita ao intercâmbio em matéria de ADN, na Decisão 2008/615/JAI, no seu artigo 7.º.

Se, no âmbito de uma investigação, não estiver disponível o perfil de ADN de uma determinada pessoa que se encontre no território do Estado-Membro requerido, é essencial solicitar a este Estado auxílio judiciário através da recolha e da análise do material genético da pessoa em causa, bem como a transmissão do perfil de ADN obtido.

Quer isto dizer, que o artigo 7.º da Decisão supra mencionada, consagra um procedimento que tem em vista a cooperação e prestação de auxílio judiciário em matéria de obtenção de provas, no que respeita à recolha e análise de material genético de uma pessoa que se encontre no Estado-Membro requerido, e ainda, a transmissão do perfil de ADN obtido.

Cabe, agora, perceber se as Decisões Prüm necessitam de "disposições de aplicação" e em que termos.

As Decisões são atos jurídicos da União Europeia, através das quais o Conselho da União Europeia exerce o seu poder de decisão, senão vejamos a definição de Decisão prevista no artigo 288º do Tratado da União Europeia *"A Decisão é obrigatória em todos os seus elementos. Quando designa destinatários, só é obrigatória para estes"*.

As Decisões podem dirigir-se aos Estados, e, podem mesmo obrigá-los a adotar, na sua ordem interna, as medidas legislativas, regulamentares ou administrativas que a própria decisão prescreve.

As Decisões não exigem "transposição" para serem válidas ou eficazes na ordem jurídica interna. O que poderá ser necessário, é adequar a legislação ou regulamentação interna, através da revogação ou da aprovação de novos atos, ao conteúdo da Decisão, caso entre eles haja incompatibilidade insanável.

Ora, vejamos agora, que quanto às disposições da Decisão 2008/615/JAI, em relação ao intercâmbio de prova genética, cabe ao legislador nacional a adoção de medidas com vista à sua plena execução na ordem jurídica interna[45].

A Decisão em análise prevê a possibilidade de os Estados-Membros poderem adotar as *"medidas necessárias para o cabal cumprimento"* das suas disposições, tal como prevê o seu artigo 36º, n.º1.

A Decisão 2008/616/JAI contém as disposições administrativas e técnicas que são necessárias à execução da Decisão 2008/615/JAI, contendo, ainda, um Anexo com todas as informações pormenorizadas quanto à sua execução técnica e administrativa.

Em matéria de transmissão de dados de ADN, não existe nenhum aspecto que seja desconforme com a ordem jurídica interna, que obrigasse à revisão ou atualização da legislação nacional com o fim de se adequar ao conteúdo da Decisão.

O legislador nacional presume como vigentes as Decisões 2008/615/JAI e 2008/616/JAI, uma vez que os artigos 3º e 4º da Lei n.º 4/2014, de 07/02, relativa ao intercâmbio transfronteiriço de informações relacionadas com a prática de infrações rodoviárias com utilização de veículo, e que transpõe a Diretiva n.º 2011/82/UE, do Parlamento Europeu e do Conselho, de 25 de outubro, aludem à susceptibilidade de aplicação do seu regime na respetiva esfera material.

2.3. A recolha de amostras em condenados e a sua inserção na Base de Dados de Perfis de ADN – em Portugal

As bases de dados de perfis de ADN têm suscitado alguns problemas, tal como o recurso a análises genéticas, como meio de prova em investigação criminal e para o próprio Processo Penal.

Problemas esses que partem da definição das próprias autoridades competentes para determinar e efetuar a recolha de amostras de desconhecidos, por exemplo, no local do crime,

[45] A Decisão do Conselho 2011/472/UE reconheceu que *"Para efeitos de consulta e comparação automatizada de dados de ADN, Portugal aplicou integralmente as disposições gerais relativas à proteção de dados previstas no capítulo 6 da Decisão 2008/615/JAI, estando habilitado a receber e a transmitir dados pessoais nos termos dos artigos 3º e 4º dessa decisão, a partir da data de entrada em vigor da presente decisão."*

na recolha de amostras em suspeitos, e, até mesmo, em arguidos, e, ainda, na recolha em condenados.

Outro problema que tem vindo a ser suscitado, prende-se com a admissibilidade do tratamento e dos pressupostos de transição para as bases de dados de perfis.

No entanto, a inserção dos dados de perfis de ADN nessas bases levantam, ainda, outros problemas, como o tipo de perfis que devem ser inseridos; a possibilidade de cruzamento desses perfis; os termos da sua conservação; quanto à remoção dos perfis, caso seja necessário; também em relação ao tratamento das amostras biológicas e o problema de saber quais as entidades que deverão ser as administradoras dessas bases.

Ora, o nosso Código de Processo Penal não é totalmente omisso quanto aos problemas da genética forense mas também não contempla, de forma satisfatória, a sua previsão e regulação.

Tal situação poderá dever-se a problemas que se poderão levantar em relação a estas questões, tais como a omissão de uma previsão expressa quanto à recolha de bioamostras em suspeitos, quanto à recolha de bioamostras em terceiras pessoas, ou, até mesmo, quanto à recolha de bioamostras em massa.

O objetivo da obtenção do perfil de ADN em relação a arguidos condenados é a integração do "ficheiro de condenados", de forma a que se possam comparar com perfis de amostras-problema, tal como preveem os artigos 8º, n.º 2 e 3, 15º, n.º1, alínea e) e 20º, n.º4 da Lei n.º 5/2008.

A recolha de amostras em condenados não tem por finalidade a produção de prova no processo em que é determinada, só podendo servir para produção de prova, no caso de ser no interesse do arguido, de modo a poder afastar a sua culpabilidade, em sede de recurso de revisão, anteriormente estabelecida no próprio processo.

A recolha de amostras de condenados destina-se, apenas, a integrar o ficheiro da base de perfis de ADN, de forma a que se possa fazer um cruzamento futuro com amostras-problema ou de outro tipo.

No entanto, a doutrina nacional tem classificado a ordem de recolha de bioamostra, para obtenção de perfil de ADN do arguido condenado, ou inimputável perigoso, e sua inserção na base, como efeito substantivo da decisão condenatória e da sentença de aplicação de medida de segurança, subordinando-se, assim, ao disposto no artigo 29, n.º3 da

Constituição da República Portuguesa, daqui em diante também designada por C.R.P, aplicando-se aos factos cometidos após a entrada em vigor da Lei n.º5/2008.

Importa, agora, perceber o sentido da epigrafe do artigo 8º da Lei n.º5/2008, *"Recolha de amostras com finalidade de investigação criminal"*.

Ora vejamos, a recolha da amostra e a obtenção do respetivo perfil de ADN tem de ter um conteúdo com utilidade e funcionalidade, justificando a inserção dos n.ºs 2 e 3 no artigo 8º, a necessidade de reconhecer que, após a inserção no ficheiro a que se refere o artigo 15º, n.º1, alínea e), se mostrará razoável proceder à sua comparação e cruzamento com os perfis de ADN obtidos através de outro tipo de amostras, como as do artigo 8º, n.º 4 e 15º, n.º1, alíns. a) – perfis de *"amostras de voluntários"*; b) – perfis de *"amostras-problema"*, do artigo 7º, n.º1: cadáver ou parte de cadáver, coisa ou local com fins de identificação civil; d) – perfis de *"amostras em cadáver, em parte de cadáver, em coisa ou em local onde se proceda a buscas com finalidade de investigação criminal"*; e) – perfis de outros condenados e f) perfis de *"amostras de profissionais"* da Lei n.º5/2008.

É necessário ter em conta que a ordem de recolha de material biológico com vista à obtenção do perfil de ADN pressupõe sempre que o perfil seja inserido no ficheiro a que alude o artigo 15º, n.º1, alínea e) da Lei n.º5/2008[46], não se destinando a servir de prova no processo em que é ordenada a recolha da amostra.

Desta forma, a Lei n.º5/2008 o que prevê, é a possibilidade de haver um ficheiro que contém amostras, de pessoas condenadas em processo crime, ou seja, em relação a certos e determinados indivíduos, a quem a Lei atribui um especial interesse em elencar essa informação para fins de investigação criminal.

Face a um determinado universo de pessoas, em que, pela sua qualidade de arguido e condenado, por decisão transitada em julgado, em pena concreta igual ou superior a três anos de prisão, mesmo que substituída por uma outra medida, pode ser objeto de um importante interesse criminalístico relevante, isto porque, o perfil desses indivíduos muitas vezes tem alguma relação com a prática de certos tipos de ilícito, daí que lhes possa ser imposta ou ordenada a recolha de amostras de material biológico para determinação de perfis de ADN.

[46] "*Apesar de ser assim, o juiz terá de determinar expressamente a inserção do perfil de ADN obtido através da amostra, no ficheiro da base (art. 18º, n.º3 da Lei n.º5/2008), determinação que nos parece poder ser concomitante com a ordem de recolha, apesar de ter uma execução de "efeito aparelho"*". (Jorge dos Reis Bravo, 2014,p. 43)

Assim, desta forma, a lei parece prever a existência de uma categoria de agentes criminosos relativamente aos quais existe interesse na recolha e obtenção dos respetivos perfis de ADN.

Parece-nos, no entanto, que aqui poderá ser levantado um problema, que se prende com uma eventual violação da presunção de inocência, uma vez que, se a recolha de amostra resulta de um juízo de prognose sobre o interesse criminalístico, que em nada tem a ver com a investigação criminal do processo em que o arguido foi condenado, então a inserção do seu perfil genético numa base de dados, com eventual utilidade futura, poderá ser violador do princípio da presunção de inocência, como bem se compreenderá.

Por outro lado, também nos parece que não deixa de ser importante a inserção do perfil genético de condenados, uma vez que pode servir para a resolução de casos anteriores e não apenas para crimes futuros.

"Para se tentar caracterizar a sua natureza jurídica substantiva, podemos enunciar os pressupostos objetivos da ordem de recolha, do seguinte modo:

i. Inexistência de procedimento prévio de recolha de amostra; torna-se evidente que a ordem de recolha de amostra, nos termos do art. 8º, n.º 2 da Lei n.º5/2008 pressupõe que não tenha sido precedida pela anterior recolha de amostra, no processo, nos termos do n.º1;

ii. A exigência de decisão condenatória por crime doloso, o que admite qualquer das modalidades de dolo, excluindo a forma negligente;

iii. A medida concreta da pena aplicada ao crime tem de ser pelo menos de três anos de prisão, não podendo tratar-se de pena única, resultante de um cúmulo jurídico;

iv. Admissibilidade da substituição da pena de prisão por outra reacção penal;

v. O trânsito em julgado da decisão condenatória." (Jorge dos Reis Bravo, 2014, p.44).

Quanto ao critério dos três anos da pena de prisão, este tem sido um critério um pouco discutível.

Sobre este ponto tem entendido Paulo Pinto de Albuquerque (citado em Jorge dos Reis Bravo, 2014) que o limite deveria ser de cinco anos de pena de prisão, considerando inconstitucional a fixação da medida inferior aquele limite, pois deveria ser proporcional e

necessário, em conjugação com o conceito legal de "criminalidade grave" previsto no artigo 1º, alínea j) do Código de Processo Penal.

Esta opinião é partilhada por Marta Madalena Botelho, (citada em Jorge dos Reis Bravo, 2014) parecendo-lhe excessiva e desproporcional a fixação no limite de três anos, para habilitar o juiz a ordenar a inserção do perfil genético na base de dados.

Antes, sugere-se a possibilidade de se adotarem outros critérios, como por exemplo, fixar um limiar inferior, de três anos, para crimes que atentem contra bens jurídicos pessoais, leia-se dos crimes contra a vida, contra a integridade física, a liberdade pessoal, a liberdade de autodeterminação sexual, terrorismo, entre outros, e um limite superior para crimes que atentem contra outros bens jurídicos.

O critério que prevaleceu foi o da fixação do limiar de três anos de pena de prisão, que se deveu essencialmente a razões de praticabilidade-exequibilidade de inserção de perfis por parte do INMLCF,I.P. – Instituto Nacional de Medicina Legal -, em relação aos dados estatísticos das condenações que ocorreram em anos anteriores à publicação da Lei n.º 5/2008.

No entanto, qualquer que seja o critério, este não deve interferir nos pressupostos autorizadores a ter em conta para a obtenção de perfis de ADN como meio de prova, no âmbito da investigação criminal.

Um dos problemas que a ordem de recolha de bioamostras em condenados tem suscitado, prende-se com a questão dos condenados em pena de prisão suspensa na sua execução, o que pode ocorrer em penas de prisão entre os três e os cinco anos.

O Acórdão da Relação do Porto de 16 de outubro de 2013, relatório do Desembargador Castela Rio, pronunciou-se pela negativa, fazendo depender, ainda, a ordem de recolha do trânsito em julgado da decisão condenatória[47].

[47] Resulta do mesmo que: "*"I – A ordem de recolha de amostra biológica contendo ADN, quando "efeito substantivo" da condenação penal, só pode ser determinada em despacho do juiz posterior ao trânsito: i) da sentença ou acórdão condenatório em pena de prisão efetiva não inferior a 3 anos; ou ii) do despacho que revogar a pena de suspensão da execução da prisão e determinar o cumprimento de pena de prisão não inferior a 3 anos."*
"Neste acórdão, justifica-se a interpretação de a ordem de recolha de amostras não ser aplicável à pena de suspensão da execução da pena privativa de liberdade, por razões de ordem infra-sistemática e extra-sistemática, que não nos parecem definitivamente procedentes. Ali se refere que: "(...) apesar do lexema "...ainda que esta tenha sido substituída" se seguir ao lexema "...a recolha de amostras em condenado por crime doloso com pena concreta de prisão igual ou superior a três anos...", entende-se que aquele não abrange o caso, como o sub judicibus, de condenação do Arguido em "Decisão Final" na pena "SUSPENSÃO DA EXECUÇÃO DA PRISÃO" quantificada pelo menos em 3 anos de substituição da pena principal de prisão

Contudo, parece-nos ser de aceitar a ordem de recolha de bioamostra para obtenção de perfil genético, ainda que a pena (entre três e cinco anos) de prisão tenha sido suspensa, uma vez que o legislador optou pelo critério da medida concreta da pena aplicada, como indicador do interesse na inclusão do perfil de ADN do arguido-condenado na base de dados.

Isto porque, uma vez inserido na base de perfis de ADN, o perfil do arguido-condenado permite, não só esclarecer crimes futuros, como crimes ocorridos anteriormente à sua inserção na base, ainda que se encontre em fase de investigação.

Ainda assim, por razões decorrentes do princípio da igualdade, aceitou-se que, em determinados casos, o julgador afastasse a ordem de recolha e inserção no ficheiro, com base na garantia jurisdicional de uma ingerência significativa nos direitos fundamentais, uma vez que se entendia que a ordem de recolha e inserção no ficheiro violariam o disposto no artigo 18º da C.R.P.

No entanto, esta é uma questão que não tem conhecido unanimidade por parte da doutrina e da jurisprudência.

Vejamos alguns exemplos,

Para Inês Ferreira Leite, a ordem tem uma natureza automática: *"Não parece que a redacção da Lei dê margem para dúvidas sobre esta conclusão. Se a recolha de material biológico em arguidos será, e bem, meramente facultativa durante a pendência do processo, devendo ocorrer apenas quando haja necessidade para efeitos de produção de prova ou a pedido do arguido, já a recolha em condenado a pena de prisão igual ou superior a 3 anos é*

---

contínua e ininterrupta em Estabelecimento Prisional prevista na norma cominadora correlativa da incriminadora violada pelo agente, sob pena de incongruência na Ordem Jurídica por duas ordens de razões:

Infra-sistemática: em complemento dos arts. 26º, n.º1, alín. d); 15º, n.º1, alín. d) e 8º, n.º4 da Lei 5/2008 conforme o qual "Os perfis de ADN e os correspondentes dados pessoais são: Eliminados, quando a amostra for procedimento criminal, previsto no Código Penal, quando integrados no ficheiro..." "...contendo a informação relativa a amostras problema", recolhidas em local de crime..." "...em cadáver, em parte de cadáver, em coisa ou em local onde se proceda a buscas com finalidades de investigação criminal... de acordo com o disposto no artigo 171º do Código de Processo penal", o art. 26º, n.º2 prescreve que "...quando o termo do processo crime conduza a uma condenação por crime doloso, com trânsito em julgado, em pena igual ou superior a 3 anos de prisão, o perfil de ADN e os respectivos dados pessoais, actualizados, transitam para o ficheiro previsto na alínea e), do n.º1 do artigo 15º, de acordo com o disposto no artigo 8º" que é o "...ficheiro contendo a informação relativa a amostras, obtidas nos termos dos n.ºs 2 e 3 do artigo 8º, de pessoas condenadas em processo crime, por decisão judicial transitada em julgado" do qual não consta o lexema "...ainda que esta tenha sido substituída" pelo que o critério de selecção é a "...pena igual ou superior a 3 anos de prisão..." efectiva aplicada na "Decisão Final" seja "Acórdão" ou "Sentença" transitada ou a "...pena igual ou superior a 3 anos de prisão..." exequenda mercê do trânsito do "Despacho" que revoga ut art. 56º, n.º1, alíns. a) e b) e 2º do Código Penal de 15.9.2007 a pena "SUSPENSÃO DA EXECUÇÃO DA PRISÃO" quantificada pelo menos em 3 anos de substituição da pena principal de prisão contínua e ininterrupta em EP prevista na norma cominadora correlativa da incriminadora violada". (Jorge dos Reis Bravo, p. 46 e 47, 2014).

obrigatória. Os juízes do julgamento têm, assim, o dever legal, de emitirem despacho no sentido de que seja realizada a recolha do material biológico"[48].

Já Paulo Pinto de Albuquerque, (citado em Jorge dos Reis Bravo, 2014) também aponta para a natureza automática da ordem, no entanto, considera que essa é uma solução inconstitucional, por se aplicar a arguido condenado pela prática de crime punido com pena de prisão inferior a cinco anos ou a *"arguido em relação ao qual se não tenha estabelecido na sentença um perigo de continuação da actividade criminosa e, designadamente, quando se aplique a arguido condenado em pena de prisão suspensa".*[49]

Marta M. Botelho defende que a obtenção de um perfil genético pode ser um dado irrelevante em certos crimes puníveis com pena de prisão igual ou inferior a três anos, entendendo que *"Um despacho judicial nesse sentido nunca poderá ter como fundamento um critério de aplicação "automática" no que respeita à sua proporcionalidade como é o da medida concreta da pena aplicada. Antes haverá de encontrar respaldo na, já referida, pertinência da prova de ADN para aquele particular crime – considerando, em primeira linha, o bem jurídico violado pela conduta do agente – e na necessidade da disponibilização daquele perfil genético para servir fins de prevenção especial ou de investigação de outros crimes cometidos pelo mesmo agente".*[50]

Parece, então, que a solução mais adequada seria a de vigorar a regra da automacidade, sem que, a título excepcional, mediante requerimento do arguido e, caso, o juiz assim o entendesse, se pudesse afastar a ordem de recolha de amostra.

Isto é, caberia ao juiz analisar, caso a caso, se os pressupostos que o legislador contemplou em termos gerais e abstratos para justificar a ordem de recolha, estavam preenchidos ou se, por outro lado, pudesse ser afastada a ordem de recolha de amostra.

---

[48] *"A nova base de dados de perfis de ADN"*, Boletim Informativo da FDUL-IDPCC, Ano 1, Ed. 5, Outubro-Novembro 2009, acessível em http://www.fd.ul.pt/LinkClick.aspx?fileticket=XFmkf-Zy5pM%3D&tabid=622 (nota 16).

