

FICHA TÉCNICA

Editor:

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Design, Paginação e Produção:

Caixa das Letras Gabinete de Design, Lda.

Fotolitos:

Caixa das Letras Gabinete de Design, Lda.

Impressão e acabamento:

Alves & David Artes Gráficas, Lda.

Tiragem:

500 exemplares

Depósito Legal:

??? ???/06

LISBOA

ÍNDICE

Introdução	9
PARTE I ACTIVIDADE DA CNPD	
Capítulo I Actividade Nacional	13
1. A CNPD em números	13
1.1 Sessões plenárias	13
1.2 Notificações	14
1.3 Queixas	15
1.4 Pedidos de acesso	16
1.5 Averiguações	17
1.6 Inspecções	18
1.7 Aplicação de sanções	18
1.8 Emissão de pareceres	19
1.9 Movimento processual	19
1.10 Pedidos de informação e esclarecimento	20
2. Organização e funcionamento interno	21
2.1 Lei orgânica	21
2.2 Registo público	22
2.3 Notificação electrónica	23
2.4 Sistemas de informação interno	23
2.5 Estágios	24
3. Acção fiscalizadora e de controlo	24
3.1 Auditoria à parte nacional do Sistema de Informação Schengen (N.SIS)	25
3.2 Auditoria aos hospitais	26
4. Áreas específicas de intervenção	26
4.1 Administração Pública (levantamento IGAP/UMIC)	26
4.2 Videovigilância	28
4.3 Dados biométricos	29
4.4 Escolas	31
4.5 Segurança Social	31
4.6 EURO 2004	32
4.7 Experiência de voto electrónico nas eleições europeias	33
5. Actividade institucional	34
5.1 Participação da CNPD na CADA	34
5.2 Audições parlamentares	35

6. Divulgação e transparência	36
6.1 Relacionamento com órgãos de comunicação social	36
6.2 Reestruturação do <i>site</i>	36
6.3 Edições da CNPD	37
6.4 Colóquio comemorativo do 10.º aniversário	37
6.5 Cursos e acções de formação	38
6.6 Participação em seminários	39
7. Avaliações a Portugal	41
7.1 Avaliação do Conselho da UE sobre a aplicação da Convenção de Aplicação do Acordo de Schengen	41
7.2 Avaliação da Comissão Europeia sobre a transposição da Directiva de Protecção de Dados	43
8. Decisões judiciais	44
Estatísticas	47
Capítulo II Actividade internacional	55
1. Representação nas autoridades comuns de controlo	55
1.1 Europol	55
1.2 Schengen	57
1.3 Alfândegas	58
1.4 Eurojust	58
2. Participação em Grupos de Trabalho	59
2.1 Artigo 29.º	59
2.2 Telecomunicações	61
2.3 Queixas	62
3. Cooperação internacional	63
3.1 Encontros ibéricos	63
3.2 Rede CIRCA	64
3.3 Grupo “Spam”	65
3.4 Rede de peritos em TIC	66
3.5 Rede Ibero Americana	66
3.6 Outras actividades	67
4. Participação nas conferências de protecção de dados	68
4.1 Conferência da Primavera	68
4.2 Conferência internacional	69
PARTE II ORIENTAÇÕES DA CNPD	
2003	73
1. Tratamento de dados por parte de partidos políticos	73
2. Tratamento de dados por parte de sindicatos	74

3. Acesso à Base de Dados do Recenseamento Eleitoral	76
a) Por partido político	76
b) Por motivos de saúde pública	79
c) Para processo de inquérito	80
d) Para promoção de eventos culturais	80
e) Para inquérito à população	81
4. Tratamento de dados por parte de entidades públicas e policiais	81
a) Dados relativos a visitantes de reclusos	81
b) Acesso da PJ aos ficheiros da AP Seguradoras	82
c) Introdução de dados no SI Schengen, no âmbito do EURO 2004	83
d) Registo de menores estrangeiros em situação irregular no território nacional	85
5. Tratamento de dados no âmbito laboral	88
a) Código do Trabalho	88
b) Medicina do trabalho antecedentes familiares	90
6. Tratamento de dados no sector da saúde	91
a) Informação genética pessoal	91
b) Testes genéticos	91
c) Dados para investigação científica	93
d) Dados relativos à vida privada	98
e) Carta dos Direitos do Doente Internado	99
f) Acesso a dados clínicos por terceiros	100
7. Tratamento de dados no sector financeiro e de informações de crédito	102
a) Princípio da actualização dos dados	102
b) Exercício do direito de acesso junto do Banco de Portugal	104
c) O consentimento no âmbito de cláusulas contratuais gerais	106
d) Circulação da informação bancária para efeitos de luta contra o branqueamento de capitais e financiamento do terrorismo	109
e) Cedência de dados pessoais	110
f) Concessão de crédito ao consumo	111
g) Gestão de programa de cartões de débito	112
h) Transferências internacionais de dados	114
8. Tratamento de dados no âmbito do marketing	115
a) Perfil de utilizador	115
b) Direito de informação tipo de letra	116
c) Direito de informação e de oposição na Internet	117
d) Código de Conduta do Marketing Directo	117
e) Comunicações electrónicas	119
9. Tratamento do dado “raça”	119
10. Videovigilância em parques naturais	123
11. Tratamento de dados em programas televisivos	126
12. Difusão de dados na Internet	127

2004	129
I Dados sensíveis	129
1. Dados de saúde	129
a) Saúde Escolar	129
b) Acesso a Dados de Saúde	131
2. Dado pessoal “vida privada”	132
a) Videovigilância	132
b) Videovigilância nos estádios	137
c) Autorizações de videovigilância nos estádios	138
d) Videovigilância nas serras	141
e) Videovigilância nas creches	143
f) Tratamento do dado pessoal “imagem”	145
3. Dado pessoal “raça”	146
4. Dado pessoal “filiação sindical”	147
II Tratamento de dados pessoais relativos a órgãos de polícia criminal e a prevenção, investigação e repressão criminal	149
III Dados relativos a situação financeira, ao crédito e à solvabilidade	149
1. Titularização de créditos	149
2. Cobrança de dívidas	151
IV Acesso a dados pessoais constantes de registos públicos e interconexão de dados pessoais	152
1. Acesso a dados pessoais constantes de registos públicos	152
2. Interconexão de dados pessoais	155
V Identificação por rádio frequência, telecomunicações e comércio electrónico	155
VI Fluxos transfronteiriços de dados pessoais	157
1. Comunicação de dados pessoais de adeptos de futebol pela PSP	157
2. Transmissão transfronteiriça de dados pessoais durante o EURO 2004	158
3. Cláusulas contratuais gerais e fluxos transfronteiriços de dados	159
VII Protecção de dados pessoais no local de trabalho	159
1. Utilização da biometria	159
2. Realização de testes de despistagem de droga e de álcool	166
VIII Outras deliberações sobre protecção de dados pessoais	167
1. Dados pessoais tratados pelos condomínios	167

PARTE III DECISÕES DA CNPD

2003	175
1. Deliberações	175
2. Autorizações	184
3. Pareceres	190
2004	195
1. Deliberações	195
2. Autorizações	205
3. Pareceres	231

INTRODUÇÃO

O presente relatório da Comissão Nacional de Protecção de Dados diz respeito ao biénio de 2003/2004.

Este procedimento – que se espera já não ter de reiterar quanto ao ano de 2005 – resultou da opção que houve que tomar, entre a elaboração anual de relatórios (como a lei prevê) e o labor necessário para, sem acréscimo de colaboradores disponíveis, corresponder a um aumento muito apreciável de solicitações vindas do exterior.

Pode dizer-se, com efeito, que no período abrangido por este relatório ocorreu um incremento generalizado de todos e cada um dos tipos de tarefas de que a Comissão está legalmente incumbida.

Na verdade, os órgãos legislativos passaram a solicitar regularmente – como a lei aliás impõe – o parecer da CNPD em relação a diplomas relativos a protecção de dados pessoais.

Nos (raros) casos em que assim não sucedeu isso ficou a dever-se, com grande probabilidade, ao facto de não se ter detectado que os projectos em questão regulavam em parte dados pessoais.

Merece apontar-se, de todo o modo, que não poucas vezes foi pedida a emissão de opinião em prazo demasiado minguado para proferir a formulação de parecer capazmente estudado por parte de um órgão colegial.

Por outro lado, e como normal resultante do melhor conhecimento das obrigações que recaem sobre os responsáveis dos tratamentos de dados, foi progressivamente maior o número de notificações que levaram a Comissão a sobre eles tomar posição.

Por seu turno, foi praticamente explosiva a evolução da quantidade de pedidos de informação e de esclarecimentos de dúvidas – feitos pessoalmente, por telefone ou por e-mail – aumentando muito a pressão sobre os elementos incumbidos desta tarefa.

O ter-se conseguido, mesmo assim, corresponder às solicitações ficou a dever-se a um esforço redobrado dos membros da Comissão – neste período, e por várias vicissitudes, nunca completa – e de todos os seus colaboradores.

No segundo semestre de 2004 ocorreu, porém, um facto que veio proporcionar à Comissão meios que se espera poderem ser decisivos para que ela possa corresponder às exigências acima referidas.

Tratou-se da publicação da Lei n.º 43/2004 de 18 de Agosto, preparada em estreita colaboração entre a CNPD e a Comissão dos Assuntos Constitucionais, Direitos, Liberdades e Garantias, e depois aprovada, em sede parlamentar, com voto de todos os partidos.

Este diploma – previsto há seis anos atrás pela Lei n.º 67/98 – veio pela primeira vez conferir à Comissão uma estrutura orgânica adequada à prossecução das suas atribuições e regular por forma ajustada o seu funcionamento.

Estabeleceu, ademais, um quadro próprio para a CNPD, o que possibilitou enfim a cessação da situação de precariedade em que o seu pessoal se encontrava e veio permitir recrutar mais técnicos juristas e informáticos – para corresponder ao considerável volume de trabalho a que terá de fazer face.

A Lei n.º 43/2004 conferiu ainda à CNPD um melhorado apoio financeiro à sua actividade, ao admitir a cobrança de taxas pelas notificações recebidas – a exemplo, aliás, do praticado em relação à generalidade dos sistemas de registo público.

Mas o segundo ano do biénio ora relatado significou também outro marco na vida da Comissão, simultaneamente para ponderação do seu passado e preparação dum futuro firme e útil para os cidadãos.

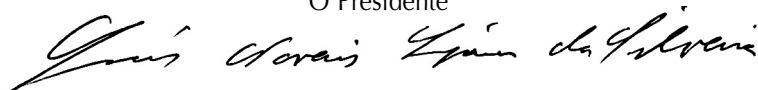
É que em 2004 completou-se a primeira década de existência da CNPD.

Para o comemorar, mas igualmente com vista a aproveitar essa ocasião para traçar as bases de um desejável salto quantitativo, a Comissão organizou um Colóquio, sob o lema “Proteger os Dados Pessoais – Um Desafio Constante” no qual intentou, colhendo opiniões externas de qualificadas personalidades, com base na apreciação desse primeiro decénio de actividade, prever e preparar a resposta às novas e futuras ameaças à integridade dos dados pessoais.

Cabe realçar, aliás, que no biénio compreendido por este relatório a Comissão e os seus membros e colaboradores tiveram de preparar-se, teórica e praticamente, para fazer face a várias evoluções tecnológicas no mundo dos dados pessoais – videovigilância, geolocalização, identificação por radiofrequência.

Este esforço não se operou, claro, isoladamente, mas em estreita cooperação com as demais autoridades de protecção de dados, com as quais a CNPD teve, como habitualmente, oportunidade de se reunir com regularidade no seio de diversas instâncias comunitárias e internacionais.

O Presidente



P A R T E I
ACTIVIDADE
DA CNPD

CAPÍTULO I

ACTIVIDADE NACIONAL

1. A CNPD em números

Embora os dados estatísticos não esgotem, de maneira nenhuma, a esfera de acção da CNPD e não abarquem muito do trabalho desenvolvido que dificilmente pode ser mensurável do ponto de vista numérico, eles ajudam-nos, sem dúvida, a ter uma melhor percepção da realidade dos últimos dois anos e da evolução da actividade da Comissão.

De uma maneira geral, podemos afirmar que, em **2003** e **2004**, se consolidou a tendência de subida verificada no biénio anterior, relativamente ao número de tratamentos de dados notificados à CNPD, bem como um aumento significativo do número de solicitações telefónicas e escritas dirigidas à Comissão por cidadãos, empresas e organismos públicos. Foi igualmente visível um acréscimo de pedidos de esclarecimento por parte de empresas estrangeiras que pretendem tratar dados em Portugal.

Em relação ao conjunto do movimento processual, é de assinalar que a CNPD conseguiu, pela primeira vez, em **2004**, inverter a tendência de aumento de pendências que acompanhava o aumento de entrada de processos, conseguindo finalizar maior número de processos do que os entrados. Este foi o resultado notório de algumas medidas concretas de organização interna empreendidas em 2001/2002, que levaram a um empenho acrescido de toda a Comissão, e que começaram a dar os seus frutos.

1.1 Sessões plenárias

A CNPD reúne-se regularmente em sessão plenária para apreciar e votar as propostas de decisão relativamente a cada um dos processos agendados – autorizações, queixas, pareceres, averiguações, pedidos de acesso a dados pessoais por parte de terceiros, contra-ordenações –, bem como para debater as áreas temáticas que se

considera merecerem, em cada momento, maior reflexão e uma tomada de posição por parte da Comissão, designadamente interpretação da lei, a aplicação de novas tecnologias e as suas incidências ao nível da privacidade, a perspectiva da CNPD nas discussões dos fóruns comunitários e internacionais.

Nas reuniões colegiais, é ainda tratado um conjunto amplo de questões relativas ao funcionamento interno e à participação da CNPD em várias iniciativas.

Também a este nível, resultando do ritmo de trabalho crescente, a CNPD reuniu-se mais nos últimos dois anos, tendo realizado 35 sessões plenárias em **2003** e 38 sessões plenárias em **2004**.

Nessas sessões, foi aprovado em **2003** um total de 1026 decisões, o que praticamente duplicou o número de decisões (520) emitidas pela Comissão em 2002. Em **2004**, o número de decisões continuou a aumentar, tendo a CNPD aprovado, em plenário, 1560 decisões (1). Destas decisões, 718 e 1341 correspondem a autorizações prévias de tratamentos de dados pessoais, aprovadas respectivamente em **2003** e **2004**, o que significa um aumento da emissão de autorizações superior a 85 por cento.

1.2 Notificações

A notificação de tratamentos de dados pessoais à CNPD, obrigatória nos termos do artigo 27.º da Lei de Protecção de Dados, registou um aumento muito acentuado em **2003**, tendo atingido uma cifra recorde acima das 2 mil notificações, para em **2004** se situar de novo abaixo desse número, mas continuando a tendência de crescimento relativamente a 2002.

Assim, em **2003**, foram notificados à Comissão 2197 tratamentos de dados, o que representa um acréscimo de quase 50 por cento em relação ao ano anterior. Em **2004**, foram notificados 1606 tratamentos de dados.

O sector da saúde é responsável por cerca de 43 por cento do total de notificações feitas à Comissão, no ano de **2003**, enquanto no ano de **2004**, é o sector dos serviços o que tem mais preponderância com quase 20 por cento das notificações.

(1) Nestas decisões, não se incluem os processos relativos a tratamentos de dados que não estão sujeitos a autorização prévia da CNPD e que, internamente, designamos por registos. Os processos de registo são despachados sem a aprovação em sessão plenária.

Mantendo aliás a tendência dos últimos anos, do total de notificações feitas à CNPD, cerca de 2/3 dizem respeito a tratamentos de dados que carecem de autorização prévia da Comissão. Deste modo, deram entrada na Comissão, 1582 pedidos de autorização, em **2003**, enquanto foram feitos 1127 pedidos de autorização de tratamento de dados, em **2004**.

Convém sublinhar que entre as notificações que estão sujeitas a autorização prévia da CNPD se encontram os tratamentos de dados através de videovigilância. Em 2001 e 2002, as notificações de sistemas de videovigilância já representavam mais de 30 por cento do volume total de pedidos de autorização prévia para o tratamento de dados pessoais. Em **2003**, verificou-se um ligeiro abrandamento, com 357 notificações, quer em termos absolutos, quer em termos percentuais, representando as videovigilâncias cerca de 20 por cento.

No entanto, em **2004**, as notificações da utilização de videovigilância elevaram-se a 655, representando mais de metade do número total de pedidos de autorização do tratamento de dados pessoais, entrados no ano passado na CNPD.

No que diz respeito às notificações de tratamentos de dados que não carecem de autorização prévia, designadas por registos, verificou-se igualmente um acréscimo nos últimos dois anos, tendo dado entrada 615 notificações em **2003** e 479 em **2004**.

Desde a entrada em funcionamento da Comissão, em 1994, até ao final do ano de 2004, foram notificados no total quase 10 mil tratamentos de dados pessoais. Do conjunto das notificações (9975), cerca de 30 por cento dizem respeito ao sector público (2859) e 70 por cento ao sector privado (7116).

Ainda no âmbito das notificações, a diferença entre tratamentos de dados que não carecem de autorização prévia e os que carecem de controlo prévio é praticamente irrelevante, repartindo-se por 4788 registos e 5187 autorizações. Valerá a pena notar que no sector público, há uma maior incidência de notificações que não requerem autorização prévia, enquanto no sector privado, o número de notificações que exigem autorização é superior.

1.3 Queixas

Em matéria de queixas, registou-se uma ligeira subida em **2003** com a apresentação de 173 queixas, contra 162 do ano anterior. Já em **2004**, o número de queixas desceu, tendo dado entrada na Comissão 156 processos de queixa.

As matérias sobre as quais recaem as queixas são variadas, apesar de as queixas contra entidades financeiras por falta de actualização dos dados representarem ainda cerca de 26 por cento do total de queixas apresentadas. Contudo, o número destas queixas continua a descer: em **2003**, foram feitas 45 queixas e, em **2004**, 40.

Quanto às queixas relativas às comunicações electrónicas não solicitadas (*spam*) para fins de marketing, bem como relacionadas com o sector das telecomunicações há uma clara tendência de subida, representando já uma percentagem na ordem dos 30 por cento. Verifica-se também que, a par do correio electrónico, há uma tendência para as mensagens não solicitadas serem enviadas por SMS sem o consentimento do titular dos dados e, ainda, para a realização de marketing por telefone em circunstâncias violadoras da lei.

Por outro lado, começaram nos últimos dois anos a aparecer algumas queixas relativas à utilização de videovigilância.

1.4 Pedidos de acesso

A CNPD pronuncia-se também sobre os pedidos de acesso a dados pessoais pelo próprio titular, quando o exercício do direito de acesso é exercido, não directamente junto do responsável do tratamento de dados, mas através da CNPD, que é designadamente o que acontece quando se trata de dados de natureza policial.

Nesta situação, estão os pedidos de acesso ao Sistema de Informação Schengen, por força do disposto na Lei 2/94, de 19 de Fevereiro, que atribui à Comissão essa competência.

Assim, são dirigidos à CNPD todos os pedidos de acesso por parte do titular dos dados ao SI Schengen, bem como os pedidos de rectificação ou de eliminação. A CNPD, feitas as diligências e verificações necessárias, responde aos requerentes.

Em **2003**, foram apresentados 36 pedidos de acesso a Schengen, enquanto em **2004** entraram 21 pedidos.

A CNPD aprecia, por outro lado, o pedido de acesso a dados pessoais de terceiros. As situações mais frequentes prendem-se com o acesso a dados de saúde de outrem ou o acesso à Base de Dados do Recenseamento Eleitoral (BDRE).

Em resultado do elevadíssimo número deste tipo de pedidos de acesso, a CNPD elaborou, em 2001, duas deliberações gerais, com os princípios aplicáveis aos casos concretos mais comuns ⁽²⁾, tendo-as difundido junto das entidades que tratam os dados em causa – hospitais e STAPE – e a quem habitualmente é solicitado primeiro o acesso. Deste modo, pretendeu-se habilitar os responsáveis dos tratamentos a responder, de acordo com a lei, à maioria dos pedidos, sem necessidade de os submeter individualmente à CNPD. Só casos mais específicos e que colocam dúvidas na aplicação das orientações gerais da Comissão e na interpretação da lei são dirigidos à CNPD.

Deste modo, foi possível reduzir substancialmente o número de pedidos de acesso, diminuindo também o tempo de resposta aos requerentes.

Assim, em **2003** e **2004**, houve um decréscimo muito notório do número de pedidos de acesso a dados de terceiros, tendo-se contabilizado 22 e 27 respectivamente, contra 177 pedidos em 2002.

1.5 Averiguações

Nos últimos dois anos, a CNPD decidiu abrir mais processos de averiguação, quanto a situações que chegam ao nosso conhecimento, passíveis de configurar violações da lei em matéria de protecção de dados, e que só uma verificação *in loco* pode determinar se efectivamente ocorrem.

A CNPD, no âmbito das suas competências, pode levar a cabo averiguações por sua iniciativa e que, no fundo, se inscrevem nos seus poderes de autoridade de controlo. Os processos de averiguação são instaurados, de uma maneira geral, no seguimento de notícias veiculadas pelos órgãos de comunicação social ou em informações ou alertas que os cidadãos cada vez mais nos comunicam, demonstrando ter uma maior consciência dos direitos e garantias que lhes assistem e do que eventualmente pode não estar correcto numa determinada situação.

De facto, em **2003**, a Comissão deliberou abrir 40 processos de averiguação, mais 12 do que em 2002, enquanto em **2004**, foram abertas 35 averiguações.

(2) Deliberação 51/2001 sobre acesso a dados de saúde, disponível para consulta em <http://www.cnpd.pt/bin/decisoes/2001/htm/del/del051-01.htm> e Parecer 22/2001 sobre o acesso à BDRE, em <http://www.cnpd.pt/bin/decisoes/2001/htm/par/par022-01.htm>

1.6 Inspeções

Ao nível das acções de inspecção, decorrentes de queixas ou averiguações, a CNPD realizou em **2003** e **2004** cerca de 300 fiscalizações no local, em todo o território nacional, embora na zona da Grande Lisboa se tenham registado aproximadamente 70 por cento do total das inspecções.

Das acções de inspecção levadas a cabo, aproximadamente 80 por cento foram efectuadas a entidades privadas, tendo-se registado um aumento do número de fiscalizações no sector público relativamente aos anos anteriores.

Relativamente ao biénio anterior, houve um decréscimo do número de acções de fiscalização, que se ficou a dever, por um lado, a uma diminuição do pessoal nesta área e, por outro, à necessidade de afectar recursos ao desenvolvimento de aplicações informáticas internas, sem custos financeiros acrescidos, com vista a permitir no futuro uma melhor gestão ao nível processual, bem como uma maior eficácia dos serviços.

1.7 Aplicação de sanções

Em **2003** e **2004**, a CNPD aplicou cerca de 150 coimas, no âmbito de processos de contra-ordenação, que perfizeram um montante de aproximadamente 90 mil euros.

A aplicação de coimas, prevista no regime sancionatório da Lei de Protecção de Dados, resultou, na maioria dos casos, de falta de notificação de tratamento de dados e do incumprimento dos direitos de informação, de acesso e de oposição.

O valor da coima varia em função da infracção cometida, da natureza dos dados e do tipo de entidade que violou a lei. No entanto, na maior parte das situações, é possível ao infractor requerer o pagamento voluntário da coima, sendo desse modo pago o montante mínimo previsto no respectivo articulado legal.

Decorre também do regime sancionatório da Lei de Protecção de Dados a participação ao Ministério Público, quando estiver em causa uma violação da lei que seja enquadrada na prática de crime. Em **2003**, a CNPD fez uma denúncia ao MP.

1.8 Emissão de pareceres

A CNPD deve ser chamada a emitir parecer, não vinculativo, sobre quaisquer disposições legais nacionais e sobre instrumentos jurídicos em preparação nas instituições comunitárias e internacionais, relativos ao tratamento de dados pessoais, tal como decorre da Lei 67/98 – Lei de Protecção de Dados.

Deste modo, os projectos de diploma que contenham matérias de protecção de dados, sejam eles da iniciativa da Assembleia da República, do Governo ou dos órgãos regionais competentes devem ser submetidos à Comissão para a emissão do necessário parecer.

Embora a lei não determine em que fase do processo legislativo deve ser solicitado o parecer da Comissão, a verdade é que a eficácia de tal parecer depende da sua emissão prévia à aprovação do diploma, de modo a que possa ser tido em conta na redacção final do projecto.

Apesar dos inúmeros alertas da CNPD para esse facto, por vezes, isso não tem acontecido; outras vezes, não chega sequer a ser pedido o parecer da Comissão. Apesar da complexidade de muitas das questões que nos são apresentadas, a CNPD sempre respondeu prioritária e atempadamente aos pedidos que nos são submetidos, tendo a consciência da necessidade de um célere processo legislativo. Tal não invalida, todavia, que os pedidos de parecer venham, na maioria das vezes, com pedidos de urgência que apontam para prazos muito diminutos, alguns inferiores a uma semana.

No entanto, é de assinalar que, nos últimos dois anos, houve um aumento muito relevante do número de pareceres solicitados à Comissão, tendo a CNPD emitido 52 pareceres em **2003**, e 42 pareceres em **2004**. A maioria das solicitações proveio do Governo, com uma maior incidência do Ministério da Justiça, do Ministério da Saúde, do Ministério das Finanças e do Ministério dos Negócios Estrangeiros. A Assembleia da República apresentou nestes dois anos 18 pedidos de parecer e o Governo Regional dos Açores solicitou 2 pedidos.