[49] *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem,* cit., pp. 466 e 467; "o Autor expressa o entendimento segundo o qual *"(...) a norma do art. 8.º, n.º2 da Lei n.º 5/2008 é uma norma de aplicação geral e automática, que não supõe a realização pelo juiz de julgamento de qualquer juízo sobre "o perigo de continuação criminosa", sendo até aplicável em relação a crimes em que não há, de acordo com a ciência criminológica, qualquer perigo de continuação criminosa (para uma crítica semelhante, o parecer n.º 18/2007, da Comissão Nacional de Protecção de Dados). Ela é, nessa medida, desnecessária e desproporcional, pondo em causa de forma insuportável o princípio constitucional da protecção de direitos (art.º 26.º, da CRP, conjugado com o artigo 18.º, n.º2, conjugado com o artigo 18.º, n.º2, lidos à luz da jurisprudência do acórdão do TEDH no caso S. e Mayer v. Reino Unido, de 4.12.2008)".*

[50] *Utilização das Técnicas de ADN no Âmbito Jurídico. Em Especial, os Problemas Jurídico-Penais da Criação de Uma Base de Dados de ADN para Fins de Investigação Criminal,* Almedina, Coimbra, 2013, p. 254.

Desta forma, defende-se que o recorte da ordem de obtenção de amostra, na nossa ordem judicial, é quase automática, sem dispensar a exigência constitucional da respectiva fundamentação, tal como prevê o artigo 205º, n.º 1 da C.R.P.

A existir outras possíveis alternativas, só iria gerar assimetrias de critérios, a que dificilmente a jurisprudência iria dar uma resposta satisfatória.

2.4. Fundamentos para a recusa do cumprimento da ordem de recolha de ADN – estudo de Direito Comparado

Outra questão que é necessário ter em conta é a do consentimento e da coercibilidade, ou seja, uma vez ordenada a recolha de ADN, será que o condenado a quem essa ordem foi dada, pode recusar-se injustificadamente a sujeitar-se aos procedimentos necessários?

Caso o condenado se recuse a sujeitar-se a esse procedimentos, pode à mesma, ser ordenada a recolha, utilizando, para isso, o uso da coação ou o recurso à força física para a sua recolha?

Ora bem, quanto a este aspeto existe, igualmente, uma divergência doutrinária.

Existem autores que admitem a coercibilidade através do uso da força física, mas outros há que rejeitam esta solução em absoluto e, ainda há os que os que assimilam a coercibilidade a uma cominação sancionatória, por exemplo, à prática do crime de desobediência, mas não admitem a possibilidade do recurso à força física.

Um dos autores que acolhe a tese da coercibilidade através do uso da força física é Paulo Pinto de Albuquerque, defendendo que para a realização do exame, a autoridade judiciária deve ordenar a realização do exame com a cominação da alínea b), do n.º 1, do artigo 348º do Código Penal, só aplicando o uso da força, quando a recusa persista.[51]

Isto porque, ao recusar a ordem, o examinando comete o crime de desobediência cominado e torna justificável o uso da força.

[51] *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem,* cit., p. 463.

Paulo Pinto de Albuquerque defende, por isso, que o uso da força é apenas uma medida de última instância, mas indispensável, pois ao não se admitir tal hipótese, torna-se fácil para o examinando impedir a recolha de prova em casos graves.

Para este Autor pode ser ordenada a detenção do examinando, caso se torne necessário, pelo tempo indispensável à realização de exame presidido por autoridade judiciária, em caso de falta injustificada a anterior diligência, a este propósito ver o Acórdão do Tribunal Constitucional n.º 161/2005.

Dos Autores que defendem a inadmissibilidade da utilização da força ou constrangimento físico, pode-se indicar Maria do Carmo S. Dias e, ainda, Benjamim da Silva Rodrigues que também defende a inadmissibilidade da utilização de meios de coerção com utilização da força física, uma vez que *"(...) o legislador português, com a Lei n.º 5/2008 não pretendeu "legitimar" a recolha coactiva, contra a vontade do visado, de elementos biológicos com vista a posterior perícia de ADN.(...)"*.

Mais refere Maria do Carmo S. Dias que *"(...) não havendo lei ordinária expressa que regule esta forma de "intromissão no direito à autodeterminação informacional", o julgador, "aplicando directamente os preceitos constitucionais, devidamente interpretados e concretizados", terá de concluir que é ilegítima a "recolha de impressão digital genética" sem o consentimento (esclarecido e informado) do arguido."* (Maria do Carmo S. Dias, 2005 *apud* Jorge dos Reis Bravo, 2014:54)

Parece-nos que não se possa legitimar, o recurso ao uso da força física no caso de recusa do visado pela intervenção corporal, não só tendo em conta a redação da Lei n.º5/2008, de 12 de fevereiro, na sua atual versão Lei n.º40/2013, de 25 de junho, mas também quanto à própria Constituição da República Portuguesa que não admite, de forma alguma, a tortura, o recurso a maus tratos, sendo a integridade moral e física inviolável, nos termos dos seus n.ºs 1 e 2 do artigo 25º.

A Lei n.º5/2008, de 12 de fevereiro apenas refere no seu artigo 8º, n.º1 que a recolha de amostras em processo-crime é realizado a pedido do arguido ou ordenada, oficiosamente ou a requerimento, por despacho do juiz, a partir da constituição de arguido.

Apesar de o legislador não explicitar o que se deve entender por "compelir" e muito embora a letra do artigo 172º, n.º1 do Código de Processo Penal preveja que *"se alguém pretende eximir-se ou obstar a qualquer exame devido ou a facultar coisa que deva ser*

examinada, pode ser compelido por decisão da autoridade judiciária competente", em lado nenhum se apela ao uso da força física, uma vez que tal artigo trata dos exames e não das perícias genéticas e aborda as situações em que se proceda a "exame exterior dos vestígios no corpo" sem qualquer intervenção que altere o equilíbrio bio-psicológico do indivíduo.

O que se pretende significar com o recurso à força física, quando o condenado recusa colaborar na diligência a que se pretende submetê-lo, é a utilização de meios coercivos estritamente necessários e adequados à finalidade pretendida e sempre com respeito pela dignidade pessoal e sem consequências irreversíveis, podendo integrar ofensa à integridade física justificada.

Assim, o recurso à força física deverá ser concebido como um expediente que há de salvaguardar a dignidade pessoal e o pudor do visado, o que parece ser *"...compatível com o emprego do método de esfregaço da mucosa bucal, através de zaragatoa bucal (emprego de um "cotonete"), para recolha de células do epitélio bucal. Não será este o procedimento que, em si mesmo considerado, constituirá o emprego da força, mas os meios coercivos necessários a realizá-lo, o que, efetivamente, pode variar em função do grau de resistência ou rejeição do visado"* (Jorge dos Reis Bravo, p.62, 2014).

A recolha de ADN contende com direitos fundamentais, em primeiro lugar contra a integridade corporal, consequentemente pode atingir a autonomia pessoal e a reserva da intimidade da vida privada daquele que configura o seu alvo.

De acordo com os ensinamentos de Patrícia Naré Agostinho, *"a autonomia pessoal actualiza-se nas mais variadas manifestações, mas no caso que ora nos ocupa, reduz-se à liberdade de dispor do próprio corpo e à liberdade de decisão e acção, ou seja, à liberdade de não ser alvo, através de formas mais ou menos intensas de pressão, de uma ingerência estatal. Liberdade geral de acção vista igualmente como a concretização, ou um meio de afirmação do direito ao livre desenvolvimento da personalidade (artigo 26º, n.º 1 da Constituição da República Portuguesa)."*[52]

O Tribunal Constitucional pronunciou-se sobre esta questão no seu acórdão n.º 288/98, segundo o qual *"o direito ao livre desenvolvimento da personalidade engloba "a autonomia individual e a autodeterminação e assegurando a cada um a liberdade de traçar o seu*

[52] Cfr. Patrícia Naré Agostinho, *"O regime legal da recusa de arguido condenado à recolha de amostra biológica para inserção na base de dados"*, p. 8

próprio plano de vida" o que implica o reconhecimento da liberdade geral de acção, sendo certo que, nesta sua dimensão, o "direito ao desenvolvimento da personalidade não protege, nomeadamente, apenas a liberdade de actuação, mas igualmente a liberdade de não actuar (não tutela, neste sentido, apenas a actividade, mas igualmente a passividade, com uma garantia não unidimensional de actuação, mas pluridimensional, de liberdade de comportamento, enquanto decorrente da ideia de desenvolvimento da personalidade".

O direito ao livre desenvolvimento da personalidade, segundo Gomes Canotilho e Vital Moreira, *"constitui um direito subjectivo fundamental do indivíduo, garantindo-lhe um direito à formação livre da personalidade ou liberdade de acção como sujeito autónomo dotado de autodeterminação decisória."*[53]

Este direito é protegido pelo crime de coação, previsto no artigo 154º do Código Penal, *"que configura o tipo fundamental dos crimes contra a liberdade de decisão e de acção e cujo tipo objectivo se preenche quando, através da violência ou de ameaça com mal importante, se constrange outra pessoa a adoptar um determinado comportamento, activo ou omissivo."* (Patrícia Naré Agostinho, p. 9)

Como tal, o recurso à força física para ultrapassar a resistência do visado, integra a prática de um crime de um crime de coação, nos termos do n.º1 do artigo 154º do Código Penal.[54]

O Acórdão do Tribunal Constitucional n.º 155/2007, considera que *"as normas que prevêem a possibilidade de determinação da realização coactiva de um exame, contra a vontade do arguido e sob ameaça do recurso à força física, contendem ainda com a própria liberdade geral de actuação."*

A questão coloca-se, agora, quanto à possibilidade da sua restrição cuja resposta passará pelo crivo do artigo 18.º da C.R.P., os quais estão assegurados constitucional e infra-constitucionalmente.

---

[53] Gomes Canotilho e Vital Moreira, Constituição da República Portuguesa Anotada, Vol. 1, p. 463.

[54] Mais acrescenta Patrícia Naré Agostinho que *"não será, porém, assim quando não obstante a intrusão corporal seja executada sem o consentimento do visado não tenha havido recurso à força física para a sua execução por aquele a ter tolerado. Factualidade que esteve subjacente ao Acórdão do Tribunal Constitucional n.º 155/2007 pois a recolha de saliva através de zaragatoa bucal foi efectuada contra a vontade expressa do arguido, mas sem que tivesse existido utilização de força física (embora tenha havido ameaça de recurso à força, ameaça esta que, no entanto, foi desvalorizada pelo Tribunal Constitucional)."*

Contudo, quando se verifique a necessidade do recurso à força física, por forma a obrigar uma pessoa à submissão a uma intrusão corporal, este pressupõe a definição prévia em lei geral e abstracta nos casos em que a coação pode ser utilizada.

Assim, *"a discussão ainda permanece acesa e controversa, pelo que o discurso e opção deve centrar-se na possibilidade da justificação da violência enquanto direccionada à execução de recolha de amostras em condenado, aferindo-se previamente se o fim justifica o meio, tarefa que incumbe, em primeira linha, ao legislador. Tal problemática impõe a abordagem do tópico da dignidade da pessoa humana, a qual servirá de referente para aferir quais os casos, pressupostos e limites em que o legislador pode prever o recurso legítimo à vis phisica. Valor da dignidade humana que, aliás, se sobrepõe mesmo em certos casos em que o visado no pleno exercício da sua autonomia pessoal consente na lesão."*

Relativamente à questão da integridade física, consagrada no artigo 25º da C.R.P. é o *"direito da pessoa a não ser agredido ou ofendido no seu corpo ou no seu espírito, seja por meios físicos, seja por meios morais"*[55] *decompõe-se em duas vertentes: a integridade moral e a integridade física. Na vertente da integridade física "traduz-se no direito de não sofrer ofensas corporais."*[56]

A integridade física é um bem jurídico protegido pelo artigo 143º do Código Penal, e o tipo objetivo fica preenchido quer através da ofensa no corpo, quer através de ofensas na saúde.

"A ofensa no corpo existirá quando haja diminuição da substância corporal (perda de órgãos, membros ou pele); lesões da substância corporal (nódoas negras, feridas ou inchaços); alterações físicas (corte de cabelo) ou perturbações de funções físicas (difusão de um ruído lesivo para a audição). A saúde, por seu turno, é caracterizada como "um estado de completo bem-estar físico, psíquico e social e não apenas a ausência de doença ou de enfermidade". Existirá assim ofensa na saúde quando se crie um estado de doença ou quando se mantenha ou agrave uma situação de doença já existente." (Patrícia Naré Agostinho, p. 10)

[55] Acórdão do Tribunal Constitucional n.º 128/92.

[56] Acórdão do Tribunal Constitucional n.º 616/98.

A lesão da integridade física não se afere em função da sua gravidade pois *"nada legitima uma interpretação do conteúdo constitucional do direito à integridade pessoal, concretamente na sua componente de direito à integridade física, em termos de apenas abranger a protecção contra um determinado grau de ofensas corporais."*[57]

A lesão da integridade corporal não depende da escassa intensidade ou de se tratar de um ato rotineiro ou usual.

"A raspagem da mucosa bucal configurará, nesta medida, um atentado à integridade física acto tido como usual e rotineiro"[58] e neste sentido decidiu o Acórdão do Tribunal Constitucional n.º 155/2007 onde se pode ler que *"Na verdade, a introdução no interior da boca do arguido, contra a sua vontade expressa, de um instrumento (zaragatoa bucal) destinado a recolher uma substância corporal (no caso, saliva), ainda que não lesiva ou atentatória da sua saúde, não deixa de constituir uma «intromissão para além das fronteiras delimitadas pela pele ou pelos músculos » (...), uma entrada no interior do corpo do arguido e, portanto, não pode deixar de ser compreendida como uma invasão da sua integridade física, abrangida pelo âmbito constitucionalmente protegido do artigo 25º da Constituição."*[59]

O artigo 25º, n.º 1 da Constituição da República Portuguesa afirma que a *"integridade física das pessoas é inviolável"*, não contendo qualquer cláusula de restrição expressa. Tal não significa, porém, que o direito à integridade física não possa ver reduzido o seu âmbito de proteção.

No entanto, o artigo 18º da Constituição da República Portuguesa não veda a imposição de limites; pelo contrário prevê os pressupostos em que ela deve assentar, pois nenhum direito deve ser tido como absoluto.

Nesta medida, o Tribunal Constitucional admite que a integridade física possa ser restringida quando esteja em causa a averiguação de crimes e dos seus autores, uma vez que *"sendo o Estado de Direito um Estado de justiça, o processo, tanto o criminal, como o civil, há-de reger-se sempre por regras que, respeitando a pessoa em si mesma (na sua dignidade*

[57] Acórdão do Tribunal Constitucional n.º 226/2000

[58] Cfr. Patrícia Naré Agostinho, *"O regime legal da recusa de arguido condenado à recolha de amostra biológica para inserção na base de dados"*, p. 11

ontológica), sejam adequadas ao apuramento da verdade, pois só desse modo se podem fazer triunfar os direitos e os interesses para cuja garantia o processo é necessário".

Também o Acórdão do Tribunal Constitucional n.º 155/2007 afirma que *"a Constituição autoriza, tendo em vista a prossecução das finalidades próprias do processo penal e respeitadas as demais e já referidas exigências constitucionais, a restrição dos direitos fundamentais à integridade pessoal, à liberdade geral de actuação, à reserva da vida privada ou à autodeterminação informacional."*

Assim, constitucionalmente permite-se a restrição do direito à integridade física para prossecução de certas finalidades, designadamente, as do processo penal.

Vejamos agora, qual a posição da Jurisprudência em Portugal quanto a esta questão.

Ora, a Jurisprudência portuguesa tem-se pronunciado pela inadmissibilidade do uso da força por falta de fundamento legal, como é o caso, por exemplo do Acórdão do Tribunal da Relação de Évora de 13 de dezembro de 2011, que expressamente consagra que o *"o artigo 8º n.º2 não permite que, em caso de recusa, o condenado possa ser forçado à recolha das amostras aí referidas; se essa fosse a intenção do legislador tê-lo ia dito, como o disse no n.º 1 daquele preceito."*

No entanto, o Acórdão do Tribunal da Relação do Porto de 10 de dezembro de 2008 foi decidido que *"não é inconstitucional a norma do artigo 172º, n.º 1 do Código de Processo Penal, interpretada no sentido de que é legítimo o uso da força física para obter, através de zaragatoa bucal vestígios biológicos de um arguido para fins de comparação com os encontrados nas cuecas da ofendida, se está em causa a investigação de um crime de violação, não havendo outras provas para além das declarações daquela, que sofre de considerável atraso mental"*.

No mesmo sentido, decidiu o Acórdão do Tribunal da Relação de Lisboa de 24 de agosto de 2007 no qual se concluiu que *"Opondo-se o arguido à realização de zaragatoa bucal para recolha de saliva, destinada à definição do seu perfil genético e subsequente comparação com vestígios hemáticos encontrados no local do crime, pode o JIC compeli-lo a submeter-se a tal exame, pois entre os interesses em confronto, deve prevalecer o da realização da justiça, já que para concretização forçada de tal exame a autodeterminação corporal é violada de forma pouco significativa."*

Para uma melhor percepção desta questão, torna-se necessário fazer um estudo comparado, de modo a que se perceba quais as diferenças e as semelhanças que existem quanto à recusa do cumprimento da ordem de recolha de ADN, noutros países como Reino Unido, Alemanha, Espanha e França.

Vejamos, primeiramente, quanto ao Reino Unido (Inglaterra e País de Gales).

Segundo Jorge dos Reis Bravo, o Reino Unido *"desenvolveu o seu UK NDNAD (National DNA Database), em vigor desde a implementação, em abril de 1995, da Criminal Justice and Public Order Act de 1994, que conta com mais de 4,5 milhões de perfis."* (Jorge dos Reis Bravo, 2015:27).

Em 1995 foi admitido aos condenados e, posteriormente, alargou-se aos condenados por crime que pudessem constar do registo criminal, mesmo que não sejam formalmente acusados ou absolvidos, até que em 2003 foi permitida *"(...)a recolha de amostras a pessoas detidas ou conduzidas à esquadra de polícia por infrações passíveis de figurar em registo criminal."*[60]

Em relação à Alemanha, a recolha de bioamostras é regulada pela Lei de Identificação Genética ou de Identificação por DNA, já a base de dados e a inserção de perfis genéticos são reguadas pela Lei da Polícia Criminal da União.

A ordem de recolha de amostra para inserção do perfil genético é dada pelo juiz, estando sujeitos a essa ordem aqueles que venham a ser acusados *"(...)por crimes de substancial gravidade ou contra a autodeterminação sexual, considerando a natureza do crime, a forma da sua execução ou a personalidade do acusado ou outros elementos que permitam concluir que no futuro haja risco da prática de novos crimes."*[61]

O juiz pode ordenar a recolha para fins de conservação e para comparação futura de impressões genéticas, como é o caso de pessoas insuscetíveis de serem julgadas, por inimputabilidade ou vicissitudes processuais, sendo que as mesmas são conservadas no caso de o facto cometido ter particular gravidade; o risco de reiteração esteja documentado ou (e) a medida seja necessária.

[60] Cfr. Jorge dos Reis Bravo, *"Recolha de amostra, interconexão de perfis de ADN de arguidos não condenados"*, 2015, p. 27
[61] Cfr. Jorge dos Reis Bravo, *"Recolha de amostra, interconexão de perfis de ADN de arguidos não condenados"*, 2015, p. 27

É, ainda, possível a recolha de amostras com o objetivo de se poder determinar o perfil genético de pessoas já condenadas ou sobre arguido na pendência de processo, enquanto não for absolvido, de modo a permitir a resolução de "casos futuros".

Foi com a publicação da Ley Orgánica 10/2007, de 08-10, que regula a base de dados policial sobre identificadores obtidos a partir do ADN, que a admissibilidade da produção de prova genética e a inserção de perfis genéticos ganhou uma maior expressão normativa em Espanha.