1.9 Movimento processual

Em **2003** e **2004**, acentuou-se o aumento do movimento processual, tendência iniciada nos dois anos anteriores. Assim, de 2002 para **2003**, registou-se um acréscimo

de cerca de 43 por cento no número de processos entrados na Comissão. Os processos correspondem a notificações de tratamentos de dados, a queixas, a pedidos de acesso, a averiguações e a pedidos de parecer.

Em **2003**, com efeito, deu-se um recorde de entradas de processo, com a abertura de 2641 novos processos, enquanto em **2004** houve um ligeiro abrandamento, com 2040 processos entrados, mas ainda assim acima da fasquia dos dois milhares.

A assinalar que, pela primeira vez, e apesar do aumento substancial de novos processos, a CNPD conseguiu em **2004** resolver e finalizar mais processos do que aqueles entrados. De facto, a Comissão passou de 1456 processos findos e arquivados em **2003** para 2756 em **2004**, o que representa um aumento da resolução de processos superior a 90 por cento.

A diminuição significativa de pendências acumuladas em 2000 e 2001 resultou, sem dúvida, de um esforço interno acrescido e de uma reorganização dos serviços, com reforço dos recursos humanos, de modo a permitir fazer face ao aumento do volume processual.

1.10 Pedidos de informação e esclarecimento

Nos anos de **2003** e **2004**, os pedidos de informação e esclarecimento, dirigidos à Comissão, por escrito, registaram um crescimento assinalável, tendo passado de cerca de 400 em 2002 para 1233 em **2003** e 1582 em **2004**.

Estes dados estatísticos apenas dizem respeito aos pedidos chegados por correio electrónico, que são a grande maioria, por fax ou por correio postal. Contudo, os pedidos de esclarecimento por via telefónica também aumentaram substancialmente, sendo, por isso mesmo, difícil, fazer um registo estatístico deste tipo de solicitações.

É de salientar que as questões colocadas, seja pelos cidadãos, seja pelas empresas, nomeadamente através de advogados, seja por associações são cada vez mais complexas e exigem frequentemente uma resposta mais elaborada e a procura de legislação específica que é necessário compatibilizar com a Lei de Protecção de Dados. De notar ainda que vai subindo o número de pedidos de informação provenientes do estrangeiro, em particular de empresas multinacionais.

O recurso crescente à CNPD para obter informações sobre protecção de dados e privacidade em geral demonstra, sem dúvida, um continuado despertar para estes novos direitos, bem como um maior conhecimento destas matérias, que resulta numa busca de informação mais exigente.

Apesar do esforço suplementar que tal impõe, tendo em conta os recursos humanos disponíveis, é com muito agrado que a CNPD verifica que, de ano para ano, quer as empresas (enquanto responsáveis de tratamento), quer os cidadãos (enquanto titulares dos dados) vão integrando a protecção de dados nas suas vidas profissionais e pessoais.

2. Organização e funcionamento interno

2.1 Lei orgânica

A CNPD vinha, há seis anos – desde a publicação da Lei n.º 67/98 – a funcionar sem estrutura interna definida e, porque desprovida de quadro de pessoal, apoiada por colaboradores todos eles admitidos a título precário.

Esta situação era claramente indesejável e não proporcionava aos trabalhadores da Comissão um mínimo de estabilidade indispensável à necessária segurança no emprego.

Por isso a CNPD vinha, há anos, a apresentar à Assembleia da República sucessivos ante-projectos da lei orgânica prevista na Lei de Protecção de Dados Pessoais.

Esses textos levaram um grupo de deputados da maioria parlamentar – PSD – CDS/PP – a apresentar formalmente, em 26 de Março de 2004, o Projecto de Lei Orgânica n.º 425/IX, acompanhado dum projecto de resolução relativo ao quadro da instituição.

Este Projecto de Lei foi objecto de apreciação e discussão na Comissão dos Assuntos Constitucionais, Direitos, Liberdades e Garantias, que para o efeito suscitou algumas audições da CNPD.

A referida Comissão Parlamentar emitiu parecer sobre o Projecto em causa em 17 de Junho de 2004.

Foi, a final, publicada, em 18 de Agosto de 2004, a Lei n.º 43/2004 – Lei de organização e funcionamento da Comissão Nacional de Protecção de Dados.

Esta lei veio a ser complementada pela Resolução da Assembleia da República n.º 59/2004, de 19 de Agosto.

A Lei n.º 43/2004 define, enfim, a estrutura interna da CNPD, através da instituição dos seus serviços de apoio e respectivas competências.

Atribuiu ainda receitas próprias à Comissão, permitindo-lhe cobrar taxas pelos actos de registo e conexos de que está incumbida.

E consagrou o regime de disponibilidade permanente do seu pessoal, com a correspondente compensação remuneratória.

A publicação do quadro de pessoal, através da Resolução n.º 59/2004, proporcionou a esperada segurança aos respectivos colaboradores, imprescindível para a estabilidade laboral destes e para a normal programação das actividades da CNPD.

2.2 Registo Público

O artigo 31.º da Lei de Protecção de Dados dispõe que os tratamentos de dados pessoais notificados e devidamente autorizados pela CNPD devem constar de um registo, aberto à consulta de qualquer pessoa.

Esse registo deverá conter o nome do responsável pelo tratamento de dados ou do seu representante, as categorias de dados tratados, as finalidades do tratamento, as categorias dos destinatários, as formas do exercício do direito de acesso e de rectificação e as transferências de dados para países terceiros.

Essa informação estava pois acessível a qualquer pessoa que a solicitasse, tendo para o efeito que o fazer junto da Comissão, mas apenas em suporte de papel.

O registo público assume especial importância como um meio de publicitar os tratamentos de dados pessoais autorizados, contribuindo para uma maior transparência da actuação dos responsáveis e da própria Comissão. Além disso, facilita a verificação por parte de qualquer pessoa ou entidade do cumprimento da lei.

A CNPD considerou, por isso, que seria desejável tornar o registo público de mais fácil acesso e consulta, colocando-o disponível no *site* da Comissão. Para tal, a

CNPD desenvolveu internamente, em **2003** e **2004**, um programa informático para o registo público e iniciou a introdução dos dados desde 1994.

Actualmente, o registo público já está disponível para consulta *on line* ⁽³⁾, embora ainda não se encontre completamente actualizado, pois ainda se está a finalizar o processo de inserção de dados. O registo é um instrumento que está em permanente actualização, devido às alterações feitas a tratamentos já autorizados e aos novos tratamentos legalizados na Comissão. Com a futura entrada em funcionamento da notificação electrónica, a actualização do registo público passará a ser praticamente automática.

2.3 Notificação electrónica

A necessidade de agilizar o procedimento de notificação à Comissão, facilitando simultaneamente o preenchimento do respectivo formulário, aliada à vantagem de reduzir progressivamente a utilização do papel foram as razões que levaram a CNPD a decidir avançar para a notificação dos tratamentos de dados por via electrónica.

Assim, em **2003** e **2004**, a Comissão, recorrendo exclusivamente ao seu pessoal informático, criou um formulário electrónico de notificação, que irá estar também disponível no *site* da CNPD e poderá ser enviado *on line*.

Este novo formulário permitirá um preenchimento mais fácil e mais correcto da notificação, melhorando conseqüentemente a sua apreciação e evitando demoras a solicitar informação adicional. Por outro lado, para as empresas ou organismos públicos que têm vários tratamentos de dados, poderão ter sempre em formato electrónico um histórico dos tratamentos notificados e solicitar as alterações necessárias com muito mais facilidade.

2.4 Sistema de informação interno

O sistema de informação interno da Comissão, que faz toda a gestão administrativa processual, é uma pedra basilar da notificação electrónica e do registo público. Para que a notificação electrónica pudesse, de facto, diminuir eficazmente a circulação

(3) <http://www.cnpd.pt/bin/registo/registo.htm>

de papel, foi necessário proceder a uma reformulação profunda do sistema de informação interno. Do mesmo modo, o registo público para ser actualizado automaticamente está dependente do funcionamento deste circuito.

Por outro lado, o novo sistema de informação foi aperfeiçoado, no sentido de responder melhor às exigências do trabalho da Comissão, com base na experiência adquirida ao longo dos anos.

A Comissão decidiu, assim, reestruturar, em **2003** e **2004**, o seu sistema de informação interno, que se encontra neste momento já em fase de testes. A sua entrada em funcionamento irá permitir o arranque da notificação electrónica.

2.5 Estágios

Em **2004**, em acordo com a Associação de Estudantes da Faculdade de Direito da Universidade Nova de Lisboa, a Comissão iniciou um programa de estágios não remunerados, destinados a estudantes dos últimos anos do curso daquela faculdade.

Tratou-se de estágios trimestrais e de estágios de Verão, que possibilitaram aos estudantes de Direito tomar contacto com as matérias de protecção de dados e aumentar os seus conhecimentos neste campo.

Sendo o regime de estágio voluntário e não integrando qualquer plano curricular, foi com agrado que verificámos que houve mais candidaturas ao estágio na Comissão do que aquelas que poderíamos satisfazer. O eco que recebemos dos estudantes estagiários que entretanto entraram no mercado de trabalho foi muito positivo, na medida em que o período de estágio na CNPD foi considerado uma mais-valia.

Esta é, indiscutivelmente, uma vertente importante na formação de futuros juristas, magistrados e advogados e insere-se na actividade da CNPD de sensibilizar e divulgar as questões sobre protecção de dados pessoais e privacidade, em particular junto de todos aqueles que se cruzam nas suas vidas profissionais, mais tarde ou mais cedo, com estas matérias.

3. Acção fiscalizadora e de controlo

A actividade fiscalizadora e de controlo da CNPD não se esgota nas acções de inspecção, realizadas no âmbito de processos concretos de averiguação ou de queixa,

e que resultam, na maior parte dos casos, numa atitude punitiva por parte da Comissão.

É da máxima importância ir aferindo, de forma mais sectorial, do nível de cumprimento das disposições de protecção de dados, para tentar não só ter uma melhor percepção da realidade, mas também encontrar soluções abrangentes que contribuam para colmatar as eventuais falhas detectadas, nomeadamente através da emissão de recomendações.

Assim sendo, a CNPD empreendeu nos últimos dois anos auditorias de grande envergadura, em áreas completamente distintas, mas ambas relativas ao tratamento de dados sensíveis e, conseqüentemente, especialmente protegidos por lei: por um lado, dados pessoais de natureza policial; e, por outro, dados de saúde e relativos à vida privada.

3.1 Auditoria à parte nacional do Sistema de Informação Schengen (N.SIS)

A CNPD, enquanto autoridade nacional de controlo de protecção de dados pessoais, para efeitos do Sistema de Informação Schengen (SIS) ⁽⁴⁾, tem como competência a verificação de todas as condições de funcionamento da parte nacional do SIS, nomeadamente em termos de segurança física e lógica.

No passado, a Comissão já tinha realizado duas acções de fiscalização, com objectivos mais específicos, ao sistema. No entanto, em **2003**, a CNPD decidiu encetar uma auditoria mais vasta e, paralelamente, mais aprofundada ao N.SIS., que decorreu durante meses.

Deste modo, a Comissão inspeccionou todas as entidades que acedem ao SIS – Serviço de Estrangeiros e Fronteiras, Gabinete SIRENE, PJ, PSP, GNR, Serviços Consulares – verificando designadamente os procedimentos internos, as medidas de segurança, o registo e controlo de acessos, os prazos de conservação dos dados, os ficheiros manuais.

Foram feitas algumas recomendações e do relatório final da auditoria foi dado conhecimento ao Ministro da Administração Interna e a todos os responsáveis pelos respectivos serviços.

⁽⁴⁾ Devido à igualdade da sigla, o Sistema de Informação Schengen (SIS) é, por vezes, confundido com o Serviço de Informação e Segurança (SIS), sendo coisas distintas.

3.2 Auditoria aos hospitais

Em **2004**, a CNPD empreendeu uma auditoria nacional aos hospitais, com vista a verificar como era tratada a informação de saúde, quer informatizada, quer em suporte de papel, nestes estabelecimentos de saúde e se os direitos dos doentes estavam garantidos.

Em particular, a Comissão pretendia conhecer o nível de informatização dos dados de saúde e as medidas de segurança existentes, a organização dos arquivos clínicos, como era feita a circulação da informação clínica internamente, como se processavam a vários níveis os acessos à informação de saúde e a outra informação pessoal de natureza sensível, os procedimentos relativos ao pedido e consulta de resultados de análises e outros meios auxiliares de diagnóstico, bem como a utilização de dados de saúde para fins de investigação científica. Foram também verificadas as experiências de telemedicina e os sistemas de videovigilância existentes nos hospitais.