Tal como refere Jorge dos Reis Bravo, "*são inseridos os perfis obtidos a partir de ADN de amostras que, no quadro de uma investigação criminal, tenham sido encontrados ou obtidos a partir de análises de bioamostras de suspeito, detido ou acusado em casos de crimes graves e, em qualquer caso, os que atentem contra a vida, a liberdade, a integridade ou a liberdade sexual, a integridade pessoal, o património sempre que forem perpetrados com força contra as coisas, ou violência ou ameaça, assim como os casos de criminalidade organizada, entendendo-se o termo na aceção do art. 282 bis, apartado 4 da Ley de Enjuiciamiento Criminal."* (Jorge dos Reis Bravo, 2015:28)

No que respeita ao emprego da força física, alguma doutrina, e mesmo alguma jurisprudência, perante a Disposição Adicional Terceira da LO 10/200736, continuam a entender não existir suficiente e satisfatória base legal ou norma legal habilitante *"(...)para tornar lícito o emprego da força física a fim de obter amostras biológicas com vista a determinar o perfil de ADN, relativamente a suspeitos, detidos, imputados ou acusados que não prestem o seu consentimento, ainda que mediante a intercessão de uma autorização ou ordem judicial. E, sem embargo, tais Autores e jurisprudência consideram, inclusivamente, existir nos procedimentos previstos legalmente (unicamente por meio de zaragatoa bucal) uma mínima ou quase inexistente ingerência na integridade física".* (Jorge dos Reis Bravo, 2015:28)

A Disposição Adicional Terceira da LO 10/2007, acima referida, admite, na ausência de consentimento do afetado, que a recolha de amostras e fluidos do suspeito que requeiram inspeções, reconhecimentos ou intervenções corporais, possa ser efetuada, requerendo autorização judicial mediante auto fundamentado.

O critério normativo para a recolha da amostra sem o consentimento do visado *"(...) é o da suspeita da prática de «delito grave», conceito que vem especificado no art. 13.º, n.º 1 do Código Penal espanhol, especificando tratar-se das infrações sancionadas com «pena*

grave», cuja relação se acha plasmada no art. 33.º, n.º 2 do mesmo diploma." (Jorge dos Reis Bravo, 2015:29)[62]

Relativamente a França, o sistema normativo de produção de prova genética e de inserção de perfis na base de dados, encontra-se regulado pelo Code de la Santé Publique, na Loi sur la Bioéthique (Lei n.º 2004-800, de julho de 2004, alterada em 6 de agosto desse ano) e decretos regulamentares, nos artigos 706-54 a 706-56-1 do Code de Procédure Penale e na Loi sur la Sécurité Intérieure (Lei n.º 2003-239, de 18 de Março).

Neste país, a ordem de recolha de bioamostra pode ser feita por iniciativa de agente da polícia judiciária, ordem do Ministério Público ou do juiz de instrução, relativamente a pessoas contra as quais existam razões plausíveis para pensar que é suspeito de um crime ou delito, embora o perfil não seja conservado indefinidamente; é o art. 706-56 do CPP francês que fixa o elenco dos crimes relativamente aos quais podem ser inseridos em ficheiros de impressões genéticas.[63]

É possível haver recolha de bioamostra coativa, através de prévia requisição escrita do Procurador da República, relativamente a pessoa condenada por crime ou delito punido com pena desde 10 anos de prisão ou medida de internamento da mesma duração mínima.

Nos termos do Regime Jurídico dos Perfis de ADN, de 20-06-2003 e da Regulamentação conexa, de 03-12-2004, são passíveis de inserção perfis de pessoas desaparecidas, falecidas e que não estão em condições de fornecer a sua identidade, amostras de locais de crime, bem como de pessoas condenadas (art. 5.º), por crime doloso com pena privativa de liberdade superior a um ano, delito intencional contra a vida, a integridade

[62] Que prevê a pena de prisão superior a cinco anos (al. a)), a proibição de comunicar com a vítima ou outros familiares que o juiz determine por mais de cinco anos (al. i)), a privação do poder paternal (al. j))

[63] Esses crimes são: 1. Os crimes sexuais que se refere o artigo 706-47 do Código e do delito previsto no artigo 222-32 do Código Penal; 2. Crimes contra a humanidade e crimes de atentados intencionais contra a vida da pessoa, tortura e atos de barbárie, de agressão, ameaças de danos a pessoas, tráfico de drogas, de atentados às liberdades do indivíduo, o tráfico de pessoas, lenocínio, a exploração da mendicidade e colocação em perigo de menores, previstos nos artigos 221-1 a 221-5 , 222-1 a 222-18 , 222-34 a 222-40 , 224-1 a 224-8 , 225-4-1 a 225-4-4 , 225-5 a 225-10 , 225-12-1, 225-12-3 a 225 - 12-5 a 227-18 a 227-21 e 225-12-7 do Código Penal; 3. Os crimes e delitos de furto, extorsão, peculato, destruição, dano, danos e ameaças de danos à propriedade nos termos dos artigos 311-1 a 311-13 , 312-1 a 312 -9, 313-2 e 322-1 a 322-14 do Código Penal; 4. Os atentados aos interesses fundamentais da nação, atos de terrorismo, moeda falsa, e a associação criminosa e os crimes de guerra, nos termos dos artigos 410-1 a 413-12, 421-1 a 421 - 4, 442-1 a 442-5, 450-1 e 461-1 a 461-31 do Código Penal; 5. Delitos previstos nos artigos L. 2353-4 e L. 2339-1 para L. 2339-11 Código de Defesa; 6. Os crimes de receptação ou branqueamento do produto de uma infracção prevista nos números 1.º a 5.°, nos termos dos artigos 321-1 a 321-7 e 324-1 a 324-6 do Código Penal.

corporal ou contra a integridade sexual, ou em que seja determinada a execução de medida de internamento (art. 7.º, n.º 4).

Somos da opinião de que é possível conciliar diversos modelos, quer no que respeita aos critérios da inserção, da conservação, da remoção de perfis genéticos em bases de dados e de conservação das amostras biológicas (em biobancos), quer em relação aos critérios de gestão e de fiscalização das bases de dados.

Em suma, a tendência será alargar as bases de dados a uma maior categoria de pessoas com intervenção processual, alargando-se a arguidos não condenados e mesmo a suspeitos.

2.5. A ordem de recolha de amostras para obtenção de perfil genético de condenados – Aspetos Jurídico-Processuais

A primeira questão a colocar, no que diz respeito aos aspetos jurídico-processuais da ordem de recolha de amostras para obtenção de perfil genético de condenados, consiste em saber se deve ou não haver um "pedido formulado" – em sede de acusação, pelo Ministério Público ou assistente – no sentido de a mesma ser decretada, caso se verifique que os seus pressupostos objetivos do n.º2 e n.º3, do artigo 8º da Lei n.º5/2008, estão preenchidos.

A resposta parece ser negativa, pois a imposição da ordem aparentemente só é admissível após o trânsito em julgado da decisão condenatória, o que leva a questionar se a determinação da ordem de recolha será um incidente pós-sentencial e, por isso, se promova ou decida apenas depois do trânsito em julgado.

Para responder a esta questão, é necessário termos em conta em que momento processual deve ser determinada a ordem.

Ora, o regime dos recursos admite a opção de a ordem ser determinada, na decisão condenatória final, ainda que condicionada ao estabelecimento definitivo da medida concreta da pena, a fixar em sede de decisão do recurso.

Sendo que, agora a questão prende-se em saber quais os termos da recorribilidade da decisão que ordenar a recolha de amostras.

Como se viu, o carácter "quase" automático da ordem faz com que esta possa ser excecionalmente derrogada ou, até, dispensada, quando é entendida como desnecessária, por exemplo, nos casos em que o arguido foi anteriormente sujeito a recolha noutros processos, ou inadequada e desproporcional, como é o caso de doente em estado terminal e, ainda, noutras situações violadoras do artigo 18º da C.R.P.

Assim, a possibilidade de recurso é conferida nos casos em que o arguido não se conforma com a decisão do juiz em determinar a ordem, podendo recorrer de tal decisão, por a considerar desproporcional ou desnecessária.

No entanto, a situação inversa também pode ser alvo de recurso, isto é, no caso em que se contenha no regime-regra da "quase automaticidade" da ordem, mas o tribunal dispensa-a. Ora, nesta situação, pode o Ministério Público interpor recurso dessa decisão de não ordenar a recolha.

Outras hipóteses existem, como a da "recolha voluntária" de amostras por arguidos, previstas no artigo 6º, n.º3 da Lei n.º 5/2008, mas que parece excluir a hipótese da admissibilidade da recolha voluntária de amostra por arguido condenado, caso o tribunal entenda dispensar oficiosamente tal ordem, uma vez que subtrai a utilização das respectivas amostras a fins de investigação criminal, o que parece contrariar o disposto no artigo 9º, alínea d) da referida lei.

No entanto, apenas aparentemente é assim, uma vez que a advertência desta norma é a que respeita à regra do regime geral, ao contrário da hipótese em que os arguidos pretendam ser "voluntários", que são a exceção.

Assim, a recolha voluntária de amostras em processo crime, nos termos do artigo 8º, n.º6 da Lei n.º 5/2008, apenas é passível de servir para perícia nesse ou nesses processo/s, não podendo o respetivo perfil integrar qualquer base de dados, antes da sua condenação.

Por último, cabe ainda referir, que o procedimento de recolha de amostras observará o estatuído nos artigos 7º a 13º da Deliberação do Conselho Médico-Legal n.º 3191/2008, de 15 de julho de 2008.

3. A compatibilidade do uso de dados PNR com a proteção dos Direitos Fundamentais - dicotomia entre Segurança e Privacidade

Como facilmente se percebe, o tratamento de dados pessoais, ainda que com a finalidade de combate ao terrorismo e outros crimes graves, permite a identificação de possíveis passageiros de risco, o que, no plano da proteção dos Direitos Fundamentais pode tornar-se uma questão um pouco polémica e controversa.

Facilmente se pode ultrapassar a barreira ténue que existe entre, por um lado, a utilização de dados pessoais, em que pode estar em causa a privacidade dos indivíduos, e por outro o combate à criminalidade, de forma a garantir a segurança de uma nação.

Quer isto dizer, que nem sempre é fácil equilibrar as duas questões e que, por vezes, os Direitos Fundamentais podem estar comprometidos.

O Acordo entre a União Europeia e os Estados Unidos da América, relativo à proteção de dados pessoais, entrou em vigor em 2012 e, desde logo, se apresentou como um exemplo onde a dicotomia "Segurança e Privacidade" conheceu uma maior fragilidade, ao não respeitar o mandato do Conselho à Comissão, que refletia os parâmetros de proteção de dados por ela definidos quanto à transferência de dados PNR para países terceiros.

No entanto, este acordo inclui no seu articulado um conjunto de disposições juridicamente vinculativas que definem o âmbito de aplicação, a finalidade da utilização dos dados PNR, a segurança dos próprios dados, o modo de transmissão, os direitos dos titulares, como por exemplo, o direito de informação, a possibilidade de acesso e retificação dos dados ou a proibição de decisões tomadas exclusivamente com base num tratamento automatizado de dados PNR, com o objetivo de analisar os comportamentos da pessoa em questão.

Muito embora assim seja, no que respeita ao regime jurídico de proteção dos titulares dos dados PNR, a União Europeia pecou ao aceitar disposições demasiado vagas e de compatibilidade considerada duvidosa em relação aos *"standards"* europeus em matéria de proteção de dados, como decorre da Diretiva 95/46/CE.

Ora a Diretiva 95/46/CE prevê princípios com vista à proteção de dados, como é o caso do princípio da limitação da finalidade, e o da proporcionalidade, que prevêm que os dados devem ser adequados em relação à finalidade para que são recolhidos e tratados.

Mais prevê a Diretiva, o princípio da minimização de dados, querendo isto dizer que o processamento desses dados deve cingir-se apenas ao estritamente necessário. Prevê ainda, um conjunto de direitos aos titulares dos dados, como é o caso do direito à informação, o

direito a aceder aos seus dados, corrigi-los, eliminá-los ou, até mesmo, a impedir que sejam comunicados a terceiros sem o seu consentimento.

Começando por analisar o princípio da limitação da finalidade, previsto no artigo 6º, n.º1, alínea b) da Diretiva 95/46/CE, cabe referir que os dados coletados são utilizados com objectivos específicos e legítimos, que justificam a sua coleta, o que faz com que este princípio impeça a recolha de dados para objetivos que não sejam especificados ou que sejam indeterminados, proibindo, assim, o tratamento de dados com uma finalidade diversa daquela para a qual foram recolhidos.

Ora, se por um lado o n.º1 do artigo 4º do acordo PNR, prevê que os EUA apenas podem recolher, utilizar e tratar os dados PNR para fins de prevenção, detecção, investigação e repressão de infrações terroristas ou de crimes transnacionais puníveis com pena de prisão igual ou superior a três anos, o n.º2 do mesmo artigo, parece ser contraditório ao permitir o tratamento casuístico de dados PNR, sempre que se mostre necessário, em que haja uma ameaça grave, ou se for ordenado por um tribunal.

Se por um lado, parece estar garantida a proteção dos dados PNR, através do n.º1 do artigo 4º, por outro, parece que se desprotege tais dados ao serem utilizados conceitos indeterminados, como é o caso de "ameaça grave" ou a utilização desses dados caso se verifique uma ordem de um tribunal em qualquer caso, mesmo que não tenha a ver com crimes de terrorismo ou crimes transnacionais puníveis com pena de prisão superior a três anos.

O n.º3 do mesmo artigo parece desproteger, igualmente, tais dados ao permitir que o Departamento de Segurança Interna os utilize e trate *"para identificar pessoas que são submetidas a um interrogatório mais aprofundado aquando da sua chegada ou saída dos Estados Unidos ou que devam ser sujeitas a um exame suplementar"*, uma vez que permite a utilização desses dados com uma finalidade indeterminada, ou seja, sem uma finalidade concreta, o que viola claramente o princípio da limitação da finalidade.

Outra questão a apontar, prende-se com o período de conservação dos dados PNR, previsto no artigo 8º do acordo PNR, em que durante um período de cinco anos, os dados são mantidos numa base de dados ativa, sendo que, seis meses após a sua recolha, são ocultados e tornados anónimos.

Depois dos cinco anos, esses dados são transferidos para uma base de dados passiva, onde são conservados durante dez anos e apenas podem ser consultados de forma mais restrita.

Ora, esta disposição aumentou o período de conservação dos dados PNR de um máximo de oito anos, no primeiro acordo de 2004, após o qual os dados eram destruídos, passando para um período de 15 anos, após o qual os dados não são destruídos, mas são transformados em dados anónimos.

Tal situação mostra-se violadora do princípio da limitação da finalidade, uma vez que, os dados devem ser conservados apenas durante o período que forem necessários para a prossecução dos fins para os quais foram recolhidos e tratados, pelo que não podem ser conservados por um período indeterminado.

Logo, o período de 15 anos previsto no artigo 8º do acordo PNR revela-se desproporcionado, uma vez que, se a recolha dos dados PNR tem uma função preventiva, servindo para detetar, na massa dos passageiros desconhecidos, os que poderão ser considerados uma ameaça pelo seu comportamento, e cuja finalidade esgota-se no momento do controlo de segunda linha e da sua detecção, após o que, esses dados apenas poderão ter alguma utilidade no âmbito das investigações criminais, em relação a determinadas pessoas, podendo, neste caso, transferir-se para o processo.

Por isso é que conservar os dados PNR de milhões de cidadãos, durante 15 anos, revela-se excessivo, uma vez que assim acabam por ser recolhidos com um intuito meramente comercial de gestão de um contrato de transporte, apenas porque hipoteticamente a base de dados possa conter os de um cidadão que venha a ser, por hipótese, objeto de investigação criminal.

Por último, este acordo confere aos titulares dos dados PNR o acesso a um recurso jurisdicional efetivo caso os seus dados sejam utilizados de uma forma abusiva, independentemente da sua nacionalidade ou da sua residência, de acordo com a legislação dos Estados Unidos, nos termos do seu artigo 13º.

Tal disposição, à partida, parece garantir aos cidadãos europeus, sem discriminação, o recurso judicial nos Estados Unidos.

No entanto, não é bem isso que acontece, visto que tal não passou de uma operação que ajudou a "vender" o acordo ao Parlamento Europeu, uma vez que, para haver acordo, era condição necessária o acesso de qualquer cidadão europeu ao recurso judicial nos Estados Unidos, por se considerar um direito fundamental inerente ao conceito de Estado de Direito e consagrado no artigo 47º da Carta dos Direitos Fundamentais da União Europeia.

Na realidade, o artigo 13º do acordo confere a possibilidade de recurso judicial mas nos termos da legislação americana, o que de acordo com a mesma, mais concretamente com

o *Privacy Act*, as vias de recurso aí previstas apenas se aplicam aos cidadãos americanos ou aos estrangeiros com residência permanente.

Ou seja, só os cidadãos europeus com autorização de residência permanente é que podem beneficiar das garantias do *Privacy Act*, nomeadamente o recurso para os tribunais.

Prova disso, é ainda o artigo 21º do acordo, ao referir que *"não cria nem confere, ao abrigo da legislação dos Estados Unidos, qualquer direito ou benefício a favor de pessoas ou entidades, privadas ou públicas"*.

Para os Estados Unidos o acordo PNR não passa de um acordo administrativo e, por isso, insusceptível de alterar a legislação interna dos Estados Unidos, logo insusceptível também de garantir a todos os cidadãos europeus, sem discriminação, o acesso aos tribunais americanos em caso de violação das normas de proteção dos dados pessoais.

Como facilmente se percebe, este acordo em nada é favorável aos cidadãos da União Europeia, acabando até por desprotegê-los quanto à defesa do seu direito fundamental à proteção dos dados pessoais, consagrado no artigo 8º da Carta dos Direitos Fundamentais da União.

No entanto, o Tribunal Europeu dos Direitos do Homem tem vindo a sublinhar que, a recolha e o armazenamento sistemático das informações pessoais, se enquadram no âmbito do direito a uma vida privada que está protegido pelo artigo 8.º da Convenção Europeia dos Direitos do Homem.

Ao abordar a questão da compatibilidade do uso de dados PNR com a proteção dos Direitos Fundamentais, rapidamente se pensa nas garantias processuais que são necessárias existir numa sociedade democrática.

Assim sendo, cabe agora perceber que garantias são essas e como devem atuar perante esta dicotomia entre a Segurança e a Privacidade.

Quando a questão respeita em perceber se qualquer interferência com o direito a uma vida privada satisfaz o critério "necessário numa sociedade democrática"; o Tribunal Europeu dos Direitos do Homem concede uma margem mais ampla de apreciação às autoridades nacionais quando em causa está a segurança nacional.

No entanto, mesmo quando os governos nacionais invocam como objectivos a segurança interna, o Tribunal Europeu dos Direitos do Homem exige que haja uma ponderação fundamentada dos diferentes interesses em causa.

Para além disso, o Tribunal Europeu dos Direitos do Homem exige, ainda, a disponibilidade de garantias processuais, de modo a que os tribunais ou as autoridades independentes possam avaliar a necessidade e a proporcionalidade das medidas de segurança.

O sistema europeu de dados PNR proposto, diz respeito ao processamento sistemático de dados relativos a um elevado grupo de pessoas.

Estes passageiros, sendo eles cidadãos da União Europeia ou de países terceiros, em geral, não são suspeitos de qualquer tipo de crime ou de medidas de segurança, nem são objecto e uma qualquer investigação criminal.

A única razão pela qual os seus dado são fornecidos ao governo de países terceiros, ou a autoridades policiais e de imigração dos Estados-Membros, é o simples facto de terem reservado um voo.

O Tribunal Europeu dos Direitos do Homem deixou claro, no acórdão *Amann v. Switzerland*, no qual aplicou o artigo 8.º da Convenção Europeia dos Direitos do Homem, que as informações recolhidas e armazenadas, nem sempre são posteriormente utilizadas na prática e, por isso, nesse caso é irrelevante para a aplicação do artigo 8.º acima referido.

Parece-nos que o Tribunal Europeu dos Direitos do Homem tem desenvolvido critérios para o necessário equilíbrio de poderes entre as autoridades de recolha de dados, por um lado e a proteção dos interesses do indivíduo por outro.

Estes critérios prendem-se, nomeadamente, com limites ao exercício dos poderes de armazenar e utilizar as informações; o dever de informar a pessoa em causa com antecedência, quanto ao armazenamento das suas informações; definir, claramente, o tipo de informações que podem ser gravadas e, ainda, definir as categorias de pessoas contra as quais podem ser tomadas medidas de vigilância e os fins para os quais essas informações podem ser utilizadas.

Em relação a este último critério, o Tribunal Europeu dos Direitos do Homem avaliou, no caso de *Segerstedt – wiberg v. Suécia*, os poderes do Serviço de Segurança Sueco para armazenar informações nos registos da polícia secreta, quando em causa estão razões consideradas especiais, conforme previsto na Lei de dados da polícia sueca.

Neste caso, o Tribunal Europeu dos Direitos do Homem concluiu que o grau de discricionariedade conferido às autoridades competentes, com o modo como procederam, foi o mais indicado de modo a dar ao indivíduo a proteção adequada[64].

Este critério está, por isso, intimamente relacionado com o princípio da proteção de dados da limitação da finalidade.

Por forma a garantir um justo equilíbrio entre os direitos dos indivíduos e os objetivos das autoridades públicas, é necessário que estes objetivos sejam sempre definidos claramente.

[64] *Segerstedt-Wiberg and Others v. Sweden,* 6 June 2006, no. 62332/00, § 79.

O nosso entendimento vai de encontro ao da autora Evelien Brouwer, ao considerar que o legislador, tanto o nacional como o da União Europeia, deve sempre fornecer as informações necessárias, relativas à eficiência das novas medidas relacionadas com o intercâmbio de dados pessoais e que, potencialmente, possam afetar os direitos relativos à vida privada dos indivíduos[65].

Por isso é que é necessário, ao avaliar o uso de novas bases de dados ou troca de dados, ter em conta as medidas existentes nesse domínio, e à luz do artigo 8.º da Convenção Europeia dos Direitos do Homem.

Assim, a inclusão do direito à proteção de dados na Carta dos Direitos Fundamentais da União Europeia tem sido, em nosso entender, um passo importante para aquilo que é o direito à proteção de dados, conferindo-lhe expressão, relevância e significado no mundo jurídico.

"Tendo em conta os atuais desenvolvimentos quanto à utilização de dados de passageiros, cabe fazer uma análise precisa e cuidadosa quanto aos princípios de proteção desses dados, e são eles:

1. Princípio do limite da finalidade;
2. Proibição de tomadas de decisão automatizadas;
3. Qualidade dos dados;
4. Prazos;
5. Direitos de acesso;
6. Supervisão de autoridades de supervisão nacionais e europeias de proteção de dados;
7. Nível adequado de proteção de dados em países terceiros;
8. Segurança dos dados"[66].

[65] Tradução livre da autora, *"This means that when considering new measures dealing with the use or Exchange of personal data and (potentially) affecting privacy rights of individuals, the (nacional and EU) legislator must always provide convincing information on the added value or efficiency of these measures. One cannot consider the proportionality of a proposal without establishing its efficiency first."* (Evelien Brouwer, p. 17, 2009).

[66] Tradução livre da autora, *"Considering the current developments with regard to the use of passenger data, the following central data protection principles need careful examination:*

- *purpose limitation principle*
- *prohibition of automated decision-making*
- *quality of data*
- *time limits*
- *individual access and correction rights*
- *supervision of national and European data protection supervisors*
- *adequate level of data protection in third countries*
- *security of data"* (Evelien Brouwer, 2009, p.19)

Quanto aos limites da finalidade, o risco de ser prejudicado pela inclusão de critérios vagos e abertos nas atuais propostas merece uma especial atenção.

De acordo com o artigo 6.º, n.º1 da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoais singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, é possível verificar pela leitura das suas alíneas, que os dados pessoais devem ser recolhidos para finalidades concretas, explícitas e legítimas, não devendo ser, posteriormente tratados de forma incompatível com essas mesmas finalidades.

Este princípio proíbe a recolha de dados pessoais para fins que sejam desconhecidos ou que não sejam de alguma forma especificados.

Proíbe, ainda, a utilização ou divulgação de informações pessoais para fins que não compreendem a sua finalidade específica para a qual foram recolhidos esses dados.

E, por último, este princípio prevê que os dados não devem ser mantidos por mais tempo do que aquele que for necessário para a finalidade concreta.

Como facilmente se compreende, a limitação da finalidade está relacionada com o princípio da especificação da finalidade, o que faz com que os detentores das informações devam especificar e tornar claras as finalidades do tratamento dos dados a que se propõem.

Ambos os princípios pretendem transmitir a ideia de que o processamento de dados deve ser previsível para a pessoa em causa e não deve ir além das expetativas razoáveis dessa pessoa.

A jurisprudência do Tribunal Europeu dos Direitos do Homem, relativa à proteção do direito à vida privada, vai no sentido de relevar a importância da "previsibilidade" quanto ao tratamento de dados pessoais por parte das autoridades governamentais[67].

A utilização de dados PNR é, de acordo com a proposta da Decisão-Quadro, limitada aos Estados Unidos e serve no auxílio ao combate às infrações terroristas ou à criminalidade organizada.

[67] Tradução livre da autora, *"(...) in its jurisprudence on the protection of the right to private life, the ECtHR explicitly emphasised the importance of "foreseeability" with regard to the processing of personal data by governamental authorities."* (Evelien Brouwer, 2009, p.20)

No entanto, o texto da proposta permite a utilização dos dados PNR para a prevenção, investigação, detecção e repressão das infrações terroristas ou da criminalidade organizada, estendendo-se a atividades das autoridades nacionais, durante as quais podem os dados PNR serem recolhidos ou utilizados.

A proposta da Decisão-Quadro, prevê a possibilidade de transmitir os dados PNR e podendo os mesmo serem analisados por parte das autoridades policiais de países terceiros para a prevenção, detecção e investigação de repressão de atos terroristas ou de outro tipo de criminalidade.

Já no que à interligação com outras bases de dados respeita, incluindo o SIS e a possibilidade das autoridades policiais de países terceiros acederem aos dados dos passageiros, é necessário conhecer se são cumpridas as normas do princípio da limitação da finalidade.

No que respeita à retenção de dados, a proposta da Comissão incluía a possibilidade de conservar os dados por treze anos, durante dois períodos, sendo o primeiro de cinco anos, após a sua transferência para o *PIU – Passenger Information Units* -, do primeiro Estado-Membro para ou de onde o voo internacional chega ou sai e, no termo desse período, um segundo período de oito anos.

Durante este segundo período é possível aceder aos dados, processá-los e utilizá-los com o consentimento da autoridade competente *"apenas em circunstâncias excepcionais, em resposta a uma ameaça ou um risco real e específico relacionado com a prevenção e luta contra as infrações terroristas e a criminalidade grave"*[68].

A proposta da Decisão-Quadro de 1 de junho de 2009 propôs um período de retenção de dados de três anos, após a transferência dos dados PNR para a *PIU* do primeiro Estado-Membro, a partir do qual o voo internacional chega ou parte e um período de sete anos para arquivar esses dados.

No que diz respeito ao período de retenção de dados, que deve ser observado pelos países terceiros que recebem e analisam os dados PNR, este proposta da Decisão-Quadro não incluía quaisquer regras vinculativas.

[68] Tradução livre da autora, *"only in exceptional circumstances in response to a specific and actual threat or risk related to the prevention or combat of terrorist offences and serious crime."* (Evelien Brouwer, 2009, p.20)

Somos da opinião de que, atualmente, o princípio da proibição da tomada de decisões automatizadas tem ganho uma maior importância, sendo que, relativamente a este princípio o artigo 15.º da Diretiva 95/46/CE prevê que toda pessoa tem *"(...)o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, como por exemplo a sua capacidade profissional, o seu crédito, confiança de que é merecedora, comportamento"*.

Tanto o considerando (20), como o artigo 3.º da Proposta da Comissão de Novembro de 2007, preveem que nenhuma ação de execução deve ser tomada pelo PIU, nem pelas autoridades competentes dos Estados-Membros, com base exclusivamente no tratamento automático de dados PNR[69].

A nova redação de acordo previa que *"(...) the PIUs shall not take any decision which produces an adverse legal effect concerning a person or significantly affects him based solely on the automated processing of a passenger´s PNR data."*[70]

Foi incluída uma disposição equivalente no que diz respeito às atividades da competência das autoridades, no artigo 4.º da referida Proposta. No entanto, é necessário ter em conta que é difícil avaliar os motivos pelos quais um indivíduo poderá ser submetido a um controlo mais específico ou até a sua entrada no país de destino ser recusada, quando não estejam em causa dados PNR.

Por esta razão, é que a proibição da tomada de decisões automatizadas está intimamente relacionada com o direito que um indivíduo tem de ser informado das razões que levaram à tomada daquelas medidas.

Somos da opinião de que a implementação dos dados PNR na Europa é, por isso, uma ferramenta importante, por duas razões:

Em primeiro lugar, porque os dados PNR transferidos pelas transportadoras aéreas para as autoridades nacionais dos Estados-Membros da União Europeia, serão avaliados com base nos perfis de corrente, resultando na possível identificação de passageiros de alto risco.

[69] Cfr. Council doc. 7656/3/2008, Proposal for a Council Framework Decision on the use of Passenger Name Record for law enforcement purposes, 19 June 2008.
[70] Cfr. Council doc. 7656/3/2008, Proposal for a Council Framework Decision on the use of Passenger Name Record for law enforcement purposes, 19 June 2008.

Em segundo lugar, os dados PNR transferidos, serão utilizados pelo *PIU* e pelas autoridades nacionais dos Estados que os recebem, para a criação de novos perfis, com vista a serem utilizados para investigações futuras ou até em curso.

Apesar de tudo, devem ser sempre utilizadas ferramentas para proteger o indivíduo da discriminação, tal como acontece na Convenção Internacional Sobre a Eliminação de Todas as Formas de Discriminação Racial e no artigo 14.º da Convenção Europeia dos Direitos do Homem.

Não nos parece, de todo, difícil a criação de uma base de dados PNR na União Europeia, uma vez que esta tem todas as condições para proteger os dados que são recolhidos pelas companhias aéreas.

Senão vejamos o artigo 14.º da Convenção Europeia dos Direitos do Homem que obriga os Estados-Membros a garantirem o gozo dos direitos e liberdades protegidos na referida Convenção, sem discriminação em razão do sexo, raça, língua, religião, opinião política, origem nacional ou social, de pertença a uma minoria nacional, em razão da riqueza ou por qualquer outra razão.

Para além do artigo 14.º da Convenção Europeia dos Direitos do Homem, o Protocolo n.º12 à Convenção Europeia dos Direitos do Homem, prevê o *"gozo de qualquer direito estabelecido por lei"*, sem discriminação pelos motivos acima identificados.

Além do mais, a União Europeia está munida de outros tantos instrumentos que acautelam de alguma forma, a proibição da discriminação, como é o caso da Convenção das Nações Unidas sobre a eliminação de todas as formas de discriminação racial.

Esta Convenção prevê a eliminação de todas as formas de discriminação racial, tendo a mesma sido ratificada por todos os Estados-Membros da União Europeia, pelo que as suas disposições têm de ser chamadas à colação quando esteja em causa alguma forma de discriminação, com a utilização dos dados PNR.

O artigo 1.º da Convenção começa por definir a descriminação racial como sendo qualquer distinção, exclusão, restrição ou preferência baseada em raça, cor, descendência ou origem nacional ou étnica que tenha por objetivo ou efeito, anular ou restringir, o reconhecimento, o gozo ou o exercício, dos direitos humanos e das liberdades fundamentais, quer no domínio político, económico, social, cultural, ou em qualquer outro.

O artigo 2.º da Convenção obriga a que não se pratique nenhum ato de discriminação racial contra pessoas, grupos de pessoas ou instituições e garante que todas as autoridades públicas e instituições públicas, nacionais e locais, devam agir em conformidade com essa obrigação.

Além disso, o artigo 2.º, n.º1, alínea c), prevê que o Estado deve tomar as medidas que considerar eficazes para rever as políticas governamentais nacionais e locais, alterando, revogando ou anulando leis e regulamentos que possam ter o efeito de criar ou perpetuar, de alguma forma, a discriminação racial.

Exemplo disso é o acórdão do Tribunal Constitucional Alemão sobre a prática de "arrastão" de dados por parte da polícia alemã.

Este acórdão traduz-se num exemplo importante para o legislador da União Europeia ter em conta, ao desenvolver cada vez mais o sistema PNR na União Europeia. Isto porque, perante a queixa de um estudante marroquino, o Tribunal considerou, no julgamento de 2006, a recolha de dados de perfis, por parte da polícia alemã, naquele caso, ilegal, por considerar que se traduziu numa violação desproporcionada do direito à privacidade, constitucionalmente consagrado.

O Tribunal Alemão pronunciou-se quanto ao alargamento do âmbito da recolha de informações; à utilização de bases de dados diferentes; ao aumento do risco para a pessoa interessada em tornar-se alvo de investigação criminal e, ainda, referiu a possibilidade de estigmatização de um grupo de pessoas.

Também o Tribunal Constitucional se pronunciou quanto à possibilidade de estigmatizar um grupo de pessoas na vida pública, especialmente quando se tratam de pessoas de alguns países específicos que também são muçulmanos.

Neste Acórdão, o Tribunal Constitucional Alemão enfatizou quais os grupos com maior risco de serem afetados por estas medidas dos dados de perfis.

Exemplo disso é a intensidade dos efeitos que a recolha de dados de perfis tem tido, desde 11 de setembro de 2001, e que se destinam a pessoas de certas origens e crenças muçulmanas, acabando por aumentar o risco de propagação de preconceitos e estigmatizar estes grupos em relação ao resto da população.

O Tribunal Constitucional acrescentou, ainda, que tal medida apenas se justificaria caso houvesse um perigo concreto de um ataque terrorista, que causasse um dano elevado, baseando-se em factos concretos.

Desta forma, o Tribunal considerou que a ameaça geral, que existe desde 11 de setembro de 2001, ou até uma situação tensa com base em questões de política externa não são razões suficientes para justificar a prática da recolha de dados de perfis.

Mais recentemente o Tribunal Europeu dos Direitos do Homem também advertiu para o risco do efeito estigmatizante do armazenamento sistemático e de longo prazo das impressões digitais e amostras de ADN de indivíduos, incluindo menores, que não foram condenados, mas eram suspeitos de prática de crimes.

Por isso, no Acórdão *S. & Marper v. Reino Unido*, o Tribunal Europeu dos Direitos do Homem considerou que a lei do Reino Unido violou o artigo 8.º da Convenção Europeia dos Direitos do Homem, uma vez que esses dados foram armazenados por períodos indefinidos e, considerou ainda, a medida desproporcional por estarem em causa pessoas não condenadas.[71]

4. PNR e dados Passenger Advanced Information (API): Distinção

Atualmente tem-se assistido, cada vez mais, a uma intensificação da segurança através de modernas ferramentas, como por exemplo os passaportes legíveis através de máquinas e com os sistemas de informações de passageiros, melhorando a segurança da aviação civil internacional.

Em abril de 2004 o Conselho adotou a Diretiva 2004/82/CE relativa à obrigação da comunicação dos dados dos passageiros pelas transportadoras aéreas às autoridades de controlo de fronteiras dos Estados-Membros da União Europeia.

Recentemente, a utilização de API – *advanced passenger information* (informações antecipadas sobre passageiros) - tem ganho uma expressão cada vez maior, como medida de segurança, sendo que, são cada vez mais os Estados que têm considerado necessária a sua utilização no combate ao terrorismo e para proteger as suas fronteiras.

Ora, *"(...) os dados PNR são as informações fornecidas pelos passageiros quando fazem uma reserva de um bilhete de avião, sendo recolhidos pelas transportadoras para*

[71] *S. and Marper v. United Kingdom,* 4 December 2008, appl. no. 30562/04 e 30566/04, ver parag. 122

gerirem as reservas e o embarque. Incluem informações muito diversas como datas e itinerário da viagem, contactos, agente de viagem onde o bilhete foi comprado, número do lugar no avião ou os dados do pagamento. Distinguem-se dos dados API (Advanced Passenger Information) contidos no passaporte, como nome, residência, local de nascimento e nacionalidade de uma pessoa e que são disponibilizados às autoridades europeias competentes em matéria de controlo de fronteiras e combate à imigração ilegal, nos termos da Diretiva API."[72] (Constança Urbano de Sousa, 2014, p.54)

Enquanto que a análise e conservação sistemática dos dados PNR constituem um meio de prevenção, detecção e investigação do terrorismo e da criminalidade grave transnacional, nomeadamente os de tráfico de droga e os de tráfico de seres humanos, os dados API constituem um meio de identificação de passageiros e de controlo de fronteiras.

Os dados PNR *"quando são utilizados em tempo real e de forma pró-ativa são um instrumento de "intelligence policial", que permite prevenir e detetar crimes, mediante uma avaliação do risco dos passageiros, identificando "pessoas desconhecidas", até ao momento insuspeitas, mas que podem, pelo seu padrão de comportamento, estar a praticar um crime, justificando assim a sua submissão a um controlo de segunda linha. Para esta finalidade, os dados PNR são comparados com indicadores de risco, bem como com outras bases de dados. Trata-se de uma avaliação de risco baseada no profiling."* (Constança Urbano de Sousa, 2014, p. 54)

Ora, tendo os dados PNR uma função preventiva, estes servem para determinar perfis de risco que permitem às autoridades decidir quais os passageiros "desconhecidos" que estão sujeitos a controlos mais rigorosos permitindo, desta forma, detetar correios de droga, por exemplo.

"Tal só é possível com prospecção de dados (data mining), ou seja, a exploração de grandes quantidades de dados à procura de padrões, bem como com o seu cruzamento com outras bases de dados." (Constança Urbano de Sousa, 2014, p.54)

No entanto, as funções do PNR não se ficam por aqui, podendo ter uma outra finalidade no campo da investigação criminal, como por exemplo, permitir a identificação dos percursos de pessoas que estejam sob investigação.

Relativamente à API - informações antecipadas sobre passageiros – API - *advanced passenger information*, esta consiste num sistema unilateral, pelo qual são recolhidos dados adicionais e, por sua vez, transmitidos às agências de controlo de fronteiras, num momento

[72] Diretiva 2004/82/CE, de 29.08.2004

anterior à chegada do voo, sendo esses elementos disponibilizados na linha principal no porto de entrada.

"A diferença mais significativa entre API e PNR é que a informação que pode ser extraída dos dados PNR é aquela que o passageiro fornece no sistema de reservas"[73].

De acordo com o artigo 3.º da Diretiva 2004/82/CE, os Estados-Membros da União Europeia podem obrigar as transportadoras aéreas a transmitirem as informações sobre os passageiros por elas transportados, até ao final do *"check-in",* a pedido das autoridades responsáveis pelo controlo das fronteiras.

Caso as transportadoras aéreas incumpram a obrigação a que estão sujeitas, o artigo 4.º da Diretiva 2004/82/CE, permite que os Estados-Membros da União Europeia tomem as medidas necessárias para impor sanções no valor máximo de € 5.000 e um mínimo de € 3.000.