Esta acção de auditoria decorreu, ao longo de vários meses, em 38 hospitais, públicos e privados, abrangendo 15 distritos do continente e regiões autónomas. Foi elaborado um relatório de auditoria⁽⁵⁾, cujas conclusões e recomendações foram remetidas aos estabelecimentos hospitalares e a um vasto conjunto de entidades, designadamente ao Presidente da República, à Assembleia da República, ao Ministério da Saúde, à Ordem dos Médicos e à Ordem dos Enfermeiros.

4. Áreas específicas de intervenção

4.1 Administração Pública

A administração pública tem sido, nos últimos anos, uma área privilegiada da intervenção da Comissão, no sentido da regularização e cumprimento das disposições de protecção de dados pelos organismos públicos.

A prossecução do interesse público que a administração pública visa, o princípio constitucional da legalidade a que está submetida e o princípio da transparência com

⁽⁵⁾ O relatório está disponível em <http://www.cnpd.pt/bin/relatorios/outros/outros.htm>

que deve actuar só por si justificam esta preocupação da CNPD, que tem procurado sempre sensibilizar as tutelas para esta matéria.

Deste modo, por despacho ministerial, iniciou-se no final de 2000, através da Inspeção-geral da Administração Pública (IGAP), com a colaboração estreita da CNPD, um levantamento exaustivo dos tratamentos de dados efectuados por entidades públicas. Foi enviado um inquérito a cerca de 950 entidades da administração pública central e institutos públicos nas modalidades de serviços ou de fundos públicos. Os resultados do inquérito foram remetidos à Comissão.

Em Março de 2002, a Comissão procedeu à análise dos resultados, tendo verificado que 21 por cento das entidades não tinham respondido ao inquérito, 30 por cento referiram proceder ao tratamento de dados pessoais e 49 por cento responderam não realizar tratamento de dados. Das entidades que responderam tratar dados pessoais, só 16,5 por cento tinham os seus tratamentos de dados devidamente legalizados junto da CNPD.

Foi então deliberado contactar directamente as entidades que não tinham respondido ao inquérito, oficiar aquelas que afirmaram ter tratamentos de dados enviando-lhes o respectivo formulário de notificação para preenchimento e levar a cabo fiscalizações aleatórias aos serviços que declararam não proceder ao tratamento de dados.

Depois de concluídas estas diligências, a CNPD fez, em Fevereiro de **2003**, um balanço de todo o processo de legalização de tratamento de dados da administração pública, cujos resultados foram comunicados à IGAP e à Assembleia da República. Nesse relatório, a Comissão considerou que os resultados obtidos, embora não “consoladores”, eram de uma maneira geral satisfatórios: o nível de regularização de tratamentos de dados pessoais na administração pública tinha aumentado significativamente.

Com efeito, ao longo de **2003** e de **2004**, essa tendência acentuou-se e verificou-se a notificação à Comissão de centenas de tratamentos de dados. Assim, no final de **2004**, já tinham sido notificados quase 3 mil tratamentos de dados pessoais ⁽⁶⁾.

⁽⁶⁾ Este número de notificações abrange também a administração local, não incluída no processo de legalização mencionado.

Ainda no plano da administração pública, a CNPD reuniu-se, em Janeiro de **2004**, com a UMIC, no âmbito do Plano de Acção para a Sociedade de Informação, no qual se prevê a articulação das duas entidades para a criação da política nacional de protecção da privacidade na utilização de sítios de serviços públicos.

Foram ainda realizadas outras duas reuniões com a UMIC, para acompanhamento do processo de legalização do Portal do Cidadão e da criação da Central de Compras do Estado, por via electrónica.

4.2 Videovigilância

A utilização de sistemas de videovigilância tem-se generalizado muito nos últimos anos, no nosso país, como o pode bem atestar o número crescente de notificações que a CNPD tem recebido, e que de **2003** para **2004** quase duplicou.

A protecção de pessoas e bens é, sem dúvida, a finalidade mais declarada no recurso a estes sistemas, embora a Comissão tenha apreciado também outras situações mais específicas. É também notório que a videovigilância deixou de ser utilizada quase exclusivamente por grandes empresas ou instituições para se estender ao pequeno comércio, aos consultórios, aos condomínios, às escolas e, ainda, às casas particulares.

Este fenómeno tem suscitado, por outro lado, vários pedidos de informação e esclarecimento por parte de empresas, que pretendem instalar equipamentos de videovigilância; de cidadãos, preocupados com a legalidade da utilização destes sistemas; de sindicatos, quanto à presença de câmaras nos locais de trabalho; e até da comunicação social, atenta a esta nova realidade.

O número de queixas apresentadas à CNPD sobre o uso de sistemas de videovigilância também vai ganhando relevo, contabilizando-se já 44 queixas. O número de processos de contra-ordenação e de averiguação ronda a centena.

A videovigilância tornou-se, pois, numa área central da actividade da Comissão, que, em **2004**, aprovou um conjunto de princípios gerais aplicáveis ao tratamento de dados pessoais através de videovigilância ⁽⁷⁾.

(7) <http://www.cnpd.pt/bin/orientacoes/principiosvideo.htm>

Estes princípios, que seguem de perto as orientações sobre esta matéria aprovadas no Grupo de Protecção de Dados da União Europeia, permitiram enunciar algumas situações padrão com que a CNPD mais se defronta, definir critérios uniformes de apreciação dos casos e determinar as condições específicas em que os sistemas de videovigilância podem funcionar.

Esta deliberação genérica permitiu, ainda, recuperar mais depressa pendências entretanto acumuladas relativas aos processos de autorização de videovigilância, na sequência da declaração de inconstitucionalidade, em 2002, por parte do Tribunal Constitucional ⁽⁸⁾ do diploma que regulava a utilização da maior parte dos sistemas de videovigilância.

Tendo o Tribunal Constitucional considerado ser a videovigilância “*uma limitação ou uma restrição do direito à reserva da intimidade da vida privada*” – o que, aliás, sempre tinha sido o entendimento da Comissão – a questão da videovigilância assume uma redobrada importância, na medida em que fica abrangida pelo elenco de dados sensíveis, logo, detentora de especial protecção por parte da lei.

A progressiva massificação destes sistemas não deve conduzir a uma diminuição do grau de protecção devido, sob risco de capitulação de um direito fundamental. Mesmo quando em confronto com outros direitos fundamentais, em particular o direito à segurança, que domina a agenda actual, exige-se uma constante ponderação de valores e aferição das vantagens reais do uso de videovigilância e o estudo de meios alternativos menos intrusivos.

4.3 Dados biométricos

O tratamento de dados pessoais com recurso aos sistemas biométricos foi uma área específica de intervenção da CNPD em **2003**: por um lado, tratava-se de uma tecnologia relativamente nova, disponível no mercado para qualquer um e acessível em termos de custos, pelo que foi facilmente difundida; por outro lado, levantou sérias preocupações e reservas aos cidadãos, a quem era exigida a cedência da impressão digital ou a leitura da íris.

⁽⁸⁾ Pode consultar o acórdão n.º 255/02 do TC em <http://www.cnpd.pt/bin/legis/juris/TC255-02-vvg.htm>

A primeira notificação de dados biométricos à Comissão data de meados de 2002 e foi, nessa altura, um acto isolado. Em finais de 2002, chega ao conhecimento da CNPD que havia vários sistemas biométricos em funcionamento, em absoluto incumprimento da Lei de Protecção de Dados. Os pedidos de informação junto da Comissão multiplicaram-se, as pessoas olharam com desconfiança para aquela tecnologia e tinham renitência em fornecer os seus dados biométricos.

A Comissão recebeu algumas queixas, abriu processos de averiguação e aplicou coimas. A questão da biometria tinha-se entretanto mediatizado e a CNPD começou a receber várias notificações relativas ao tratamento de dados biométricos.

Sendo uma matéria complexa, pela especificidade dos dados em causa, foi objecto de muita discussão no interior da CNPD e, mais tarde, nalgumas instâncias comunitárias onde a Comissão está representada. A Assembleia da República foi também sensibilizada para esta nova realidade e para todas as dúvidas suscitadas pela utilização da biometria. A regulamentação do Código de Trabalho passou a exigir o parecer das comissões de trabalhadores.

Uma vez que a maioria dos tratamentos de dados biométricos era realizada no contexto laboral e tinha como finalidade controlar a assiduidade dos trabalhadores, substituindo os meios até aí em vigor, por outros considerados mais fiáveis, a CNPD elaborou, em **2003**, um documento com orientações gerais relativas à utilização de sistemas biométricos para controlo de acessos e assiduidade ⁽⁹⁾.

Em **2003** e **2004**, a Comissão recebeu, respectivamente, 56 e 42 notificações de tratamento de dados biométricos.

O leque de possibilidades de utilização de sistemas biométricos para outras finalidades tem vindo a alargar-se, não só no âmbito das entidades públicas, decorrente em parte de legislação comunitária, mas também ao nível das entidades privadas.

Esta será, pois, uma matéria cuja evolução a CNPD irá acompanhar atenta e activamente nos próximos tempos.

⁽⁹⁾ <http://www.cnpd.pt/bin/orientacoes/principiosbiometricos.htm>

4.4 Escolas

Em **2003** e **2004**, levantaram-se vários problemas relacionados com o tratamento de dados pessoais pelas escolas, o que levou a uma intervenção particular da CNPD nesta área.

Com efeito, em 2003, na sequência de queixas, a Comissão teve de intervir quanto à publicação na Internet, nos *sites* das escolas, de nomes e fotografias de alunos em actividades variadas, bem como à difusão de informações referentes à ficha de avaliação dos alunos, faltas, transferências. Esta divulgação de dados era feita sem o consentimento dos titulares ou dos seus representantes legais.

Ainda nesse ano, começa a ser introduzida em escolas a utilização de cartões magnéticos para controlo de acesso ao recinto escolar e compras no bar ou cantina, sem a devida autorização da Comissão.

Por outro lado, chega ao conhecimento da CNPD que, através das escolas, são feitos inquéritos aos alunos, menores, nos quais se recolhe muita informação pessoal, frequentemente de carácter sensível, sem o conhecimento e autorização prévios dos encarregados de educação. Esses questionários destinavam-se à realização de estudos académicos ou outros e, na maior parte dos casos, também não se encontravam autorizados pela Comissão.

Na sequência destes casos, a CNPD alertou o Ministério da Educação para a necessidade imperiosa de as escolas não colaborarem na realização desses estudos, a menos que estivessem devidamente notificados e autorizados. Foi então enviada uma circular às escolas, pelas direcções regionais de educação, nesse sentido.

Em **2004**, a CNPD manteve também contactos e reuniões com o Ministério da Educação, para esclarecimento e regularização de uma situação detectada em algumas escolas e que se prendia com o tratamento do dado “raça” ou “etnia”, no âmbito da gestão de alunos.

4.5 Segurança social

No final de **2003**, a CNPD decidiu integrar um grupo de trabalho, promovido no âmbito da segurança social, para tratar as questões de protecção de dados de modo mais expedito e eficaz.

Deste modo, realizaram-se várias reuniões, ao longo de **2004**, durante as quais a Comissão sempre prestou todos os esclarecimentos solicitados pelas entidades, quer no tocante à notificação de tratamentos de dados pessoais, quer no tocante a normas que viessem a integrar ante-projectos de diplomas legais. Neste contexto, foram aliás discutidas algumas matérias relativas ao cruzamento de dados entre a segurança social e a administração fiscal, bem como sobre o acesso da Polícia Judiciária aos dados destas entidades.

A participação neste grupo de trabalho permitiu agilizar a legalização de alguns tratamentos de dados por parte da segurança social, de forma mais coordenada e eficiente.

4.6 Euro 2004

A realização do Campeonato Europeu de Futebol – Euro 2004, em Portugal, contrariamente ao que à primeira vista poderia parecer, teve grandes implicações ao nível da protecção de dados.

Por um lado, tratava-se dos tratamentos de dados pessoais referentes à organização e realização dos jogos – um forte controlo de bilhetes, credenciações, grupos identificados que seguiam a sua equipa pelo país, transferência internacional de dados pessoais para a UEFA.

Por outro lado, a construção de novos estádios equipados com sistemas sofisticados de videovigilância e com ligações às autoridades policiais.

No plano da segurança interna, foi tomado um vasto conjunto de medidas, que incluía uma actuação específica das forças policiais nos recintos desportivos, a partilha de informação entre as autoridades nacionais e internacionais, o controlo exigente nas fronteiras, a colocação de videovigilância em espaços públicos de maior afluência.

Por tudo isto, a CNPD decidiu fazer um acompanhamento constante de todo o processo conducente ao Euro 2004. Assim, em **2003**, a Comissão promoveu uma reunião com todas as entidades envolvidas na organização do campeonato, designadamente a Sociedade Euro 2004, representantes das sociedades gestoras dos estádios de futebol, as forças de segurança representadas no comité coordenador de segurança.

Foram várias e profícuas as reuniões e os contactos tidos durante a fase preparatória do campeonato, bem como durante o seu decurso e após o encerramento do evento.