Antes da adoção final da Diretiva, foram incluídas duas importantes extensões no projeto de texto, devido à pressão por parte do Reino Unido.

A primeira alteração a registar, consta do artigo 6.º da Diretiva, no qual foi introduzida uma exceção à regra geral de que os dados fornecidos às autoridades devem ser apagados no prazo de vinte e quatro horas a contar desde a sua transmissão, assim, essa exceção permite que os dados possam ser armazenados por um período mais alargado, caso sejam necessários *"(...) para o exercício das funções legais das autoridades responsáveis pelo controlo de passageiros nas fronteiras externas, segundo o seu direito interno e sob reserva das disposições sobre protecção de dados da Directiva 95/46/CE."*[74]

Em segundo lugar, o artigo 6.º prevê que os Estados-Membros também podem usar os dados dos passageiros para efeitos de aplicação da lei.

Ora, esta última alteração à proposta original amplia o objetivo da Diretiva de uma forma significativa, colocando-se a questão de saber se este objetivo da Diretiva ainda se pode sustentar na sua atual base jurídica: artigo 62 (2) (a) e 63 (3) (b) do Tratado da Comunidade Europeia.

Além disso, o artigo 6.º e a referência explícita que o considerando (12) da presente Diretiva faz ao princípio da limitação da finalidade, presente no artigo 6.º (1) (b) da Diretiva 95/46/CE parece conter uma dupla contradição.

---

[73] Tradução livre da autora, *"The most importante difference between API and PNR is that the information that can be extracted from PNR data mainly depends on the information that the passenger submits him/herself to the reservation system."* (Evelien Brouwer, 2009, p.3)

[74] Diretiva 2004/82/CE do Conselho de 29 de Abril de 2004, relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras.

Isto porque, ou o único objetivo da Diretiva 2004/82/CE é combater a imigração ilegal e, aí, ultrapassa os fins da aplicação da lei, infringindo o princípio da limitação da finalidade da Diretiva 95/46/CE, ou então a Diretiva API não se enquadra no âmbito de aplicação do artigo 3.º da Diretiva 95/46/CE."[75]

"O *Advanced Passenger Information (API)* envolve a captura de dados biográficos dos passageiros, bem como outros detalhes do voo, por parte da transportadora aérea antes da partida, e que posteriormente os transmitirá, através de meios electrónicos, para as agências de controlo de fronteiras do país de destino.

Os dados API podem ser uma ferramenta bastante importante na tomada de certas decisões por parte das agências de controlo das fronteiras, pois, após receberam as informações sobre os passageiros, estas agências fazem o rastreio dos mesmos, podendo identificar passageiros de alto risco aos quais será necessário fazer um controlo mais detalhado à chegada."[76]

Iremos agora passar a uma breve análise das vantagens da utilização dos dados API para os passageiros, para as transportadoras aéreas, para as agências de controlo de fronteiras e para as autoridades aeroportuárias.

Começando pelas vantagens para os passageiros, os dados API, ao serem transmitidos antecipadamente, torna-se extremamente benéfico para os passageiros, uma vez que permite uma economia do tempo despendido pelo passageiro, quando se submete às formalidades normais no destino de chegada.

Para as companhias aéreas, o facto de os dados serem capturados no momento em que a reserva é feita ou durante o check-in, em certo casos, pode aumentar a segurança da transportadora, ajudando a garantir que todos os passageiros viajam com documentos oficiais válidos, exigidos para a admissão no país de origem.

---

[75] Tradução livre da autora, *"This latter amendment to the original proposal extends the purpose of Directive significantly, raising the question as to whether this goal of the Directive could still be based on its current lagal basis: Articles 62 (2) (a) and 63 (3) (b) EC Treaty. Furthermore, Article 6 and the explicit reference in preamble 12 of this Directive to the purpose limitation principle of Article 6 (1) (b) of the 95/46/EC Directive seem to include a (twofold) contraiction. Either the sole purpose of this Directive 2004/82 is to combat irregular immigration, and then further use for law enforcement purposes will infringe the rule of purpose limitation in Directive 95/46, or the API Directive clearly implies the use for law enforcement purposes, but then this use will fall outside the scope of Directive 95/46, as is provided in Article 3 of this Directive."* (Evelien Brouwer, 2009, p.3)

[76] Tradução livre da autora, *"Advanced Passenger Information (API) envolves the capture of a passenger´s biographic data and other flight details by the carrier prior to departure and the transmission of the details by electronic means to the Border Control Agencies in the destination country. API can also act as a decision making tool that Border Control Agencies can employ before a passenger is permitted to board an aircraft. Once passengers are cleared for boarding, details are then sent to the Border Control Agencies for screening against their enforcement database(s) and can identify high risk passengers requiring for exemple more intensive questioning upon arrival."* (Guidelines on Advance Passenger Information, 2010)

Tal situação permite reduzir a possibilidade de a transportadora aérea transportar passageiros que não estejam devidamente documentados, evitando, assim, sanções.

Os Estados-Membros que têm implementado os programas de API, são capazes de fornecer de imediato a informação sobre se aquele passageiro pode ou não embarcar.

Ou seja, o facto de as transportadoras aéreas poderem identificar de imediato quais os passageiros que podem ou não embarcar, faz com que se evitem custos associados à detenção e/ou ordem de remoção de pessoas, com base em factores específicos disponíveis para os órgãos de controlo de fronteira, evitando que essas pessoas embarquem, impedindo, assim, a chegada ao seu destino.

A principal vantagem da API para as agências de controlo de fronteiras, é o facto destas serem notificadas previamente à chegada de potenciais infractores.

Para além disso, o facto de os dados dos passageiros serem fornecidos em formato eletrónico, e serem prontamente processados, faz com que haja uma economia de captura de dados, uma vez que assim o funcionário da alfândega não é obrigado a realizar a operação normal de entrada de dados, aquando da chegada do passageiro.

A API permite, também, um controlo mais eficaz das fronteiras e, para além disso, o facto de ser um processo automático faz com que haja uma redução dos custos em pessoal.

Por último, é reconhecido à API um potencial catalisador para uma maior cooperação entre agências, tanto a nível nacional como internacional.

Relativamente às autoridades aeroportuárias, a API auxilia o crescimento do tráfego de passageiros através do uso melhorado da tecnologia.

Para além disso, registou-se uma maior satisfação dos passageiros em relação às instalações, tendo havido um menor número de queixas, o que também contribuiu para melhorar a imagem pública, tanto a nível nacional, como a nível internacional, o que, consequentemente, se torna bastante positivo para o turismo.

Cabe, por último, perceber como são recolhidos e transmitidos os dados API.

"Por forma a que a API funcione com sucesso e a nível global, é essencial que haja um grau de uniformização em relação aos dados exigidos pelas agências de controlo das fronteiras, que irá receber e processar esses dados.

Do ponto de vista da atuação das agências de controlo das fronteiras, esta limitação e harmonização desses dados, pode restringir um pouco as suas operações.

No entanto, é evidente que, para as operadores capturarem e poderem transmitir dados de passageiros em larga escala para um grande número de agências de controlo das fronteiras, esta limitação e harmonização é essencial.

A polícia WCO, IATA e ICAO concordaram entre si que o conjunto de dados API deve ser incorporado na mensagem PAXLST – Passenger List Message -, a ser utilizada para a transmissão desses dados pelas transportadoras para as agências de controlo de fronteiras no país de destino.

No entanto, é importante notar que os países devem limitar as suas exigências de dados ao mínimo necessário e de acordo com a legislação nacional em vigor.

Estes dados podem ser divididos em duas categorias distintas:

a) *Os dados relativos ao voo;*
b) *Os dados relativos a cada passageiro em questão.*

Os detalhes dos elementos de dados individuais para cada uma destas categorias, consta do anexo IV, da folha de Anexos.

Os dados do voo devem desde logo estar disponíveis para as transportadoras nos seus próprios sistemas automáticos.

Os dados deverão ser os que constam no Anexo I da folha de Anexos, e apenas estes, uma vez que se o conjunto destes dados fosse ampliado, acabaria por prejudicar a Transportadora e o próprio normal funcionamento do aeroporto.

A WCO, a IATA e ICAO recomendam aos seus membros que os dados API não devem exceder aqueles que constam do Anexo I da folha de Anexos."[77]

[77] Tradução livre da autora, *"For API to function successfully and on a widespread basis, i tis essential that there be a strict limitation and a very high-degree of uniformity in relation to the data required by the Border Control Agencies which will receive and process that data. From the perspective of the Border Control Agencies, the limitation and harmonization of this data may be somewhat restrictive to their operations. However i tis clear that for carriers to capture and transmit passenger data on a large scale to a large number of Border Control Agencies, this limitation and harmonization is essential.*
With the above in mind, the WCO, IATA and ICAO have jointly agreed on the maximum set of API data that should be incorporated in the PAXLST message to be used for the transmission of such data by the carriers to the Border Control Agencies in the destination country. However, i tis importante to note that countries should limit their data requirements to the minimum necessary and according to the national legislation. This data can be divided into two distinct categories:

a) *Data relating to the Flight (Header Data)*
b) *Data relating to each individual passenger (Item Data).*

Details of the individual data items for each of these two categories are given below. It should be noted that the Flight data should already be available to carriers from their own automated systems. The passenger data corresponds to those items of data that currently appear on machine-readable passports, other official travel documents or those which may be available in the transporting carrier´s reservation system. From the point of view of promulgating the use of API, extending the required data elemento set beyond that limit would hinder carrier´s and airport operation. The WCO, IATA and ICAO recommend to their members that the API data must not exceed that given in this guideline." (Guidelines on Advance Passenger Information, 2010)

5. A relação entre o PNR e outros sistemas de informação na União Europeia

Com os acontecimentos do último século têm sido desenvolvidos instrumentos relacionados com o uso de base de dados pessoais, sendo que se torna importante perceber como se relaciona o sistema de dados PNR com outros sistemas de informação utilizados na União Europeia.

Um destes instrumentos passa pelo *European Border Management Strategy*, ou seja, pela estratégia europeia de gestão das fronteiras, sendo este uma proposta da Comissão Europeia e considerado um dos mais importantes sistemas de informação.

Em Fevereiro de 2008, a Comissão lançou uma proposta da criação de um sistema de entrada e saída, permitindo a gravação electrónica das datas de entrada e saída de nacionais, de países terceiros, no espaço Schengen.

Este sistema de controlo de entradas e saídas, permite às autoridades nacionais identificarem todos aqueles que ultrapassam o período de estadia, tomando as medidas adequadas à situação em concreto.

Outra proposta da Comissão inclui a instalação de portas automáticas, que leem os dados biométricos contidos nos documentos de viagem, ou que estejam armazenados num sistema ou banco de dados, comparando-os com os dados biométricos do viajante, por forma a permitir a identificação automatizada do mesmo sem a intervenção de guardas de fronteira, com o objetivo de aumentar e acelerar os controlos nas fronteiras.

Após um exame adequado, é concedida à pessoa o estatuto de "viajante registado", tendo em conta certos critérios, fazendo prova, por exemplo, se a pessoa tem meios de subsistência suficientes.

Em abril de 2009, o grupo de trabalho do Conselho sobre o Terrorismo numa nota referiu-se à importância da utilização de dados PNR junto de outros bancos de dados com o propósito de *"estabelecer um quadro mais claro do movimento de terroristas conhecidos e suspeitos, permitindo a realização de intervenções apropriadas."*[78]

[78] Tradução livre da autora, *"establishing a clearer picture of the movement of known and suspected terrorists and allowing for appropriate interventions to be made."* (Council doc. 8667/09, 14 April 2009)

De acordo com este grupo, o uso de dados API, conjuntamente com os dados PNR é necessário para que se consiga uma melhor detecção de movimentos terroristas.

Desta forma, conseguir-se-ia maximizar a utilidade dos dados PNR se fossem combinados com os dados API, uma vez que estes são considerados dados necessários para identificar viajantes.

Esta possibilidade de ligação dos dados PNR com outras bases de dados foi ligeiramente alterada no projeto de junho de 2009.

Atualmente, o Sistema de Informação Schengen – *SIS* -, é uma das bases de dados mais importantes, utilizadas para controlo de fronteiras e para fins de aplicação da lei na União Europeia.

Na bases de dados SIS é possível encontrar a identificação de cidadãos de países terceiros, uma vez que tal é permitido através de decisão nacional que considere essa pessoa como sendo perigosa constituindo, assim, uma ameaça para a ordem pública, para a segurança pública e, até mesmo, para a segurança nacional.

Essas decisões nacionais normalmente são baseadas na lei da imigração sobre a deportação e recusa de entrada da pessoa em questão.

Constando informações acerca de uma pessoa na base de dados do SIS, essa pessoa fica impedida de entrar em todos os outros Estados-Membros, o mesmo é dizer que essa pessoa fica impedida de circular no espaço Schengen.

Outra das consequências é essa pessoa, cujas informações constam no SIS, poder ver recusada a emissão de um visto ou uma autorização de residência ou até mesmo ser expulso ou detido.

O uso de bancos de dados como o SIS e, agora o SIS II, incluindo a sua utilização por pessoal consular em países terceiros para emissão de vistos, levanta questões importantes no que respeita à responsabilidade e prestação de contas dos Estados-Membros.

Como o SIS é baseado no princípio da confiança mútua e na execução mútua das decisões administrativas nacionais, significa que os Estados-Membros podem invocar uma outra decisão de qualquer outra Estado-Membro com o propósito de legitimar a sua atuação,

como a recusa de entrada daquele indivíduo nas suas fronteiras, ou a rejeição dos pedidos de visto, ou até mesmo expulsões.

Por último foi lançada a proposta de incluir no SIS os chamados "perturbadores", cujo objetivo é compartilhar as informações acerca dessas pessoas, relativamente às quais existem razões para se acreditar que vão cometer uma qualquer infração penal grave.

No entanto, esta proposta não dá qualquer definição de infração penal grave, mas acreditamos que será aquela que é susceptível de perturbar a paz pública.

Desta forma, através das informações partilhadas, os tais "perturbadores", incluindo cidadãos da União Europeia, poderiam ser impedidos de aceder a um determinado Estado-Membro, evitando-se assim, a consumação de uma qualquer infração penal grave.

Capítulo III – A criação de um sistema Europeu de PNR

1. Antecedentes

Como tem vindo a ser dito até aqui, a recolha, a retenção, a manipulação, a troca e a correção de dados pessoais na Europa voltou a ser, mais uma vez, uma questão de grande interesse, sendo que a última vez que o uso de dados constituiu uma política importante na Europa, foi na década de 1970, com a Convenção do Conselho Europeu para a proteção da utilização dos dados pessoais das pessoas singulares e que foi aberta a assinatura em 1981.

Esta Convenção define, ainda, o padrão para a utilização de dados pessoais na Europa.

Em 2001 foi criada a Autoridade Europeia para a proteção de dados, de modo a assegurar que os direitos e liberdades fundamentais dos indivíduos, em particular a sua privacidade, são sempre respeitados pelas instituições e organismos comunitários no tratamento de dados pessoais ou aquando do desenvolvimento de novas políticas.

Os critérios desenvolvidos pelo Tribunal Europeu dos Direitos do Homem, com base no artigo 8º da Convenção Europeia dos Direitos do Homem, devem, na nossa opinião, ser também levados em conta ao avaliar as propostas atuais sobre o sistema PNR da União Europeia.

Os critérios são importantes em termos de acessibilidade e previsibilidade da lei.

De acordo com a opinião do Tribunal Europeu dos Direitos do Homem, os critérios de "em conformidade com a lei" e "qualidade de direito", do artigo 8.º, requerem procedimentos de supervisão e as garantias adequadas e eficazes contra o abuso do Estado de Direito.

Tendo em conta o critério "acessibilidade da lei", todo o processo de transmissão de dados PNR, com base no projeto da Decisão-Quadro, deverá ser abrangido por quatro regimes legais: a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados; o projeto de Decisão-Quadro do PNR aplicável à transmissão de dados PNR pelas companhias aéreas às unidades de informações de passageiros e, por último, a Decisão-Quadro sobre a proteção de dados para países terceiros e, finalmente, as transferências de dados entre PIU – *Passenger Information Units* -, e as autoridades nacionais responsáveis pela aplicação da lei serão abrangidos por legislação nacional de proteção de dados.

A questão que se coloca quanto à existência de uma base de dados PNR na Europa, prende-se com o facto de que, as regras jurídicas que lidam com a recolha e utilização dos

dados de passageiros, bem como, com as competências do PIU; os poderes das autoridades nacionais e autoridades de países terceiros; os direitos das pessoas em causa e as autoridades de proteção de dados, ainda não são suficientemente claras e precisas.

Foi com os atentados de 11 de setembro de 2001, nos Estados Unidos da América, que a utilização de dados voltou a ter um maior destaque na agenda política, tendo sido concedida às autoridades dos Estados Unidos autorização para recolher e conservar dados sobre os indivíduos que chegam aos Estados Unidos por via aérea, sendo esta uma medida com vista a aumentar a segurança no país.

No entanto, tal medida teve as suas implicações na União Europeia no que respeita à proteção dos dados.

Assim, com o objectivo de fornecer uma base comum para a transmissão de dados pessoais pelas transportadoras aéreas da União Europeia para as autoridades dos Estados Unidos da América, foi celebrado um primeiro, de muitos acordos, entre os Estados Unidos e a União Europeia em 28 de maio de 2004, a regular tal situação.

1.1 O Acordo PNR entre a União Europeia e os Estados Unidos da América

E foi assim, que surgiu o primeiro acordo entre a União Europeia e os Estados Unidos da América, daqui em diante EUA, longe de ser pacífico, uma vez que as relações transatlânticas, sobre a matéria em questão, sempre foram pautadas por uma enorme tensão, pela abordagem securitária e mais intrusiva dos Estados Unidos e a posição da União Europeia que se pauta pela defesa mais intransigente das liberdades e direitos individuais.

Foi esta tensão que levou à celebração de quatro acordos PNR entre a União Europeia e os Estados Unidos.

Começando pelo primeiro acordo, que remonta a 2004, apraz fazer um breve enquadramento temporal.

Com os atentados de 11 de setembro de 2001, os EUA, a fim de reforçar o controlo das suas fronteiras, adotaram legislação, obrigando as companhias aéreas que viajavam para o seu território a permitirem o acesso eletrónico da Autoridade Americana de Alfândegas e Controlo de Fronteiras *(Buereau of Customs and Border Protection – CBP)* do Departamento de Segurança Interna dos EUA *(DHS – Department of Homeland Security)* aos dados pessoais

dos passageiros que voam para, de ou através dos EUA, que constam da base de dados *PNR* e que estão armazenados nos seus sistemas de reserva e de controlo de partidas.

As companhias aéreas que negassem tal acesso, eram punidas com sanções e perdiam o direito de aterragem nos EUA.

Ora, tal situação traduzir-se-ia num prejuízo gravoso para as companhias. No entanto, é aqui que começa a surgir a dicotomia para as companhias aéreas europeias, uma vez que se colocava num dos pratos da balança, a questão de aceder aos sistemas de reserva e gestão de passageiros, violando as normas europeias de proteção de dados pessoais e, no outro, as sanções em que podiam incorrer. No limite, a perda das rotas comerciais para os EUA, caso não autorizassem o acesso a esses dados por parte das autoridades americanas.

As companhias aéreas europeias estavam agora com o problema da incompatibilidade da transmissão para os EUA de dados recolhidos com uma finalidade meramente comercial e a Diretiva 95/46/CE, em vigor na UE, como o principal instrumento legislativo em matéria de proteção de dados pessoais.

Perante todas estas adversidades, a Comissão iniciou negociações com as autoridades americanas, a 14 de maio de 2004, ao abrigo do artigo 25.º da Diretiva 95/46/CE.