Os tratamentos de dados pessoais foram devidamente notificados à Comissão; os sistemas de videovigilância dos estádios foram igualmente autorizados pela CNPD; os fluxos internacionais de dados foram apreciados pela Comissão; foram apresentados à CNPD relatórios periódicos relativos ao tratamento de dados.

A CNPD foi também chamada a emitir parecer sobre projectos de diploma elaborados especificamente para o período do campeonato.

Na sequência da intervenção activa da CNPD, as autoridades de protecção de dados da Alemanha e da Suíça solicitaram a colaboração da Comissão, para, beneficiando da experiência alcançada, acompanharem a organização do Mundial de Futebol de 2006 e do Euro 2008.

4.7 Experiência de voto electrónico nas eleições europeias

Em **2004**, nas eleições para o Parlamento Europeu, foi lançada pela UMIC uma experiência piloto de voto electrónico, presencial, não vinculativo. Esta experiência, que decorreu em seis freguesias do continente, foi autorizada e acompanhada pela CNPD, uma vez que previa o acesso a informação da Base de Dados do Recenseamento Eleitoral (BDRE) e o seu subsequente processamento.

Sob o ponto de vista de protecção de dados, a questão em causa prendia-se com o sigilo do voto; isto é, foi necessário adoptar medidas de segurança, que impedissem que fosse possível a ligação entre a identificação do eleitor e o correspondente voto expresso.

A Comissão acompanhou o processo, auditando previamente a metodologia utilizada, fiscalizando o acto eleitoral em três freguesias e garantindo a destruição dos dados de identificação dos eleitores, após conclusão da experiência.

O acompanhamento deste processo assumiu especial importância, uma vez que se pretendia com esta experiência verificar as condições da aplicabilidade da votação electrónica em actos eleitorais futuros, de forma já vinculativa.

Tendo em conta as implicações que o voto electrónico tem, ao nível da protecção de dados pessoais, a CNPD decidiu estabelecer, em 2005, os princípios gerais que devem ser adoptados aquando da realização de eleições por votação electrónica.

5. Actividade institucional

5.1 Participação da CNPD na CADA

Durante o ano de 2003 a CADA emitiu 310 Pareceres, dos quais 36 foram relatados pelo representante da CNPD, o vogal Amadeu Guerra.

Durante o ano de 2004, a CADA emitiu 330 Pareceres, tendo o representante da CNPD relatado 27 Pareceres.

No decurso destes dois anos subsistem os problemas relativos à delimitação de competências da CADA e da CNPD. Conforme foi sublinhado no relatório relativo aos anos de 2001/2002, considera-se ser fundamental a adopção de providências legislativas que clarifiquem a intervenção destas duas autoridades independentes.

Na óptica do representante da CNPD, continua a CADA a fazer a apreciação de processos em que se pede o acesso a informação constante de tratamentos automatizados (v.g. listas de endereços), sem que seja considerado o princípio da finalidade constante do artigo 5.º n.º 1 alínea b) da Lei 67/98, de 26 de Outubro – isto essencialmente por serem diferentes as noções de dados pessoais na lei n.º 65/93 e na lei n.º 67/98. Por outro lado, o acesso de terceiros a listas de endereços – sem conexão com os princípios da “Administração Aberta” – pode suscitar problemas em sede de utilização de dados para fins de marketing ou outra forma de prospecção, na medida em que os titulares dos dados nunca foram informados sobre a possibilidade de utilização dos seus dados para esta finalidade (cf. artigo 10.º da Lei 67/98), nem lhes foi facultada a possibilidade de se oporem à utilização dos seus dados para esta finalidade (cf. artigo 12.º alínea b) da Lei 67/98). Por isso, têm sido apresentadas declarações de voto que visam alertar para a necessidade de ser ponderada a observância destes princípios.

Um outro aspecto que merece especial realce prende-se com a publicação da Directiva 2003/98/CE do Parlamento Europeu e do Conselho, de 17 de Novembro de 2003, relativa à “reutilização de informação do sector público” (*in* JO L 345/90, de 31/12/2003). Esta Directiva obriga os Estados Membros a pôr em vigor disposições legislativas, regulamentares e administrativas até Maio de 2005 (artigo 12.º). Até ao fim de 2004 não temos conhecimento que tenham sido introduzidas alterações legislativas que tenham tido em vista transpor esta Directiva.

Considerando esta Directiva, no seu artigo 1.º n.º 4, que não está em causa a modificação ou afectação do nível de protecção dos indivíduos relativamente aos princípios estabelecidos na Directiva de protecção de dados (Directiva 95/46/CE), salienta-se que a “reutilização” terá que respeitar a protecção da privacidade consignada na Lei 67/98. Por isso, afigura-se que a transposição da Directiva 2003/98/CE não tem qualquer implicação em relação ao nível de protecção assegurado pela Lei de Protecção de Dados.

Considera-se, porém, que será uma boa oportunidade para poder ser equacionada e estabelecida a delimitação de competências da CNPD e da CADA na medida em que os procedimentos de “reutilização” podem vir a ter implicações no âmbito de intervenção da CADA.

5.2 Audições parlamentares

A CNPD foi convocada pela Assembleia da República, nos anos de **2003** e **2004**, para ser ouvida no âmbito de vários projectos de diploma em apreciação nas comissões parlamentares especializadas:

- Comissão de Obras Públicas, Transportes e Telecomunicações sobre a transposição das directivas de telecomunicações (29/10/2003);
- Comissão de Trabalho sobre a regulamentação ao Código do Trabalho (Março de 2004);
- Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias sobre a lei orgânica da CNPD (18/5/2004);
- Comissão de Saúde sobre o regime jurídico aplicável à realização de ensaios clínicos com medicamentos de uso humano (27/5/2004).

A pedido da CNPD, realizou-se também uma reunião com a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, em 26/2/2003, para apresentação do ante-projecto da lei de organização e funcionamento da CNPD, e para apresentação do plano anual de actividades. Foram ainda abordadas outras questões relacionadas com a actividade da Comissão.

Durante o ano de 2003, foram ainda realizadas reuniões com os grupos parlamentares sobre a actividade da CNPD, nomeadamente acerca de algumas questões emergentes como a videovigilância e a biometria.

6. Divulgação e transparência

6.1 Relacionamento com os órgãos de comunicação social

A CNPD manteve, em 2003 e 2004, um bom e regular relacionamento com os órgãos de comunicação social, que cada vez mais procuram os temas da protecção de dados e da privacidade.

É de sublinhar que, além das notícias diárias sobre temas da actualidade noticiosa, há um interesse crescente por parte dos jornalistas em desenvolver temas de modo mais aprofundado sob a forma de reportagem ou entrevista.

As questões de protecção de dados, até aqui tratadas quase exclusivamente pelos grandes jornais, pela rádio e pela televisão, alargaram-se também à imprensa regional, às publicações especializadas e à esfera das revistas femininas. As solicitações recebidas na Comissão demonstram isso mesmo, o que significa que estas matérias vão chegando a um público mais vasto, que ganha consciência do quanto a protecção de dados está presente em tantos aspectos da sua vida.

Nestes dois anos, a Comissão emitiu oito comunicados de imprensa, promoveu uma conferência de imprensa e respondeu às solicitações de cerca de 200 telefonemas de jornalistas. Participou ainda em programas de rádio e de televisão temáticos. Nalguns casos, foi-nos pedida a colaboração para participar com textos sobre protecção de dados para dossiês temáticos.

6.2 Reestruturação do *site* da Internet

Em **2004**, a CNPD procedeu a uma reestruturação do seu *site* na Internet, de modo a torná-lo mais apelativo, mais funcional e, principalmente, mais rico sob o ponto de vista do conteúdo, disponibilizando um vasto conjunto de informação sobre a Comissão e a sua actividade nacional e internacional.

O *site* passou a dispor também de dois programas de pesquisa, um geral e outro só para decisões da CNPD, e permitiu a disponibilização *on line* do registo público das entidades devidamente legalizadas junto da Comissão. Dadas as muitas solicitações que recebemos do estrangeiro, considerou-se ser útil colocar no *site* alguns recursos em versão inglesa e francesa.

A reformulação do nosso *site* foi inteiramente desenvolvida pelos serviços da CNPD. Poderá visitar-nos em **www.cnpd.pt**

6.3 Edições da CNPD

Em **2003**, a Comissão iniciou a publicação de uma colecção intitulada “Documentos da CNPD”, cujo objectivo é editar pequenos cadernos de divulgação das matérias de protecção de dados.

Assim, a colecção começou com a publicação dos “Princípios sobre a Privacidade no Local de Trabalho: o tratamento de dados em centrais telefónicas, o controlo do e-mail e do acesso à Internet”.

Em **2004**, a CNPD publicou o segundo caderno, também dedicado à privacidade no local de trabalho, mas já sobre “A utilização de dados biométricos para controlo de acessos e de assiduidade”.

Em função da especificidade dos temas, a CNPD procede à sua distribuição pelas entidades que são destinatários privilegiados.

Também em **2004**, no âmbito do seu 10.º aniversário, a CNPD editou um livro contendo as “Principais Orientações da Comissão Nacional de Protecção de Dados 1994-2004”. Trata-se de uma compilação e sistematização de dez anos de doutrina de protecção de dados pessoais, que permite ter uma visão global dos critérios que têm norteado a actuação da Comissão ao longo de uma década.

6.4 Colóquio comemorativo do 10.º aniversário

A CNPD promoveu, em **2004**, um colóquio subordinado ao tema “Proteger os dados pessoais – um desafio constante”, que se realizou no dia 28 de Outubro, na Fundação Calouste Gulbenkian, em Lisboa.

A sessão de abertura foi presidida pela Vice-Presidente da Assembleia da República, Leonor Beleza, e contou também com a presença do Presidente da Comissão de Assuntos Constitucionais, António Montalvão Machado, e do administrador da Fundação Diogo de Lucena.

Além dos membros da CNPD, foram oradores do colóquio João Salgueiro, Presidente da Associação Portuguesa de Bancos, Diogo Vasconcelos, Gestor da UMIC, Carlos Cabreiro, Director da Brigada de Criminalidade Informática da PJ, Filipe Custódio, perito em segurança informática, e Álvaro Canales, Secretário-geral da autoridade de protecção de dados espanhola.

Neste colóquio comemorativo dos dez anos de actividade da Comissão, foram abordadas várias questões muito actuais em torno da protecção de dados, tais como a videovigilância, o cibercrime, as redes abertas e a segurança, as novas tecnologias, o governo electrónico e a circulação de dados num mundo global. O colóquio contou com uma grande participação do público e os períodos de debate foram animados.

6.5 Cursos e acções de formação

A participação crescente da Comissão em cursos e acções de formação denota a consciencialização da importância da protecção de dados e a vontade de conhecer melhor esta matéria.

É de assinalar que as solicitações vieram essencialmente de entidades públicas e de universidades.

A CNPD sempre tem considerado que é de grande importância estar presente e contribuir para a formação profissional de um vasto universo de pessoas que ajudarão certamente, no âmbito da sua actividade – e também no plano da sua cidadania –, a garantir o respeito por um direito fundamental.

Nos anos de 2003 e 2004, a CNPD participou nas seguintes acções:

- *“Os Sistemas de Informação e Vigilância e a Protecção de Dados Pessoais”*, por Alexandre Pinheiro, 2.º Curso de Investigação Criminal – Oficiais, GNR, Queluz, Janeiro 2003;

- *“Videovigilância quais os limites?”*, por Luís Silveira, conferência no âmbito do Curso de Formação de Oficiais de Polícia, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa, Abril 2003;
- *“Utilização e controlo de dados pessoais nas sociedades contemporâneas”*, por Luís Silveira, debate no âmbito do curso de Sociologia, ISCTE, Lisboa, Maio 2003;
- *“Os Sistemas de Informação e Vigilância e a Protecção de Dados Pessoais”*, por Alexandre Pinheiro, 1.º Curso de Investigação Criminal – Sargentos, GNR, Queluz, Dezembro 2003;
- Acção de formação sobre protecção de dados ministrada aos dirigentes do Ministério da Agricultura, por Isabel Cruz, Lisboa, Abril 2004;
- Acção de esclarecimento sobre protecção de dados dirigida aos técnicos superiores do Tribunal de Contas, por Luís Silveira, Tribunal de Contas, Lisboa, Abril 2004;
- Sessão sobre protecção de dados pessoais no âmbito do curso de Engenharia Informática, por Amadeu Guerra, Instituto Politécnico de Castelo Branco, Maio 2004;
- II Jornadas de Ciência de Informação, no âmbito do curso de Ciências de Informação, Faculdade de Letras da Universidade do Porto, Maio 2004;
- Curso sobre protecção de dados, por Alexandre Pinheiro, Conselho Distrital da Ordem dos Advogados, Lisboa, Junho 2004;
- Conferência *“A Comissão Nacional de Protecção de Dados”*, por Luís Silveira, no âmbito do Curso de Promoção a Oficial Superior da Guarda Nacional Republicana 2004/2005, Instituto de Altos Estudos Militares, Lisboa, Novembro 2004;
- *“Os Sistemas de Informação e Vigilância e a Protecção de Dados Pessoais”*, por Eduardo Campos, 2.º Curso de Investigação Criminal – Sargentos, GNR, Queluz, Dezembro 2004.