A decisão confirmou a adequação do nível de proteção dos dados PNR transferidos para a autoridade de controlo de fronteiras dos EUA, acabando por legislar a transmissão desses dados.

Esta decisão teve por base uma declaração unilateral do Departamento de Segurança Interna, na qual este garantia assegurar uma proteção adequada aos dados PNR quando solicitados às companhias aéreas europeias e que constavam de um anexo à Decisão da Comissão.

De entre os compromissos assumidos, destacavam-se os seguintes: *"a utilização dos dados PNR apenas para fins de prevenção e combate ao terrorismo e crimes graves que revelem a origem racial, étnica, opiniões políticas, crenças religiosas, situação de saúde, pertença a um sindicato ou orientação sexual); a utilização do método de extração dos dados dos sistemas de reserva (sistema pull) só até as companhias aéreas se dotarem de um sistema de exportação de dados (sistema push), considerado menos intrusivo; um período de retenção de 3,5 anos para os dados PNR que não tenham sido tratados manualmente, findo o qual*

eram destruídos; os dados PNR objeto de tratamento manual transitavam no final deste período de 3,5 anos para um ficheiro de registos apagados, onde permaneceriam 8 anos" (Constança Urbano de Sousa, 2014, p.57).

Esta decisão foi acompanhada por uma Decisão do Conselho, de 17 de maio de 2004, que aprovou um acordo entre a Comunidade Europeia e os EUA, ao abrigo dos artigos 95.º e 300.º do Tratado da Comunidade Europeia (atuais artigos 114.º e 218.º do Tratado sobre o Funcionamento da União Europeia), que impunha às companhias aéreas a obrigação de transferir os dados PNR para os Estados Unidos.

No entanto, ambas as decisões foram anuladas pelo Tribunal de Justiça, em 2006, em virtude de um recurso de anulação interposto pelo Parlamento Europeu, que invocou abuso de poder, violação de princípios essenciais sobre proteção de dados, violação de direitos fundamentais e, ainda, a violação do princípio da proporcionalidade.

"No seu acórdão de 30 de maio de 2006, o Tribunal de Justiça considerou que o artigo 95.º do TCE, conjugado com o artigo 25.º da Diretiva sobre proteção de dados, não constituía a base legal para a competência da Comunidade nesta matéria. Isto porque o tratamento e transferência dos dados PNR não visavam a prestação de um serviço, mas a salvaguarda da segurança pública e fins repressivos. Assim, esta transferência estava excluída do âmbito da Diretiva sobre proteção dos dados pessoais e da competência da Comunidade Europeia". (Constança Urbano de Sousa, 2014, p.58)

Foi a 16 de outubro de 2006 que o novo acordo entre os Estados Unidos da América e a União Europeia foi publicado, embora sujeito a controlos de idiomas.

Este acordo manteve na sua estrutura o conteúdo do acordo de 2004, permitindo à autoridades americanas o acesso electrónico aos dados PNR contidos nos sistemas das transportadoras aéreas, sob o compromisso por parte dos EUA em matéria de proteção dos dados PNR.

Importa, agora, analisar as doze principais questões relativas ao novo acordo e à sua interpretação.

A primeira questão prende-se com o método *"push-pull"*, de acordo com o qual, no primeiro acordo, as autoridades dos Estados Unidos, mais concretamente o Departamento de

Segurança Interna, podia aceder às bases de dados das operadoras e retirar as informações que considerasse necessárias.

Isto deveu-se ao facto de as transportadoras europeias não disporem de tecnologia própria para lidar com o sistema de *"push"*, que é considerado o mais adequado, do ponto de vista de proteção de dados, uma vez que, caso as autoridades americanas necessitassem de algumas informações especificadas, deveriam fazer um pedido aos portadores dessas informações.

Em 2004 chegou-se a um acordo de que o sistema deveria ser alterado para o método *"push"*, no entanto, apesar de o relatório do grupo de trabalho da União Europeia sobre a proteção das pessoas em relação ao tratamento de dados pessoais, datado de 14 de junho de 2006, considerar que todas as condições estavam reunidas para se implementar o método *"push"*. O novo acordo estabeleceu que as autoridades americanas deveriam ser autorizadas a aceder às informações de que necessitassem.

Quanto aos limites de tempo e à frequência, o acordo de 2004 previa que as autoridades americanas dispunham, apenas de 72 horas antes de um voo para recolherem as informações que considerassem necessárias e, ainda, dispunham de um número limitado de vezes para verificar esses dados.

Com o novo acordo, deixou de haver o limite de 72 horas para a recolha das informações e, ainda, deixou de haver limite quanto ao número de vezes que as autoridades americanas podem verificar esses dados.

Quanto à finalidade, no primeiro acordo, os fins para os quais podiam esses dados serem utilizados eram bastante amplos, auxiliando no combate a diversos tipos de crimes. No entanto, com o novo acordo, as finalidades dos dados foram aumentando, servindo hoje em dia, não só no combate à criminalidade, como também no combate a doenças infecciosas, de forma a proteger interesses vitais.

Em relação à partilha de dados, o novo acordo amplia substancialmente o número de agências com as quais as autoridades dos Estados Unidos podem compartilhar os dados.

Quanto à natureza e ao número de dados possíveis de serem recolhidos, no relatório de 14 de junho de 2006, o grupo de trabalho sobre a proteção das pessoas no que respeita ao

tratamento de dados pessoais, especificou que apenas 19 itens de dados que foram fornecidos, eram apropriados e úteis para partilha.

Relativamente à retenção de dados, de acordo com o acordo inicial, os dados tinham que ser destruídos após 3 e 5 anos. Com o novo acordo, discute-se a questão de saber se e quando destruir os dados PNR que foram recolhidos, em conformidade com os compromissos que serão abordados pelos Estados Unidos e pela União Europeia como parte de discussões futuras.

Em relação à proteção de dados, o Conselho determinou que as autoridades americanas seguem procedimentos satisfatórios para a proteção de dados da União Europeia.

Já quanto à situação jurídica dos cidadãos da União Europeia, devem ser postos em prática os procedimentos necessários para informar os cidadãos da União Europeia, quanto à transferência dos seus dados, garantindo que eles têm as informações necessárias para o caso de necessitarem reclamar sobre alguma questão.

Assim, a análise jurídica detalhada revela-se essencial por forma a estabelecer um nível de proteção dos dados e de forma a ter resposta para potenciais lacunas.

No que respeita à transferência de outros dados, existem preocupações relativas às consequências que o acordo PNR pode acarretar para outros acordos de transferência de dados.

Existem muitas outras questões que o novo acordo suscita, em particular, no que diz respeito à reparação e proteção do indivíduo.

Quanto à proteção do indivíduo, há uma situação que, em nosso entender, é necessário ser referida, para que se perceba qual o impacto da transferência de dados.[79]

Tal situação prende-se com a transferência de dados defeituosos por parte das autoridades canadianas para as autoridades americanas. Esses dados pertenciam a Maher Arar, um cidadão com dupla nacionalidade, canadiana e síria, que foi impedido de continuar a sua viagem de Nova Iorque para o Canadá, por suspeitas de envolvimento terrorista em Setembro de 2002.

Maher Arar foi enviado para a Síria, onde foi detido e torturado por mais de um ano.

[79] Guild, Elspeth (2007), *Inquiry into the EU-US Passenger Name Record Agreement*, Centre for European Policy Studies

Mais tarde, em outubro de 2003, regressou ao Canadá e foi realizado um inquérito federal, ordenado e liderado por um juiz do Supremo Tribunal, de forma a perceber como tal situação ocorreu.

Em setembro de 2006 foram publicadas as conclusões desse inquérito, tendo as mesmas considerado o Sr. Arar livre de qualquer suspeita de ligações a quaisquer atividades terroristas, acrescentando ainda, que foram encontradas falhas graves na forma como os dados tinham sido transferidos pelos serviços canadenses para os serviços americanos, o que levou as autoridades americanas a considerar, erradamente, que o Sr. Arar tinha ligações a atividades terroristas.

A 26 de janeiro de 2007, o Primeiro-Ministro canadiano emitiu um pedido formal de desculpas ao Sr. Arar, tendo-lhe oferecido uma indemnização.

Tendo em conta este exemplo, e já tendo sido tratada esta questão ao longo da dissertação, mais uma vez se percebe o impacto que a transmissão de dados imprecisos ou defeituosos, pode ter na vida de um indivíduo.

E, para além disso, estas são situações que podem ser muito dispendiosas para os governos.

Assim, o novo acordo PNR entre a União Europeia e os Estados Unidos da América contém uma inovação em relação ao anterior, ao afirmar que *"este acordo não cria nem confere qualquer direito de vantagem a qualquer pessoa ou entidade, pública ou privada"* , privando, desta forma, alguém, que se encontre numa situação semelhante à do Sr. Arar, de obter uma indemnização caso os seus dados sejam indevidamente transmitidos.

Ora, não nos parece uma solução muito adequada, sendo esta, em nosso atender, uma forma de descarte de responsabilidade das partes pelos seus atos, desprotegendo de uma forma severa os cidadãos que se deparem na sua vida com as consequências de uma transmissão errada dos seus dados.

A nova decisão do Conselho que aprova o referido acordo, inclui uma nova redação do artigo 4.º, estabelecendo que os Estados-Membros têm competência para suspender a transferência de dados para as autoridades americanas, por forma a proteger as pessoas do tratamento dos seus dados pessoais em dois casos:

1.º Se uma autoridade americana determina que o Departamento de Segurança Interna desrespeita as normas de proteção aplicáveis; ou

2.º Quando exista uma suspeita fundada de que as normas de proteção aplicáveis estão a ser violadas, isto é, quando existam motivos razoáveis que levam a crer que o Departamento de Segurança Interna não toma ou não irá tomar as decisões adequadas na devida altura, por forma a impedir a continuação da transferência de dados pessoais, o que leva a que haja um iminente risco de causar graves prejuízos à(s) pessoa(s) em causa e, ainda assim, as autoridades competentes nos Estados-Membros tiverem feito esforços razoáveis, dadas as circunstâncias, de modo a informar o Departamento de Segurança Interna;

Se por um lado esta nova decisão do Conselho permite que se interrompa a transferência no sistema de fornecimento de dados, por outro lado, não prevê que, se um Estado-Membro determina que as autoridades americanas não estão a aplicar as regras devidas de proteção, deva haver solidariedade dos outros Estados-Membros.

O que significa que, se este é um acordo comum, os compromissos deveriam ser, igualmente, comuns, ou seja, se qualquer cidadão de qualquer Estado-Membro corre o risco de ter um tratamento semelhante ao que o Sr. Arar teve, todos os Estados-Membros deviam ser envolvidos na proteção desse cidadão e agir em solidariedade para proteger todos os cidadãos da União Europeia, contra o uso abusivo e prejudicial de dados pessoais.

Devido à urgência na sua celebração, o acordo de 2006 tratou-se de um acordo provisório, com o objetivo de evitar um vazio legal, causado pelo acórdão anulatório do Tribunal de Justiça, cuja caducidade estava prevista para o dia 31 de julho de 2007.

Ora, tendo o acordo de 2006 um carácter provisório, o Conselho iniciou as negociações para a celebração de um terceiro acordo PNR, que viria a ser aprovado no dia 23 de julho de 2007, acordo este que seguia a estrutura do anterior.

As regras sobre a recolha e proteção de dados PNR não constavam de um acordo internacional vinculativo mas sim de compromissos unilaterais do Departamento de Segurança Interna dos Estados Unidos, relativamente aos quais a União Europeia reconhecia níveis de proteção adequados.

A União Europeia apenas tinha que garantir que esses dados, quando solicitados, eram fornecidos aos EUA pelas companhias aéreas europeias.

Na realidade este acordo nunca chegou a ser concluído. Apenas teve uma aplicação provisória com a sua assinatura, uma vez que a sua conclusão ficou dependente do consentimento do Parlamento Europeu, que já em 2007 manifestou uma certa preocupação em relação a ele.

Isto porque, em algumas matérias, sobretudo quanto à proteção de dados pessoais, este acordo significou um retrocesso em relação aos anteriores, uma vez que o destinatário dos dados era já o Departamento de Segurança Interna, no seu todo, incluindo os serviços secretos, e não apenas o seu serviço de controlo de fronteiras, como deveria ser. Depois porque a condição da utilização de dados sensíveis em situações excepcionais, antes excluída, começou a ser possível em determinadas situações; e, ainda, porque se alargou o período de conservação dos dados PNR não tratados manualmente de 3 e 5 para 8 anos.

Ora, o facto de o Parlamento Europeu não ter chumbado o acordo de 2007, fez com que houvesse um novo acordo que garantisse a conformidade da transferência dos dados PNR com as normas europeias de proteção de dados e que, ao mesmo tempo, tivesse em conta as novidades do Tratado de Lisboa neste domínio, principalmente o reforço das competências da União Europeia e a atribuição de efeito jurídico vinculativo à Carta dos Direitos Fundamentais, uma vez que, o seu artigo 8.º consagra o direito fundamental à proteção de dados pessoais.

"(...)O PE exigiu um acordo internacional, juridicamente vinculativo, que satisfizesse determinados parâmetros em matéria de proteção de dados, como por exemplo a limitação da utilização dos dados PNR à luta contra a criminalidade organizada e transnacional ou contra o terrorismo internacional, tal como definido pela UE; a proibição de data mining da utilização dos dados PNR para determinação de perfis (profiling), não podendo qualquer decisão ser tomada com base nos resultados de pesquisas automatizadas; ou a utilização exclusiva do sistema de exportação (push) para transmissão dos dados PNR." (Constança Urbano de Sousa, 2014, p. 60)

Assim, o quarto acordo foi assinado a 14 de dezembro de 2011.

Este acordo contém aspetos do regime de utilização de dados PNR pelos EUA, que até então eram condenados pelo Parlamento Europeu, visto que este acordo não proíbe o *profiling*, autoriza a continuidade do sistema de importação de dados (*pull*), estabelecendo

períodos de armazenamento longos e indeterminados e, para além disso, veda a possibilidade de recurso jurisdicional aos cidadãos europeus não residentes nos EUA.

1.2. O Acordo PNR entre a União Europeia e o Canadá

"A legislação canadiana autoriza a Agência dos Serviços de Fronteiras do Canadá (Border Services Agency) a solicitar a todas as transportadoras aéreas que asseguram um serviço de transporte de passageiros a partir de e com destino ao Canadá que lhe facultem um acesso electrónico aos dados contidos nos registos de identificação dos passageiros (dados PNR) antes da chegada ou da partida dos passageiros do Canadá. Os pedidos das autoridades canadianas baseiam-se no artigo 107.º, n.º1, da Lei Aduaneira, na regulamentação (aduaneira) em matéria de informações sobre os passageiros, no artigo 148.º, n.º1, alínea d), da Lei relativa à imigração e à proteção dos refugiados e no Regulamento n.º 269 de execução desta última lei."[80]

O objetivo da referida legislação é assegurar a obtenção dos dados PNR por via eletrónica, antes da chegada de um voo, por forma a que a Agência dos Serviços de Fronteiras do Canadá consiga proceder de uma forma eficiente e eficaz a uma avaliação prévia dos passageiros, facilitando as deslocações legítimas e, desta forma, assegurando a segurança do Canadá.

Este Acordo entre a União Europeia e o Canadá, permitiu uma colaboração mais eficaz na luta contra o terrorismo e demais criminalidade transnacional grave, promovendo, desta forma, a cooperação policial e judicial internacional, através da partilha de informações que contém dados PNR obtidas pelo Canadá com as autoridades policiais e judiciais competentes dos Estados-Membros.

Assim, as transportadoras aéreas ficam obrigadas a *"(...) facultar à Agência dos Serviços de Fronteiras do Canadá o acesso a determinados dados PNR, na medida em que*

[80] Cfr. Proposta de Decisão do Conselho relativa à assinatura do Acordo entre o Canadá e a União Europeia sobre a transferência e o tratamento dos dados dos registos de identificação dos passageiros/*COM/2013/0529 final – 2013/0251 (NLE)*/

sejam recolhidos e armazenados nos sistemas automatizados de controlo das reservas e partidas das transportadoras aéreas."[81]

É no nosso entender, importante referir que, em matéria de proteção de dados, a legislação da União Europeia não permitem às transportadoras aéreas dos países europeus e de países terceiros que asseguram voos a partir do território da União Europeia, transmitir os dados PNR dos seus passageiros a países terceiros que não sejam capazes de assegurar um nível adequado de proteção dos dados pessoais.

Assim, neste acordo entre a União Europeia e o Canadá, ficou reconhecida a importância desta transferência dos dados PNR, na luta contra o terrorismo e contra a criminalidade grave assegurando, ainda, a segurança jurídica das transportadoras aéreas.

Esta é uma solução que se pretende que seja uniforme em toda a União Europeia, com o objetivo de garantir a segurança jurídica das transportadoras aéreas e, simultaneamente, o respeito dos direitos das pessoas à proteção dos seus dados pessoais e da sua segurança física.

"Em 2005, a União Europeia celebrou com o Canadá um acordo sobre o tratamento dos dados PNR, baseado num série de compromissos assumidos pela Agência dos Serviços de Fronteiras do Canadá no que respeita à aplicação do seu programa PNR. Os compromissos figuram num anexo a uma Decisão da Comissão sobre o nível de proteção adequado dos dados pessoais contidos no registo de identificação dos passageiros aéreos transferidos para o serviço de fronteiras canadiano (Canada Border Service Agency). Após o termo de vigência da Decisão da Comissão em 2009, a Agência dos Serviços de Fronteiras do Canadá comprometeu-se unilateralmente a garantir à UE que os compromissos continuariam a vigorar plenamente até à entrada em vigor de um novo acordo."[82]

Com a entrada em vigor do Tratado de Lisboa, foi adotada pelo Parlamento Europeu, a 5 de maio de 2010, uma resolução que apelava a uma renegociação do Acordo.

[81] Cfr. Proposta de Decisão do Conselho relativa à assinatura do Acordo entre o Canadá e a União Europeia sobre a transferência e o tratamento dos dados dos registos de identificação dos passageiros/*COM/2013/0529 final – 2013/0251 (NLE)*/

[82] Cfr. Proposta de Decisão do Conselho relativa à assinatura do Acordo entre o Canadá e a União Europeia sobre a transferência e o tratamento dos dados dos registos de identificação dos passageiros/*COM/2013/0529 final – 2013/0251 (NLE)*/

Foi então que a 21 de setembro de 2010, o Conselho recebeu uma recomendação da Comissão autorizando a abertura das negociações, tendo em vista um Acordo entre a União Europeia e o Canadá relativo à transferência de dados PNR.

O Acordo foi assinado a 6 de maio de 2013 e leva em linha de conta os critérios gerais definidos na Comunicação da Comissão, sobre a abordagem relativa à transferência dos dados do registo de identificação dos passageiros (PNR) para países terceiros.

O Acordo salvaguarda aspectos relevantes no que diz respeito à privacidade das pessoas, como por exemplo, os dados PNR só podem ser utilizados na prevenção, identificação, investigação e repressão das infrações terroristas e das formas graves de criminalidade transnacional.

Também quanto ao prazo de conservação dos dados PNR, o Acordo prevê um prazo limitado, devendo os dados passar ao anonimato decorrido um período de 30 dias, sendo que, qualquer pessoa tem direito de acesso, de retificação, de recurso e de informação.

Para além disso os dados são transferidos através do método de exportação *"push"*, de acordo com o qual são as transportadoras aéreas as responsáveis por transferir os dados PNR necessários para a Agência dos Serviços de Fronteiras do Canadá, sendo os dados eliminados decorrido um prazo muito curto.

O cumprimento de todas estas regras será assegurado pelo comissário canadiano incumbido de garantir a proteção da vida privada e pelos serviços de recurso da Agência suprareferida.

Assim, pretende-se que esta seja uma forma de prevenir, combater e eliminar o terrorismo e outras formas de criminalidade transnacional, através de uma cooperação entre as Partes, com o objectivo de proteger as suas sociedades democráticas e os seus valores comuns e, simultaneamente, garantindo os direitos e as liberdades fundamentais, em especial os direitos à privacidade e à proteção dos dados, promovendo a segurança e o Estado de Direito.

1.3. O Acordo PNR entre a União Europeia e a Austrália

Comparativamente com o que sucede com o Canadá, também *"a legislação australiana* confere *poderes ao Serviço Aduaneiro australiano para exigir a todas as transportadoras aéreas que efectuem voos de passageiros para e a partir da Austrália o acesso electrónico electrónico ao registo de identificação dos passageiros (PNR) antes da sua chegada ou partida da Austrália. (...)*

A referida legislação visa a obtenção de dados PNR por meios electrónicos antes da chegada de um voo e, portanto, reforça consideravelmente a capacidade do Serviço Aduaneiro australiano para levar a cabo uma avaliação eficaz e eficiente dos riscos representados pelos passageiros e para facilitar as viagens de boa-fé, melhorando assim a segurança da Austrália. A União Europeia, ao cooperar com a Austrália em matéria de luta contra o terrorismo e outros crimes transnacionais graves, considera que a transferência de dados para a Austrália promove a cooperação policial e judiciária internacional graças à transferência de informações analíticas dos dados PNR pela Austrália para as autoridades competentes dos Estados-Membros, bem como para a Europol e a Eurojust, no âmbito das respectivas competências."[83]

Ora, as transportadoras aéreas são obrigadas a fornecer ao Serviço Aduaneiro australiano o acesso aos dados que este considere essenciais na execução da sua tarefa.

Tal como foi referido em relação ao Canadá, é necessário que seja assegurado um nível de proteção adequado dos dados pessoais.

É, por isso, *"(...) necessária uma solução que forneça a base jurídica para a transferência de dados PNR da UE para a Austrália, tendo em conta a necessidade e importância da utilização de dados PNR para fins de luta contra o terrorismo e outros crimes transnacionais graves, evitando simultaneamente a incerteza jurídica para as transportadoras aéreas. Além disso, essa solução deve ser aplicada de modo uniforme no conjunto da União Europeia, a fim de assegurar a segurança jurídica das transportadoras*

[83] Decisão do Conselho relativa à assinatura do Acordo entre a União Europeia e a Austrália sobre o tratamento e a transferência de dados do registo de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Serviço Aduaneiro e de Protecção das Fronteiras australiano/*COM/2011/0280 final */

aéreas e o respeito do direito dos indivíduos à protecção dos dados pessoais, bem como a sua segurança física."[84]

Foi em 6 de maio de 2011 que a União Europeia e a Austrália assinaram o acordo quanto à transferência e tratamento de dados PNR com base num conjunto de compromissos assumidos pelo Serviço Aduaneiro australiano em relação à aplicação do seu programa PNR.

O presente Acordo estabeleceu diversas garantias eficazes no que diz respeito à proteção dos dados que serão objecto de transferência e de tratamento.

O tratamento dos dados destina-se, apenas, à prevenção, detecção, investigação e repressão de infracções terroristas e da criminalidade transnacional grave.

O método utilizado para a transferência dos dados é o método de exportação *"push"*, sendo proibida a utilização de dados sensíveis.

Os dados têm um período de conservação limitado, tornando-se os mesmos anónimos após um determinado período de tempo, sendo que o cumprimento destas regras fica sujeito à supervisão independente do Comissário para a proteção de dados e informação australiano.

Tal como o Acordo celebrado entre a União Europeia e o Canadá, este é um Acordo que garante, igualmente, os direitos e as liberdades fundamentais, em especial os direitos à privacidade e à proteção dos dados, promovendo a segurança e o Estado de Direito.

2. A Proposta de Decisão-Quadro COM (2007) 654 final SEC (2007) 1422 e 1453 relativa à utilização dos dados do Registo, de Identificação de Passageiros (Passenger Name Record) para efeitos de aplicação da lei para fins de combate ao terrorismo e à criminalidade organizada

Em novembro de 2007, a Comissão Europeia publicou uma proposta de Decisão-Quadro relativa à utilização dos dados PNR para fins de aplicação da lei.[85]

[84] Decisão do Conselho relativa à assinatura do Acordo entre a União Europeia e a Austrália sobre o tratamento e a transferência de dados do registo de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Serviço Aduaneiro e de Proteção das Fronteiras australiano/*COM/2011/0280 final */

[85] COM (2007) 654, ver também a Avaliação de Impacto da Comissão que acompanha a presente proposta, 6 novembro 2007, SEC (2007) 14253 e o seu resumo SEC (2007) 1422.

Enquanto que a Diretiva 2004/82/CE, tinha como único objetivo a luta contra a imigração ilegal, a Proposta tem por objetivo prevenir e lutar contra as atividades terroristas e contra a criminalidade organizada.

De acordo com a Avaliação de Impacto da Comissão, os dados PNR devem ser úteis para a aplicação da lei, da seguinte forma:

" **1.** Comparando os dados PNR com os sistemas de alerta, a fim de identificar terroristas e criminosos conhecidos;

2. Identificação de passageiros que tenham alguma ligação a um conhecido terrorista ou outro tipo de criminoso (por exemplo, quando utilizam o mesmo endereço, o mesmo número de cartão de crédito, entre outros...);

3. Identificar "passageiros de alto risco", cruzando os dados PNR com uma combinação de "características e padrões de comportamento";

4. Identificar "passageiros de alto risco" cruzando os dados PNR com a inteligência de risco relevante num determinado momento;

5. Fornecendo informações sobre a viagem realizada depois de algum crime terrorista ter sido cometido."[86]

O primeiro e o segundo ponto identificam terroristas, criminosos ou aqueles que, de alguma forma, estejam ligados a essas pessoas, já o terceiro e o quarto ponto identificam os chamados "passageiros de alto risco". Por último, o quinto ponto visa a criação de novos perfis ou fornece novas informações sobre a viagem em si ou determinados padrões de comportamento.

Os motivos pelos quais se apresentou tal proposta, são um pouco ambíguos. Isto porque, por um lado, apenas um número limitado de Estados-Membros adotou legislação

[86] Tradução livre da autora, *"- Running PNR data against alert systems in order to identify known terrorista and criminals;*

- *Identification of (unsuspected) passengers connected to a known terrorista or criminal (for exemple when they use the same address, credit number, contact details);*
- *Identifying "high-risk passengers" by running PNR data against a combination of "characteristics and behavioural patterns";*
- *Identifying "high-risk passengers" by running PNR data against risk intelligence relevant at a certain crime;*
- *Providing intelligence on travel patterns associations after a terrorista offence has been committed."* (Evelien Brouwer, 2009, p.4)

neste domínio, o que significa que potenciais benefícios, quanto ao regime de prevenção do terrorismo e do crime organizado, que poderiam ser a uma escala da União Europeia, não são plenamente realizados.

Por outro, a Comissão sublinha a necessidade de uma abordagem harmonizada, por forma a que se consiga o intercâmbio de informações relevantes a nível da União Europeia.

A proposta da Comissão previa a obrigação das transportadoras aéreas transmitirem os dados dos seus passageiros dos voos internacionais para o Estado-Membro a que se destina ou em relação ao voo que está saindo desse mesmo Estado.

Segundo a proposta da Comissão, os dados deveriam ser disponibilizados, em vinte e quatro horas, ao PIU – *Passenger Information Units* -, estabelecido em cada Estado-Membro, antes da partida programada do voo.

Para além disso, os dados podiam ser conservados durante treze anos, cinco após a sua transferência para o PIU do primeiro Estado-Membro, em cujo território o voo internacional está a entrar ou a sair e, no termo desse período de cinco anos, um novo período de oito.

Durante este período de tempo, é possível ter acesso aos dados, processá-los e utilizá-los mediante aprovação da autoridade competente e, apenas, em resposta a uma ameaça ou risco real, relacionado com a prevenção e com a luta contra o terrorismo e a criminalidade organizada.

Por último, o artigo 8º da proposta da Comissão previa que os dados dos passageiros podiam ser transmitidos às autoridades policiais de países terceiros com as finalidades de prevenção, detenção, investigação e repressão de atos terroristas ou de criminalidade organizada.

No entanto, com a entrada em vigor do Tratado de Lisboa, a proposta inicial da Comissão de 2007, tornou-se obsoleta.

Assim, em 2011 a Comissão voltou a apresentar uma nova proposta.

A proposta da Comissão consistia na transferência dos dados sobre os passageiros de voos internacionais, realizados nos sistemas de reserva das transportadoras aéreas, para uma entidade especializada no Estado-Membro da União Europeia, de chegada ou de partida, que

analisasse e retivesse esses dados para efeitos de prevenção, detecção, investigação e repressão da criminalidade grave e de atividades terroristas.

Outro ponto importante da proposta, é que por forma a proteger a privacidade dos dados pessoais, estes apenas poderiam ser utilizados para fins de combate à criminalidade grave e às atividades terroristas, sendo que as autoridades policiais dos estados da União Europeia não poderiam reter os dados por mais de cinco anos.

Os dados pessoais que pudessem revelar a origem racial ou étnica, opiniões políticas ou crenças religiosas não podiam ser transferidos pelas transportadoras aéreas para, ou usados de qualquer forma pelos Estados-Membros da União Europeia.

Qualquer Estado-Membro da União Europeia deveria solicitar às transportadoras aéreas os dados de que necessitasse, sendo os mesmos, posteriormente, enviados pela transportadora aérea em causa – método *"push",* já anteriormente referido.

Os Estados-Membros da União Europeia deveriam criar entidades especializadas para trabalhar com os dados, garantindo a segurança dos mesmos e que essas entidades fossem monitorizadas por uma autoridade supervisora independente.

Outra das propostas da Comissão seria o direito dos passageiros a uma informação precisa sobre a recolha de dados PNR, bem como a previsão de regras que proporcionassem aos passageiros o direito de acesso, rectificação e eliminação dos dados e recurso a vias judicias, caso fosse necessário.

Por último, a Comissão propunha a existência de regras sobre a forma como os dados deveriam ser transferidos, sobre o número de vezes que os dados poderiam ser transferidos pelas transportadoras aéreas para os Estados-Membros da União Europeia e como proteger essas transferências a fim de minimizar o impacto da evasão na privacidade e minimizar os custos para as transportadoras aéreas.

A Proposta esteve a ser discutida no Parlamento Europeu, sendo que, na sua resolução de 11 de março de 2015, o Parlamento comprometeu-se a trabalhar para a finalização de uma Diretiva PNR da União Europeia, até ao final desse ano.

Uma vez adotada, a Diretiva servia o propósito de melhorar a cooperação entre os sistemas nacionais, de reduzir lacunas que existissem respeitantes à segurança entre os

Estados-Membros. Ou seja, no fundo, o objetivo é que existam indicadores comuns para o tratamento de dados PNR, tendo em vista o combate a qualquer tipo de criminalidade.

3. A Diretiva 2016/681 do Parlamento Europeu e do Conselho de 27 de Abril de 2016 relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, detecção, investigação e repressão das infrações terroristas e da criminalidade grave

"Em 6 de novembro de 2007, a Comissão adotou uma proposta de decisão-quadro do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros (passenger name record – PNR) para fins policiais. No entanto, com a entrada em vigor do Tratado de Lisboa em 1 de dezembro de 2009, a proposta, que não fora adotada pelo Conselho até essa data, tornou-se obsoleta."[87]

Assim, surgiu a Diretiva 2016/681 com o duplo objectivo de garantir a segurança e, ainda, de proteger a vida e a segurança das pessoas, criando um regime jurídico que se aplique à proteção dos dados PNR, relativamente ao seu tratamento por parte das autoridades competentes.

Segundo a Diretiva em análise *"a utilização eficaz de dados PNR, nomeadamente mediante a sua comparação com várias bases de dados sobre as pessoas e os objetos procurados a fim de obter provas e, se for caso disso, detetar cúmplices de criminosos e desmantelar redes criminosas, é necessária para prevenir, detetar, investigar e reprimir infrações terroristas e a criminalidade grave e, assim, reforçar a segurança interna."*

Como já foi anteriormente explicado nesta dissertação, os dados PNR têm uma função importante na luta contra o terrorismo e criminalidade grave, pois através da sua análise é possível identificar pessoas que deverão ser sujeitas a um controlo mais minucioso e cuidado pelas autoridades competentes, por terem, de alguma forma, um envolvimento em atividades terroristas ou em qualquer outro tipo de criminalidade grave.

[87] Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, detecção, investigação e repressão das infrações terroristas e da criminalidade grave.

Esta Diretiva não impõe às transportadoras aéreas a obrigação de recolherem ou conservarem dados adicionais dos passageiros, nem sequer impõem aos passageiros a obrigação de fornecerem outros dados para além dos que são fornecidos às transportadoras aéreas.

Os dados PNR, juntamente com os dados API, permitem aos Estados-Membros verificarem a identidade dos indivíduos, evitando o risco de controlarem e investigarem pessoas inocentes e permite retirar um melhor aproveitamento para fins policiais.

A transmissão antecipada de dados referentes a informações prévias sobre os passageiros (API) pelas transportadoras aéreas, é regulada pela Diretiva 2004/82/CE que prevê a transferência desses dados para as autoridades nacionais competentes, de modo a melhorar os controlos nas fronteiras e combater a imigração ilegal.

Para isso é necessária a adoção de disposições, por parte dos Estados-Membros, que obriguem as transportadoras aéreas que operem voos para fora da União Europeia, a transferirem os dados PNR recolhidos, incluindo os dados API, muito embora, os Estados-Membros tenham a possibilidade de alargar esta obrigação às transportadoras aéreas que operem voos no território da União Europeia.

Esta Diretiva prevê ainda, no seu artigo 11.º, n.º1, alínea b) que o tratamento de dados deverá ser proporcional relativamente aos objectivos de segurança que a Diretiva se propõe prosseguir.

Os dados PNR deverão ser transferidos para a unidade de informações de passageiros (UIP), com o objectivo de tornar essa informação mais clara e reduzir os custos para as transportadoras aéreas.

A unidade de informações de passageiros pode ser criada em conjunto por vários Estados-Membros, e aí trocar informações entre si através de redes de intercâmbio de informações, facilitando a partilha de informações e garantindo a interoperabilidade.

São os Estados-Membros que suportam os custos da utilização, da conservação e do intercâmbio de dados PNR.

O objectivo será aumentar *"(...) a segurança interna na União e salvaguardando os direitos fundamentais, nomeadamente o direito à privacidade e à proteção dos dados pessoais. Para o efeito, deverão ser aplicadas normas exigentes, de acordo com a Carta dos*

Direitos Fundamentais da União Europeia (a "Carta"), a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (a "Convenção n.º 108") e a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (a "CEDH"). Essa lista não deverá basear-se na raça ou origem étnica, na religião ou nas convicções da pessoa, nem nas suas opiniões, políticas ou outras, na sua filiação sindical nem na sua saúde, vida ou orientação sexual. Os dados PNR deverão incluir unicamente informações pormenorizadas sobre as reservas e os itinerários do passageiro que permitam às autoridades competentes identificar os passageiros aéreos que representem uma ameaça para a segurança interna."[88]

Caso alguma transportadora aérea se recuse a transferir os dados PNR, os Estados-Membros têm legitimidade para as sancionar.

O tratamento automatizado dos dados PNR não pode prejudicar ninguém, nem nenhuma decisão que advenha desse tratamento deve induzir a uma discriminação em razão de qualquer factor, seja ele sexo, raça, origem étnica ou social. Quer isto dizer que, a aplicação desta Diretiva, deve garantir o respeito pelos direitos fundamentais, pelo direito à privacidade e pelo princípio da proporcionalidade.

Tendo em vista a cooperação policial e judiciária, os Estados-Membros devem partilhar entre si, e com a EUROPOL, os dados PNR que recebem, caso seja necessário para a obtenção de resultados na luta contra o terrorismo e criminalidade organizada, devendo a segurança ser sempre garantida.

Para isso, as UIP devem transmitir sem demora o resultado do tratamento dos dados PNR às UIP de outros Estados-Membros, para efeitos de investigação.

O prazo durante o qual deverão ser conservados os dados PNR deve ser o necessário e proporcional à prossecução dos objetivos de prevenção, detecção, investigação e repressão das infrações terroristas e da criminalidade grave, não podendo exceder um prazo superior a cinco anos.

[88] Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, detecção, investigação e repressão das infrações terroristas e da criminalidade grave.

Para além disso os passageiros são informados quanto ao tratamento dos seus dados pessoais, podendo aqueles aceder, retificar ou apagá-los, tendo, ainda, direito a uma indemnização e direito a recurso judicial, de acordo com a Decisão-Quadro 2008/977/JAI.

Desta forma, é nossa opinião que, ao longo da presente Diretiva, é possível verificar que existe toda uma preocupação no sentido de proteger e salvaguardar os direitos, liberdades e garantias tutelados pela União Europeia.

Quer isto dizer que, apesar da União Europeia ter bem definido quais são os seus objetivos na luta contra a criminalidade, ela nunca descura a importância que o indivíduo tem, tendo sempre em conta a salvaguarda da sua individualidade e o direito à sua vida privada, o que nos leva a concluir que é possível conciliar a existência de uma base de dados PNR na União Europeia sem que se coloquem em risco os direitos fundamentais dos cidadãos.

Capítulo IV

1. Conclusões

Após toda esta reflexão que foi feita sobre o tema e, através da metodologia que foi utilizada, é possível tecermos alguma considerações finais sobre o mesmo.

Como se percebeu, o fenómeno da Globalização, apesar de benéfico em algumas questões, levantou problemas quanto a outras.

O facto de hoje em dia haver uma facilidade nas deslocações, por todo o Mundo, faz com que se levantem uma série de problemas, sendo que, os mais graves e os principais de combater são o terrorismo e a criminalidade organizada transnacional.

Como se referiu, em algum momento desta dissertação, nem todas as viagens que se realizam são de boa fé, havendo algumas cujo objetivo é provocar a instabilidade e a desordem em alguma parte do Mundo.

Desta forma, a criação de uma base de dados PNR revelou-se um grande avanço para a investigação criminal e num contributo para a mesma, no âmbito da União Europeia.

Isto porque, esta base de dados revelou-se uma ferramenta importante, uma vez que permite a identificação de passageiros de alto risco e porque esses dados servirão para a criação de novos perfis, com vista a serem utilizados para investigações futuras ou até em curso.

Para além disso, para esta base de dados não importam informações do foro íntimo dos indivíduos, como a sua origem racial, étnica, as suas opiniões políticas, as suas crenças religiosas ou filosóficas, a sua filiação sindical e vida sexual.

Além do mais, a União Europeia teve o cuidado de celebrar acordos PNR com os EUA, com a Austrália e com o Canadá, de forma a poder alargar a transmissão dessas informações o mais possível, o que garante um combate transnacional contra o terrorismo e a criminalidade organizada.

A nosso ver, os Acordos com a Austrália e com o Canadá asseguram os direitos de todos os cidadãos.

No entanto, o Acordo entre a União Europeia e os EUA, peca no que diz respeito à defesa dos cidadãos nacionais da União Europeia, privando-os de um recurso jurisdicional, quando os mesmos constatarem que os seus dados foram utilizados de uma forma abusiva e lesiva.

É nosso entender, que este Acordo deveria ser revisto e repensado no que diz respeito a estas lacunas, uma vez que os cidadãos da União Europeia que não tenham residência permanente nos Estados Unidos da América encontram-se desprotegidos, sendo obrigação da União Europeia acautelar estas garantias e proteger os seus cidadãos.