6.6 Participação em seminários

Nos últimos dois anos, a Comissão continuou com regularidade a ser convidada a participar em vários colóquios e seminários, promovidos por entidades públicas e privadas, apresentando comunicações sobre a protecção de dados aplicada a dife-

rentes sectores de actividade ou moderando debates relativos às questões da privacidade.

Participámos nas seguintes iniciativas:

- *“Novas tecnologias e direito à privacidade”*, moderado por Luís Silveira, 3.ª Conferência do Montepio Geral, Lisboa, Março 2003;
- *“Ponto da situação no e government em Portugal”*, por Luís Barroso, APDSI, Arrábida, Novembro 2003;
- Seminário sobre a Directiva de acesso, reutilização e comercialização de informação do sector público, por Amadeu Guerra, INETI, Lisboa, Dezembro 2003;
- *“Utilização do Genoma Humano implicações ao nível da protecção de dados”*, por Luís Silveira, Seminário “Genoma Humano: problemas e desafios”, Assembleia da República, Lisboa, Março 2004;
- *“Acesso às bases de dados”*, por Luís Silveira, Jornadas em Direito dos Seguros, FDUL/SPAIDA, Lisboa, Abril 2004;
- *“Comunicação não solicitada”*, por Alexandre Pinheiro, Comércio Electrónico – o novo regime legal, GPLP, Ministério da Justiça, Lisboa, Abril 2004;
- *“Whois a protecção de dados pessoais na Internet”*, por Luís Barroso, Lisboa, Abril 2004;
- *“Direitos fundamentais dos trabalhadores no âmbito do novo Código do Trabalho”*, por Amadeu Guerra, XXII Encontro de Gestores de Recursos Humanos, Associação Portuguesa das Empresas do Sector Eléctrico e Electrónico, Tavira, Maio 2004;
- *“O acesso e a protecção de dados”*, por Ana Luísa Geraldes, Seminário sobre Documentação, CENJOR/ISCSP, Lisboa, Maio 2004;
- Fórum sobre comunicações de emergência e segurança, por Luís Silveira, Fundação Portuguesa das Comunicações, Lisboa, Junho 2004;
- Workshop *“Genetic Information Day and recommendations to the EC”*, por Luis Silveira, Privireal, Universidade de Sheffield, Coimbra, Julho 2004;
- *“Sistemas públicos: da segurança à protecção de dados pessoais”*, por Luís Barroso, Jornadas da Administração Pública Inter.Face, Lisboa, Setembro 2004;

- “*Política de acesso à informação*”, por Luís Silveira, na apresentação pública dos resultados preliminares do INSAAR (Inventário Nacional de Abastecimento de Água e de Águas Residuais), LNEC, Lisboa, Outubro 2004;
- “*Privacidade e Biometria*”, por Fernando Silva, Networkers Fórum 2004, Lisboa, Outubro 2004;
- Colóquio sobre “*O sistema das garantias da Privacy no Ordinamento Italiano à luz do novo código e a protecção de dados pessoais em Portugal*”, por Luís Silveira, Instituto Italiano de Cultura em Portugal, Lisboa, Setembro 2004;
- Colóquio “*A liberdade de expressão na Internet*”, por Alexandre Pinheiro, APDSI, Lisboa, Novembro 2004;
- “*A perspectiva constitucional e da protecção de dados pessoais*”, por Alexandre Pinheiro, Seminário sobre Métodos Biométricos, Faculdade de Direito da Universidade do Porto, Novembro 2004;
- Encuentro Europeo de Mejores Prácticas Públicas de Protección de Datos, Luís Silveira, Agencia de Protección de Datos de la Comunidad de Madrid, Madrid, Dezembro 2004.

7. Avaliações a Portugal

7.1 Avaliação do Conselho da UE sobre a aplicação da Convenção de Aplicação do Acordo de Schengen

No ano de **2003**, Portugal foi sujeito a uma avaliação por parte do Conselho da União Europeia quanto à forma como é aplicada, nas suas várias vertentes, a Convenção de Aplicação do Acordo de Schengen (CAAS). Trata-se de avaliações periódicas que são feitas em todos os Estados-Membros pelo Grupo de Trabalho de Avaliação Schengen. Neste âmbito, a actividade e intervenção da CNPD, enquanto autoridade nacional de controlo responsável pela supervisão da parte nacional do Sistema de Informação Schengen (N.SIS) e pela verificação do tratamento de dados pessoais introduzidos no sistema ⁽¹⁰⁾, foi também avaliada por uma equipa de peritos de vários Estados-Membros.

⁽¹⁰⁾ Competência atribuída pela Lei 2/94 de 19 de Fevereiro. Disponível em www.cnpd.pt

Para aferir a situação portuguesa em matéria de protecção de dados pessoais e a sua especificidade em termos legislativos, uma vez que a Convenção Schengen remete frequentemente a aplicação concreta dos princípios para as legislações nacionais, foi respondido pela CNPD um extenso questionário que serviu de base para o trabalho do grupo de peritos que viria a Portugal em Julho desse ano.

Assim, no quadro da visita do grupo de avaliação ao nosso país, estava também incluído um dia de trabalho com a CNPD, que decorreu nas nossas instalações.

Aí, foi feita uma apresentação mais detalhada do quadro legal existente, da natureza e competências da CNPD e da sua actividade enquanto autoridade de supervisão de protecção de dados para o acervo de Schengen.

Esta actividade tem dois aspectos essenciais: por um lado, um carácter de fiscalização das condições técnicas e de segurança do funcionamento do Sistema de Informação Schengen (SIS) a nível nacional, incluindo o modo como as várias entidades autorizadas acedem ao sistema; por outro lado, a questão do exercício dos direitos dos cidadãos e a verificação da conformidade legal do tratamento de dados pessoais, que envolve nalguns casos a colaboração com as autoridades congéneres de outros Estados-Membros.

Em Portugal, o direito de acesso, rectificação ou eliminação é realizado de forma indirecta, através da CNPD, sendo os pedidos dos cidadãos sempre dirigidos à Comissão, o que resulta num maior acompanhamento de todos os casos.

A equipa de peritos solicitou vários esclarecimentos sobre o funcionamento do sistema, as medidas de segurança adoptadas, os poderes efectivos da CNPD, a acção inspectiva da Comissão, a verificação dos pressupostos legais para a introdução de dados pessoais no SIS, o número de pedidos de acesso por parte dos cidadãos, a informação disponibilizada aos cidadãos e o seguimento dos seus pedidos, a cooperação com as autoridades nacionais de controlo de outros Estados-Membros do espaço Schengen na resolução de casos.

Após esta visita de trabalho, o grupo de avaliação elaborou um relatório de protecção de dados, que veio a integrar o relatório final da avaliação Schengen a Portugal. As conclusões do relatório foram bastante positivas, indicando um nível de protecção de dados satisfatório e elogiando a atitude empenhada da CNPD no auxílio aos

cidadãos, em particular, os curtos prazos de resposta aos pedidos de acesso e a informação de apoio disponibilizada ao público, bem como as acções de divulgação das matérias Schengen.

O grupo de avaliação sugeriu que a Comissão seguisse de perto a execução das recomendações feitas no âmbito das inspecções realizadas pela CNPD e encorajasse auditorias internas nos serviços com acesso ao SIS, de modo a melhor garantir as condições de segurança.

7.2 Avaliação da Comissão Europeia sobre a transposição da Directiva de Protecção de Dados

A Comissão Europeia efectuou, no ano de **2004**, uma avaliação à forma como a Directiva de Protecção de Dados (Directiva 95/46/CE, de 24 de Outubro) tinha sido transposta para a legislação nacional. Nesse sentido, a Comissão Europeia realizou uma análise comparativa entre as disposições da Directiva e a Lei de Protecção de Dados portuguesa. Os resultados dessa análise foram submetidos à CNPD e ao Governo, através do Ministério da Justiça, para um comentário preliminar.

No seguimento desse primeiro passo, deslocou-se a Portugal um representante da Comissão Europeia, a fim de discutir com a CNPD (e com o Governo) da adequação da transposição da Directiva e avaliar se haveria necessidade de alguma alteração legislativa.

Com efeito, a CNPD prestou todos os esclarecimentos quanto ao quadro constitucional português, bem como ao conjunto de legislação que legitima o tratamento de dados pessoais e contém normas específicas de protecção de dados, sem necessidade de, por isso, pormenorizar na Lei de Protecção de Dados alguns aspectos específicos já cobertos por outras disposições legais.

Por outro lado, a CNPD informou ainda qual o seu entendimento da lei e de que modo a aplica na prática.

De um modo geral, verificou-se que a Lei de Protecção de Dados segue de perto a Directiva, não tendo sido assinaladas grandes discrepâncias. A Comissão Europeia considerou, no entanto, que o elenco de dados sujeitos a controlo prévio é demasia-

do extenso, tendo Portugal usado o espaço de manobra deixado aos Estados-Membros de uma forma mais garantística (tal como Itália) que outros países.

Quanto ao regime de transferência internacional de dados, a CNPD concordou com as observações da Comissão Europeia, no sentido de não obrigar a autorização prévia os fluxos de dados para destinos considerados de protecção adequada por decisões da Comissão Europeia, cuja aplicação é obrigatória, bem como nos casos de derrogação previstos no artigo 26.º n.º 1 da Directiva (transposto para o artigo 20.º n.º 1 da LPD).

Nesse sentido, a CNPD comprometeu-se a aligeirar esse procedimento, tendo, ainda em **2004**, aprovado uma Deliberação Interpretativa⁽¹¹⁾ dos artigos 19.º e 20.º da Lei de Protecção de Dados, na qual se estabelece que as transferências internacionais de dados realizadas ao abrigo das derrogações do artigo 20.º n.º 1, ou no âmbito de Decisões da Comissão Europeia, incluindo através da utilização de cláusulas contratuais-tipo, têm de ser notificadas à CNPD mas não requerem autorização prévia para a sua concretização.

8. Decisões judiciais

Em **2003**, ocorreram duas decisões judiciais sobre recursos interpostos de decisões da CNPD em matéria de coimas, em ambos os casos por falta de notificação de tratamentos de dados pessoais.

Num caso, estava em causa um tratamento de dados de munícipes por parte duma câmara municipal; no outro, um tratamento de dados de utentes por parte duma instituição privada de segurança social.

Em ambos os casos os tribunais confirmaram a existência das contravenções verificadas pela CNPD. No tocante à cometida pela câmara municipal, o Tribunal Judicial da Maia rejeitou integralmente o respectivo recurso; no concernente à instituição de segurança social, o Tribunal Judicial de Valongo reduziu a coima aplicada.

Durante o ano em referência, a CNPD enviou ao Ministério Público um processo em que, no seu entendimento, se apresentavam indícios da prática de crime de falta de

⁽¹¹⁾ Poderá consultar esta Deliberação em <http://www.cnpd.pt/bin/orientacoes/orientacoes.htm>

colaboração por parte de entidade privada. O Ministério Público arquivou a queixa, por considerar que não se comprovavam suficientemente tais indícios.

No decurso de **2004**, foram proferidas por tribunais de 1.^a instância três decisões sobre recursos de coimas aplicadas pela CNPD.

Num dos casos, estava em causa a publicação na Internet, por entidade privada, de fotografias de devedores e de cheques por eles alegadamente não pagos; noutro, a falta de notificação, por uma câmara municipal, dum tratamento de dados relativos a munícipes; no outro, a cedência, sem conhecimento dos clientes, por uma empresa de telecomunicações a uma outra com ela conexas, de dados daqueles susceptíveis de compor os respectivos perfis, para efeitos de marketing.

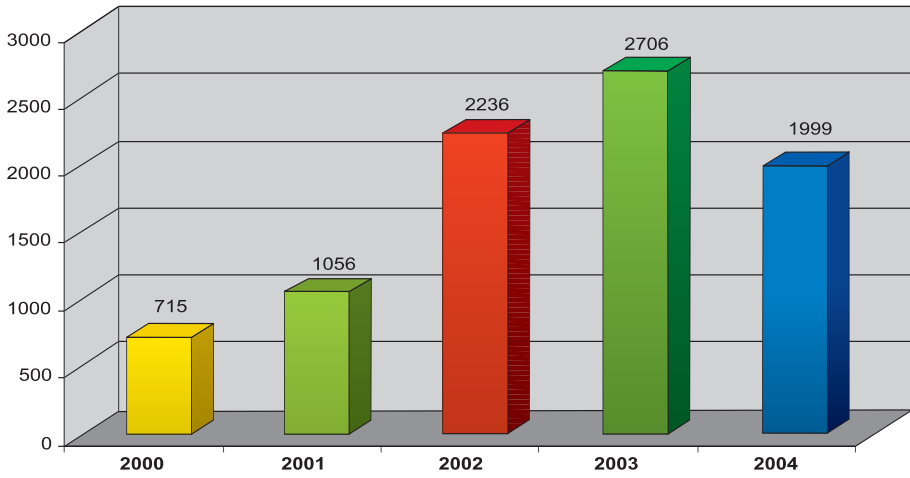
Todos esses processos foram decididos – respectivamente pelos Tribunais de Família e Menores de Portimão; da Comarca de Vila Real de St.º António e de Pequena Instância Criminal de Lisboa – no sentido da rejeição dos recursos interpostos.