Para além disso, este Acordo, em nosso entender, tem, igualmente, de ser revisto no que diz respeito à solidariedade entre todos os Estados-Membros. Isto é, se qualquer cidadão de qualquer Estado-Membro corre o risco de ter um tratamento semelhante ao do Sr. Arar, então todos os Estados-Membros devem ser envolvidos na proteção desse cidadão e agir em solidariedade para proteger todos os cidadãos da União Europeia contra o uso abusivo e prejudicial dos seus dados pessoais.

Outra questão que nos parece ser fundamento para a revisão deste Acordo, são os longos e indeterminados períodos de tempo estabelecidos para o armazenamento dos dados.

Isto porque, tal como foi explicado ao longo desta dissertação, o período de armazenamento dos dados constitui uma questão importante, uma vez que, estipulado esse período é também uma salvaguarda da segurança desses dados.

Pensamos, assim, que quanto à primeira questão da investigação, a que nos propusemos responder, ficou claro sobre qual o contributo que a base de dados PNR trouxe para a investigação criminal no âmbito da União Europeia.

Quanto à segunda questão levantada, dúvidas não restam quanto à possibilidade de conciliar, por um lado, o aumento da segurança no espaço europeu com a proteção dos direitos fundamentais.

Senão vejamos, o que se pode concluir quanto a este ponto.

Em primeiro lugar, ao lidar com as atuais medidas da União Europeia, quanto ao processamento de informações, as autoridades nacionais não devem ter apenas em conta as normas internacionais de proteção dos direitos fundamentais, mas também, devem ter em conta as suas próprias leis constitucionais.

É por isso que, a União Europeia, tornou possível a conciliação do aumento da segurança no espaço europeu com a proteção dos direitos fundamentais, ao estar munida das ferramentas necessárias, por exemplo, quanto à proteção do indivíduo quanto à discriminação, como é o caso da Convenção Internacional sobre a Eliminação de todas as formas de discriminação racial e do artigo 14.º da Convenção Europeia dos Direitos do Homem.

Desta forma, é nossa opinião de que a União Europeia tem todas as condições para proteger os dados que são recolhidos pelas companhias aéreas, como é o caso, da Convenção das Nações Unidas e da já referida Convenção Europeia dos Direitos do Homem.

Para além disso, como se viu, a União Europeia garante a transparência para com os indivíduos, ao informá-los que os seus dados são recolhidos e com que finalidade, garantindo-lhes o acesso à via judicial, em caso de uma utilização abusiva dos seus dados.

Assim, quanto à segunda questão, também ela parece estar devidamente respondida, encontrando-se afastada a ideia de que, havendo uma base de dados como esta, os direitos fundamentais dos indivíduos correm um sério risco de serem violados.

Para além disso, consideramos essencial que, em relação às bases de dados de perfis de ADN, a União Europeia deva reunir esforços para tornar mais organizada a coexistência de várias bases de dados de perfis de ADN, pois parece-nos prejudicial para o indivíduo que este possa ter o seu perfil de ADN inserido em ficheiros de várias bases, sendo numas a título de mero suspeito e noutras como condenado.

A cooperação internacional pode trazer grandes vantagens para a segurança internacional, em áreas como o terrorismo, tráfico de droga, tráfico de seres humanos e muitos outros crimes hediondos.

As futuras abordagens da Comissão para o intercâmbio de dados PNR com países fora da União Europeia terão em conta a necessidade de se aplicarem padrões consistentes e proteções mais específicas na área dos direitos fundamentais, tendo em conta um modelo que estabelecerá os requisitos que os países terceiros terão de cumprir para que possam receber esses dados PNR da União Europeia.

O essencial para que tudo isto dê resultado é o respeito pelo reconhecimento mútuo das decisões judiciais em todos os Estados-Membros da União Europeia.

Assim, a par do que tem vindo a ser proposto pelo Conselho Europeu, parece-nos essencial a regulamentação da utilização dos dados dos registos de identificação dos passageiros, isto é, somos da opinião da criação de um regulamento que abranja todos os Estados da União Europeia, por forma a harmonizar as decisões de todos os Estados-Membros, evitando a incerteza jurídica e as possíveis lacunas em termos de segurança e, ao mesmo tempo, garantindo a proteção dos dados.

Pode-se, então, concluir que a União Europeia está devidamente preparada para ter uma base de dados PNR, tendo os seus objetivos bem definidos na luta contra a criminalidade, salvaguardando sempre a individualidade e os direitos fundamentais dos indivíduo, o que nos leva a concluir que é possível conciliar a existência de uma base de dados PNR na União Europeia, sem que se coloquem em risco os direitos fundamentais dos cidadãos.

Bibliografia

1. Obras Gerais

1.1. Em língua portuguesa

- Albuquerque, Paulo Pinto de, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem,* 3ª Ed. Atualizada, Universidade Católica Ed., 2009 (anotações aos artigos 126º, 127º, 151º a 177º);

- Botelho, Marta Madalena, *Utilização das Técnicas de ADN no Âmbito Jurídico. Em Especial, os Problemas Jurídico-Penais da Criação de Uma Base de Dados de ADN para Fins de Investigação Criminal,* Almedina, Coimbra, 2013;

- Bravo, Jorge dos Reis, *"I- O aprofundamento da cooperação transnacional em matéria de intercâmbio de prova genética; II – A ordem de recolha de amostras em condenados, para análise e inserção na Base de Dados de Perfis de ADN"*, Conselho de Fiscalização da Base de Dados de Perfis de ADN, Coimbra, 2014;

- Bravo, Jorge dos Reis, *"Recolha de amostra, inserção e interconexão de perfis de ADN de arguidos não condenados",* Colóquio "A Lei 5/2008, da 12 de fevereiro, que aprovou a criação da base de dados de perfis de ADN, e a investigação criminal – balanço e perspetivas", Lisboa, 2015;

- Duarte, Maria Luísa, *Estática e Dinâmica da Ordem Jurídica Eurocomunitária*, Volume I, Coimbra: Almedina, Reimp., 2011;

- Gorjão-Henriques, Miguel, *Direito Comunitário,* 5ª Edição, Coimbra: Almedina, 2008;

- Leite, Inês Ferreira, *"A nova base de dados de perfis de ADN",* Boletim Informativo da FDUL-IDPCC, Ano 1, Ed. 5, Outubro-Novembro 2009;

- Miranda, Jorge, *Curso de Direito Internacional Público*, 3ª Edição, Estoril: Princípia Editora, 2006;

- Rodrigues, Benjamim Silva, Da Prova Penal T.1 – *A Prova Científica: Exames, Análises ou Perícias de ADN? Controlo de Velocidade, Álcool e Substâncias Psicotrópicas (à luz do Paradigma da Ponderação Constitucional Codificado em Matéria de Intervenção no Corpo Humano, face ao Direito à Autodeterminação Corporal e à Autodeterminação Informacional Genética), 3ª Ed., revista, actualizada e aumentada, Rei dos Livros, Lisboa, 2010;*

- Silva, Inês T. M. Pedroso da, *"A (i)legitimidade da colheita coerciva de ADN para efeitos de constituição da base de dados genéticos com finalidades de investigação criminal"*, Lex Medicinae – Revista Portuguesa de Direito da Saúde – Ano 7, n.º 15, 2011, pp. 159-188;

- Sousa, Constança Urbano de, Segurança *Versus* Privacidade: Breves notas a propósito do acordo UE-EUA sobre a transmissão de dados PNR (Passenger Name Record), Coimbra: Almedina, 2013;

- Valente, Manuel Monteiro Guedes, *Teoria Geral do Direito Policial*, 4ª Edição, Coimbra: Almedina, 2014.

1.2. Em língua estrangeira

- Papakonstantinou, Vagelis; Hert, Paul de, *"The PNR Agreement and transatlantic anti-terrorism co-operation: no firm Human Rights Framework on either side of the Atlantic", Common Market Law Review, 46, Issue 3,* pp. 885-919, 2009;

- Razak, Adilah Abd, *"Understanding Legal Research"*, in Integration & Dissemination*,* 2009, p. 19 e segs.

2. Coletâneas de Textos

- Oliveira Pais, Sofia, *Direito da União Europeia, Legislação e Jurisprudência Fundamentais*, 2ª Edição, Lisboa: Quid Juris, 2013.

3. Bibliografia específica

- Código Penal;
- Constituição da República Portuguesa;
- U.S Department of Homeland Security and U.S. Customs and Border Protection – *U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy,* 2013;
- ICAO – *Guidelines on Passenger Name Record (PNR) Data* – 2010;
- WCO/IATA/ICAO – *Guidelines on Advance Passenger Information (API)* – 2010.

4. Publicações Periódicas

- Agostinho, Patrícia Naré, "O regime legal da recusa de arguido condenado à recolha de amostra biológica para inserção na base de dados";

- Brouwer, Evelien, "*The EU Passenger Name Record System and Human Rights, Transferring Passenger data or passenger freedom?",* Centre for European Policy Studies, 2009;

- Guild, Elspeth, *"Inquiry into the EU-US Passenger Name Record Agreement",* Centre for European Policy Studies, 2007;

- Nouskalis, G., *"Biometrics, e-Identity, and the Balance between Security and Privacy: Case Study of the Passenger Name Record (PNR) System",* in The Scientific World Journal, 2011.

5. Jurisprudência

- Acórdão *S. & Marper v. Reino Unido,* de 4 de dezembro de 2008;
- Caso Segerstedt-Wiberg and Others v. Sweden. 6 June 2006, no. 62332/00, § 79;
- Acórdão do Tribunal Constitucional n.º 128/92;
- Acórdão do Tribunal Constitucional n.º 288/98;
- Acórdão do Tribunal Constitucional n.º 616/98;
- Acórdão do Tribunal Constitucional n.º 226/2000;
- Acórdão do Tribunal Constitucional n.º 155/2007;
- Acórdão do Tribunal da Relação de Lisboa de 24 de agosto de 2007;
- Acórdão do Tribunal da Relação do Porto de 16 de outubro de 2013;
- Acórdão do Tribunal da Relação do Porto de 10 de dezembro de 2008;
- Acórdão do Tribunal da Relação de Évora, de 13 de dezembro de 2011.

6. Principais sítios na Internet

- Comissão Europeia (www.ec.europa.eu) [consultado em 19/10/2015]: Passenger Name Record (PNR);

- Conselho Europeu (www.consilium.europa.eu) [consultado em 19/10/2015]: Regulamentar a utilização dos dados dos registos de identificação dos passageiros;
- Conselho Europeu (www.consilium.europa.eu) [consultado em 19/10/2015]: Lista UE de terroristas;
- Direção-Geral da Administração Interna (www.dgai.mai.gov.pt) [consultado em 18/05/2016]: Tratado de Prüm;
- Direção-Geral da Administração Interna (www.dgai.mai.gov.pt) [consultado em 18/05/2016]: Cooperação Policial;
- EUR-Lex (www.eur-lex.europa.eu) [consultado em 19/10/2015]: informação direta e gratuita do direito da União Europeia, incluindo a consulta do Jornal Oficial, o acesso ao texto dos Tratados, legislação, jurisprudência e atos preparatórios;
- Ministério da Administração Interna (www.sg.mai.gov.pt): Cooperação Policial e Segurança;

- Parlamento Europeu (www.parleurop.pt): Comunicado de Imprensa;
- Parlamento Europeu (www.parleurop.pt): *EU Passenger Name Record (PNR) proposal: an overview Justice and home affairs* – 26-01-2015;
- Parlamento Europeu (www.europarl.europa.eu): Fichas Técnicas sobre a União Europeia – 2016: Cooperação Judiciária em Matéria Penal;
- Parlamento Europeu (www.europarl.europa.eu) [consultado em 10/05/2016]: Cooperação Policial.

Anexos

ANEXO I

PNR DATA ELEMENTS[89]

An operator's system(s) may include the following data elements:

Data groups or categories	Component data elements
PNR name details	Passenger name, family name, given name/initial, title, other names on PNR
Address details	Contact address, billing address, emergency contact, email address, mailing address, home address, intended address [in State requiring PNR data transfer]
Contact telephone number(s)	[Telephone details]
Any collected API data	Any collected API data, e.g. name on passport, date of birth, sex, nationality, passport number
Frequent flyer information	Frequent flyer account number and elite level status
PNR locator code	File locater number, booking reference and reservation tracking number
Number of passengers on PNR	[Number]
Passenger travel status	Standby information
All date information	PNR creation date, booking date, reservation date, departure date, arrival date, PNR first travel date, PNR last modification date, ticket issue date, "first intended" travel date, date of first arrival [in State requiring PNR data transfer], late booking date for flight
Split/divided PNR information	Multiple passengers on PNR, other passengers on PNR, other PNR reference, single passenger on booking
All ticketing field information	Date of ticket issue/purchase, selling class of travel, issue city, ticket number, one-way ticket, ticket issue city, automatic fare quote (ATFQ) fields

Data groups or categories	Component data elements
All travel itinerary for PNR	PNR flight itinerary segments/ports, itinerary history, origin city/board point, destination city, active itinerary segments, cancelled segments, layover days, flown segments, flight information, flight departure date, board point, arrival port, open segments, alternate routing unknown (ARNK) segments, non-air segments, inbound flight connection details, on-carriage information, confirmation status

[89] Cfr. Guidelines on Passenger Name Record (PNR) Data, International Civil Aviation Organization, 2010, p. A1-1

Form of payment (FOP)	
Information	All FOP (cash, electronic, credit card number and expiry date, prepaid ticket advice (PTA), exchange), details of person/agency paying for ticket, staff rebate codes
All check-in information	Generally available only after flight close-out: check-in security number, check-in agent I.D., check-in time, check-in status, confirmation status, boarding number, boarding indicator, check-in order
All seat information	Seats requested in advance; actual seats only after flight close-out
All baggage information*	Generally available from DCS only after flight close-out: number of bags, bag tag number(s), weightof bag(s), all pooled baggage information, head of pool, number of bags in pool, bag carrier code, bag status, bag destination/offload point
Travel agent information	Travel agency details, name, address, contact details, IATA code
Received-from information	Name of person making the booking
Go-show information*	Generally available only after check-in and flight close-out: go-show identifier
No-show information*	Only available after flight close-out: no-show history
General remarks	All information in general remarks section
Free text/code fields in OSI,	
SSR, SSI, remarks/history	All IATA codes

---

* These elements are contained in the DCS and are not available prior to departure. A recommendation has been made to the World Customs Organization (WCO) to consider incorporating these elements in future API messaging. Depending on the airline system these elements may or may not be part of a PNR.

ANEXO II

MODEL PASSENGER INFORMATION/NOTICE FORMS[90]

FORM A

NOTICE FOR TRAVEL TO [NAME OF DESTINATION STATE]

Under [name of State of departure] law, the [name of destination State's public authority] will either access or receive certain travel and reservation information, known as Passenger Name Record or PNR data, about passengers flying to [name of destination State] from aircraft operators and travel agents.

The [name of destination State's public authority] has undertaken to use these PNR data for such purposes as improving aviation security, enhancing national and border security and preventing and combating terrorism, transnational and organized crimes. The PNR may include information provided during the booking process or held by airlines or travel agents, including credit card details and other similar private financial information.

The information will be retained for no longer than is reasonably necessary for the stated purposes related to its collection and for auditing and redress purposes, in accordance with the law of [name of destination State].

Further information about these arrangements, including measures to safeguard your personal data, can be obtained from your airline or travel agent or [name of destination State's public authority].

[90] Cfr. Guidelines on Passenger Name Record (PNR) Data, International Civil Aviation Organization, 2010, p. A2-1

ANEXO III

FORM B

NOTICE REGARDING PASSENGER NAME RECORD DATA[91]

A growing number of States require airlines to provide access to their records containing certain travel and reservation information, known as Passenger Name Record (PNR) data. The International Civil Aviation Organization (ICAO) has developed guidelines to help States design their requirements and procedures for handling PNR data.

PNR data should be used by States only for such purposes as improving aviation security, enhancing national and border security and preventing and combating terrorism, transnational and organized crimes. PNR data may include information about passengers provided during the booking process or held by airlines or travel agents, including credit card details and other similar private financial information.

PNR data should be retained by State authorities for no longer than is reasonably necessary for the stated purposes related to their collection and for auditing and redress purposes, in accordance with national laws.

Further information about these arrangements, including measures to safeguard your personal data, can be obtained from the relevant national authority or your airline or travel agent.

[91] Cfr. Guidelines on Passenger Name Record (PNR) Data, International Civil Aviation Organization, 2010

ANEXO IV

Data Relating to the Flight (Header data)

Flight Identification

(IATA Airline code and flight number[92])

Scheduled Departure Date

(Date of scheduled departure of aircraft (based on local time of departure location)

Scheduled Departure Time

(Time of scheduled departure of aircraft (based on local time of departure location)

Scheduled Arrival Date

(Date of scheduled arrival of aircraft (based on local time of arrival location)

Scheduled Arrival Time

(Time of scheduled arrival of aircraft (based on local time of arrival location)

Last Place/Port of Call of Aircraft

(Aircraft departed from this last foreign place/port of call to go to "place/port of aircraft initial arrival")

Place/Port of Aircraft Initial Arrival

(Place/port in the country of destination where the aircraft arrives from the "last place/port of call of aircraft")

Subsequent Place/Port of Call within the country

(Subsequent place/port of call within the country)

Number of Passengers

(Total number of passengers on the flight)

[92] Where the aircraft operation is not represented by an IATA airline code (such as a private aircraft movement), then information to be provided for this element will be determined by the implementing authority.

Data Relating to Each Individual Passenger

A) Core Data Elements as may be found in the Machine Readable Zone of the Official Travel Document

- **Official Travel Document Number**
  (Passport or other official travel document number)

- **Issuing State or Organization of the Official Travel Document**
  (Name of the State or Organization responsible for the issuance of the official travel document)

- **Official Travel Document Type**
  (Indicator to identify type of official travel document)

- **Expiration Date of Official Travel Document**
  (Expiration date of the official travel document)

- **Surname/Given Name(s)**
  (Family name and given name(s) of the holder as it appears on the official travel document)

- **Nationality**
  (Nationality of the holder)

- **Date of Birth**
  (Date of birth of the holder)

- **Gender**
  (Gender of the holder)

B) Additional Data elements normally found in Airline systems

- **Seating Information**
  (Specific seat assigned to the passenger for this flight)

- **Baggage Information**
  (Number of checked bags, and where required, the baggage tag numbers associated with each)

- **Traveller's Status**
  (Passenger, Crew, In-transit)

- **Place/Port of Original Embarkation**
  (Place/port where traveller originates foreign travel)

- **Place/Port of Clearance**
  (Place/port where the traveller is cleared by the Border Control Agencies)

- **Place/Port of Onward Foreign Destination**
  (Foreign place/port where traveller is transiting to)

- **Passenger Name Record Locator Number (or unique identifier)**
  (As available in the traveller's Passenger Name Record in the carrier's airline reservation system)

C) Additional data not normally found in Airline systems and which must be collected by, or on behalf of the Airline

- **Visa Number**
  (Number of the Visa issued)

- **Issue Date of the Visa**
  (Date of the Visa issuance)

- **Place of Issuance of the Visa**
  (Name of the place where the Visa was issued)

- **Other Document Number Used for Travel**
  (The other document number used for travel when the official travel document is not required)

- **Type of Other Document used for Travel**
  (Indicator to identify type of document used for travel)

- **Primary Residence**

- **Country of Primary Residence**
  (Country where the traveller resides for the most of the year)

- **Address**
  (Location identification such as street name and number)

- City

- **State/Province/County**
  (Name of the State, Province, County, as appropriate)

- **Postal code**
  (Postal code)

- Destination Address

- **Address**
  (Location identification such as street name and number)
- **City**
  (City)
- **State/Province/County**
  (Name of the State, Province, County, as appropriate)

- **Postal code**
  (Postal code)
- **Place of Birth**

(Place of birth such as city and country)