Da última decisão mencionada foi tentado recurso para o Tribunal da Relação de Lisboa, que manteve a decisão da 1.^a instância.

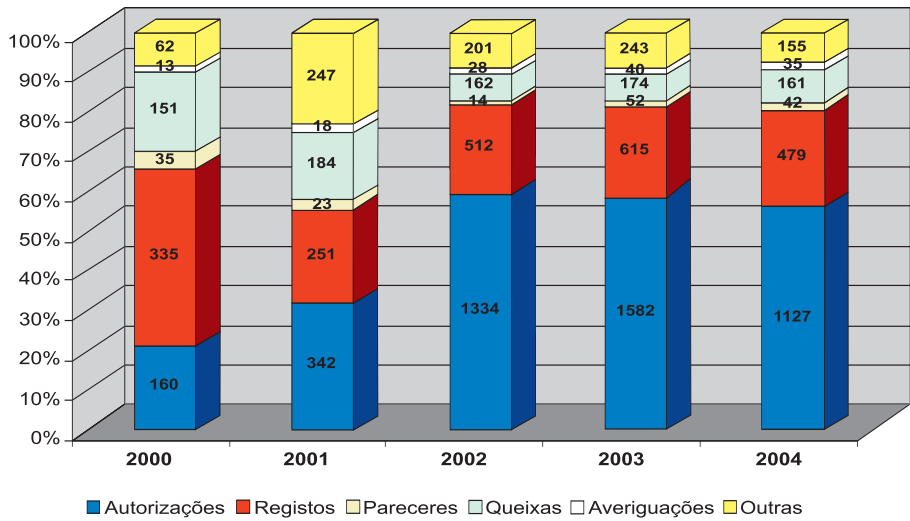
Poderá consultar as decisões judiciais em: <http://www.cnpd.pt/bin/legis/juris/jurisprudencia.htm>

ESTADÍSTICAS

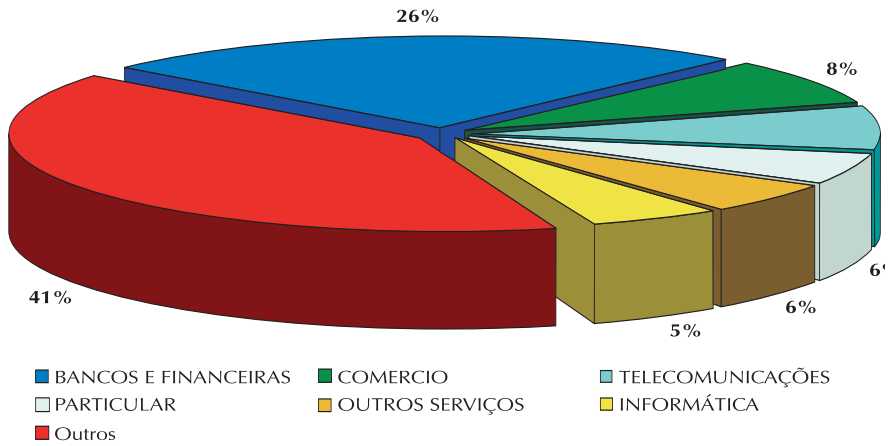
Processos Entrados



Peso comparativo dos processos por espécie

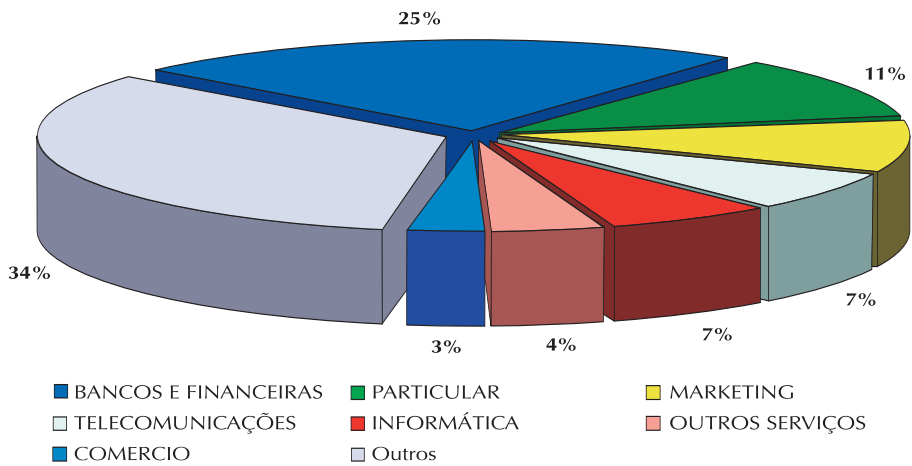


Queixas em 2003 - Entidade Participadas

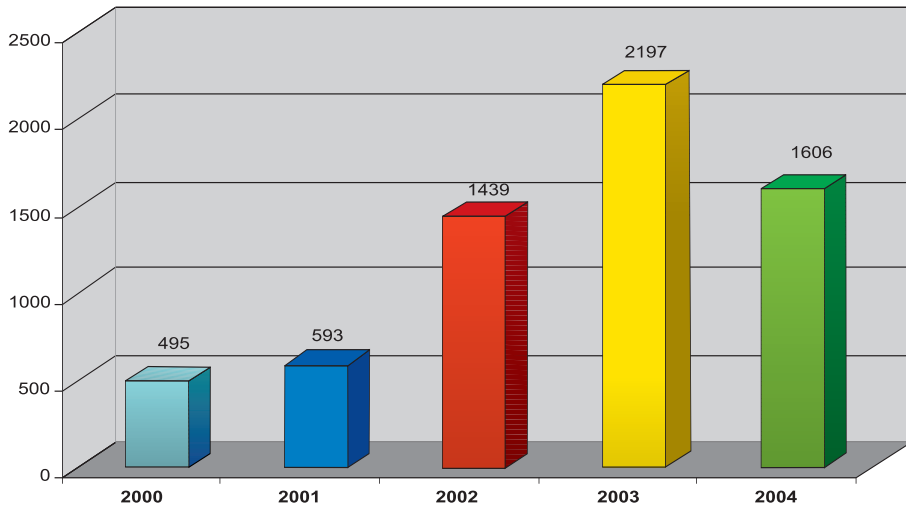


ESTATÍSTICAS

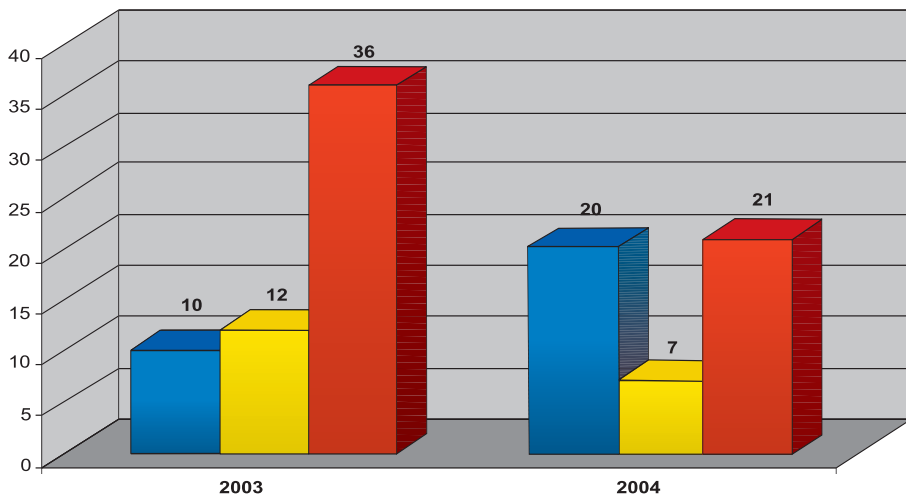
Queixas em 2004 - Entidade Participadas



Evolução do número de Notificações de tratamento recebidas

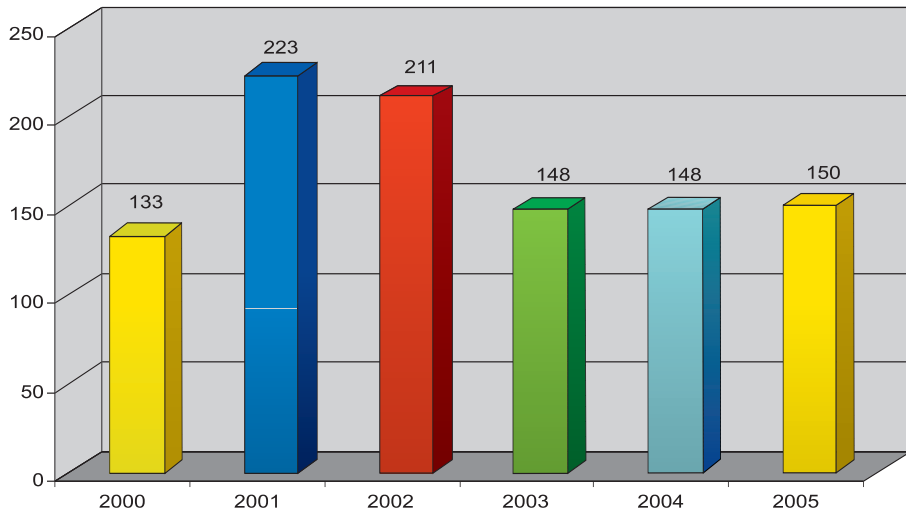


Pedidos de Acesso

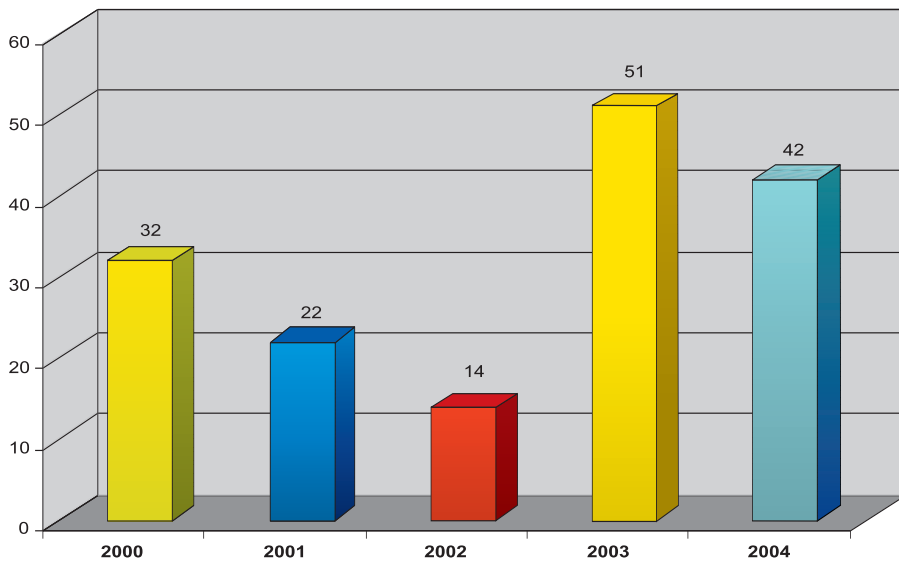


■ Dados de Saúde ■ BDRE ■ Schengen

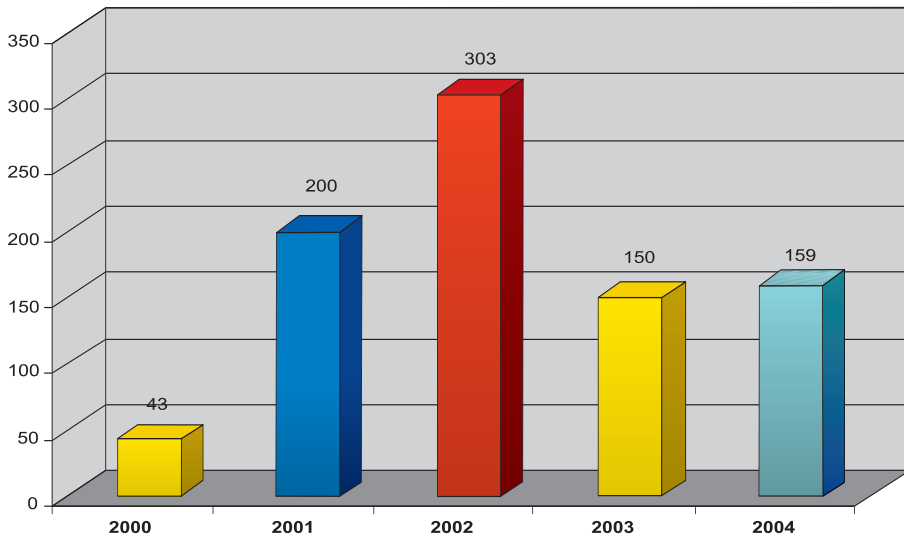
Fiscalizações



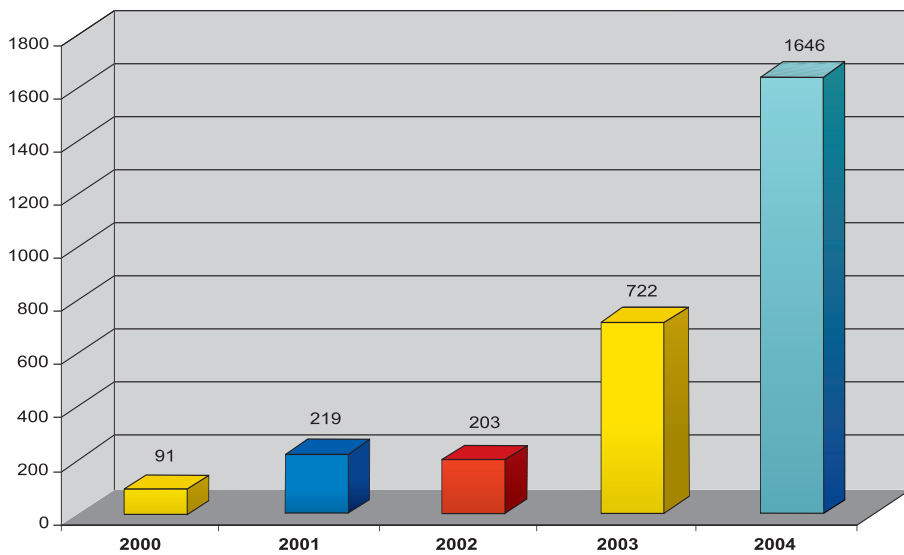
Evolução do número de Pareceres dados



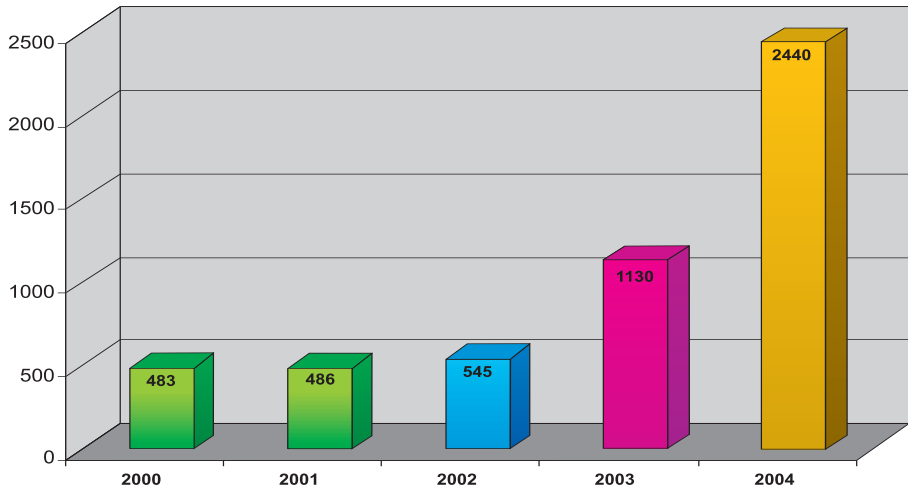
Evolução do número das Deliberações dadas



Evolução do número de Autorizações emitidas



Ficheiros Legalizados por Ano



CAPÍTULO II

ACTIVIDADE INTERNACIONAL

1. Representação nas autoridades comuns de controlo

1.1 EUROPOL

A CNPD está representada na Instância Comum de Controlo (ICC) da EUROPOL, que tem como principal atribuição supervisionar a actividade da EUROPOL em matéria de dados pessoais e garantir os direitos dos cidadãos consignados na Convenção EUROPOL ⁽¹²⁾.

Em **2003** e **2004**, a CNPD participou em 9 reuniões plenárias da ICC, tendo ainda contribuído activamente ao nível de subgrupos de trabalho. Este período foi de particular importância para a ICC, quer no plano do desenvolvimento da operacionalidade da EUROPOL que foi necessário acompanhar de perto, quer devido à entrada de novos membros no seguimento do alargamento da EU.

Com efeito, em **2003**, os quinze países do alargamento foram convidados a participar nas reuniões da ICC como observadores, permitindo-lhes familiarizarem-se com o seu funcionamento e as matérias em discussão. Foi-lhes também proporcionada uma visita à EUROPOL. Em **2004**, apesar de consumada a sua entrada na UE, só alguns Estados-Membros estavam em condições de integrar-se na ICC como membros de pleno direito, dependendo da sua adesão à Convenção EUROPOL.

Por outro lado, nestes dois anos, estiveram em discussão propostas de alteração à Convenção EUROPOL, para as quais a ICC foi chamada a pronunciar-se, em particular quanto ao prazo de conservação dos dados em ficheiros de análise, tendo sido acolhidas as suas sugestões.

⁽¹²⁾ Poderá obter mais informação sobre esta Autoridade e a sua actividade em http://www.cnpd.pt/bin/actividade/icc_europol.htm

A ICC, durante 2003 e 2004, emitiu pareceres sobre acordos a realizar entre a EUROPOL e outros países, designadamente com os EUA, a Bulgária e a Roménia, e também com a EUROJUST, impondo determinadas salvaguardas para a prossecução dos acordos.

A ICC emitiu ainda parecer sobre nove ordens de criação de ficheiros de análise e acompanhou o desenvolvimento do sistema de informações, bem como a participação da EUROPOL em projectos operacionais ou em equipas de investigação conjuntas dos Estados-Membros.

A ICC realizou também duas inspecções à EUROPOL, uma em Fevereiro de **2003** (seguida de uma inspecção de reavaliação em Novembro), e outra em Março de **2004**. A apreciação feita pela equipa de peritos foi globalmente satisfatória, tendo-se verificado uma melhoria do respeito pelos padrões exigíveis de protecção de dados relativamente à inspecção feita em 2000. No entanto, registaram-se alguns problemas quanto à qualidade dos dados, denotando uma incapacidade dos Estados-Membros em avaliarem a proveniência e fiabilidade dos dados pessoais transmitidos à EUROPOL.

Durante os dois anos em referência, a ICC recebeu dois pedidos de cidadãos para verificar a forma como a EUROPOL procedia ao tratamento dos seus dados pessoais, tendo concluído que a EUROPOL agiu em conformidade com o disposto na Convenção.

No âmbito do Comité de Recursos da ICC, foram apreciados dois recursos, que envolveram importantes questões de princípio. Uma decisão do Comité de Recursos apontou para a necessidade da EUROPOL considerar cada pedido de acesso individualmente e não aplicar na sua apreciação uma abordagem global. Em causa estava o facto da EUROPOL, perante um pedido de acesso aos dados por parte do seu titular, não lhe ter comunicado que não procedia ao tratamento dos seus dados, tal como a legislação aplicável do Estado-Membro previa. Numa segunda decisão, o Comité de Recursos considerou que a EUROPOL tem de responder a um pedido de acesso na mesma língua utilizada pelo requerente, desde que se trate de uma língua oficial da UE.

1.2 Schengen

A CNPD está igualmente representada na Autoridade de Controlo Comum (ACC) Schengen, que é constituída por todos os Estados-Membros do espaço Schengen ⁽¹³⁾, e para cuja vice-presidência Portugal foi aliás eleito no final de 2003.

Os anos de **2003** e **2004** foram anos particularmente activos para a ACC Schengen, devido às várias iniciativas legislativas, com vista à alteração da Convenção Schengen e ao desenvolvimento da segunda geração do Sistema de Informação Schengen (SIS II).

Na verdade, a ACC dedicou uma grande parte do seu trabalho a acompanhar de perto as propostas legislativas e o processo de desenvolvimento do novo sistema, que conterà novas categorias de informação e permitirá acesso a um maior número de entidades, bem como ampliará as finalidades para a utilização de dados pessoais.

Neste âmbito, emitiu pareceres, manteve uma estreita relação com as instituições envolvidas neste processo e teve duas audiências no Parlamento Europeu para expor o seu entendimento sobre a importância de manter altos padrões de protecção de dados num sistema com muito mais funcionalidades e potencialidades.

A ACC realizou ainda, em **2003**, uma inspecção ao sistema central do SIS, em Estrasburgo, na sequência da qual efectuou recomendações, cujo cumprimento veio a verificar durante **2004**.

No que diz respeito ao trabalho de divulgação dos direitos e da actividade da Autoridade, nestes dois anos, a ACC lançou um novo sítio na Internet, desenvolveu uma nova campanha de informação em todos os Estados Schengen e publicou o seu 1.º boletim informativo, que se pretende venha a ser editado periodicamente.

A ACC decidiu também, em estreita colaboração com as autoridades nacionais de controlo que a compõem, verificar como se processa a aplicação em cada um dos Estados-Membros das disposições da Convenção quanto aos dados do artigo 96.º.

Nos termos do artigo 96.º da Convenção Schengen, as autoridades dos Estados-Membros podem inserir no SIS indicações relativas a estrangeiros a quem é recusada a entrada no espaço Schengen. Tal indicação tem de ser precedida de uma decisão

⁽¹³⁾ Poderá obter mais informação sobre esta Autoridade em http://www.cnpd.pt/bin/actividade/acc_schengen.htm

tomada pelas autoridades administrativas ou pelos órgãos jurisdicionais competentes, de acordo com as regras processuais previstas na legislação nacional.

A maioria dos dados pessoais inseridos no SIS são-no ao abrigo do artigo 96.º, pelo que a ACC elaborou um plano de acção para que cada autoridade nacional de controlo verificasse no seu país a inserção destes dados e avaliasse a aplicação e interpretação do artigo 96.º em cada Estado-Membro.

Após um levantamento exaustivo sobre a legislação de cada EM, foram lançadas pela ACC, em **2004**, de forma coordenada, acções de fiscalização em cada país.

1.3 Alfândegas

A Autoridade Supervisora Comum (ASC) do Sistema de Informação Aduaneiro (SIA) é a entidade que fiscaliza aquele sistema em matéria de protecção de dados pessoais. Nela estão representadas as autoridades nacionais de protecção de dados, pelo que a CNPD tem também assento neste colégio, no âmbito da sua actividade internacional.

Em **2003**, a ASC foi chamada a pronunciar-se sobre alterações à Convenção aduaneira de 26 de Julho de 1995, quanto à criação de uma base de dados de identificação e quanto ao acesso por parte da EUROPOL e da Eurojust ao SIA.

Em **2004**, a ASC adoptou orientações gerais para a realização de inspecções ao sistema de informação, tendo constituído uma equipa de peritos para realizar as acções de fiscalização.

Durante estes dois anos, a ASC manteve contactos periódicos com a Organização de Luta Anti-Fraude (OLAF) e com o Grupo de Trabalho de Cooperação Aduaneira, acompanhando de perto o desenvolvimento do SIA.

1.4 Eurojust

Relativamente ao ano de **2003**, as acções mais significativas desta Autoridade consistiram: na realização de uma reunião com os membros da Eurojust a 21 de Março; na apreciação de projecto de acordo a celebrar entre a Eurojust e a EUROPOL.

A primeira teve essencialmente por finalidade o conhecimento mútuo e o debate em torno das competências da entidade de controlo, de modo a evitar futuras dúvidas de

interpretação. O projecto de acordo foi considerado adequado sob a perspectiva da protecção de dados.

Relativamente ao ano de **2004**, foi aprovado o regulamento interno desta Autoridade de Controlo. Foi aprovado um conjunto de emendas sobre regras de tratamento e protecção de dados no âmbito do Eurojust. Foi apreciado um acordo a celebrar entre a Eurojust e a Noruega.

2. Participação em grupos de trabalho

2.1 Artigo 29.º

O chamado “Grupo do artigo 29.º”, organismo consultivo da Comissão Europeia composto por representantes das autoridades de protecção de dados da UE (e no qual participaram, em 2003, em representação da CNPD, o Presidente e o Vogal Procurador-Geral Adjunto Amadeu Guerra), apreciou, no ano de **2003**, algumas questões gerais de protecção de dados de maior actualidade.

Assim, designadamente, deu parecer sobre um projecto de directiva relativa à reutilização de documentos das entidades públicas. Reconhecendo o interesse económico a que esta operação pode corresponder, o Grupo chamou a atenção para as implicações que em termos de protecção de dados pode envolver, e sugeriu procedimentos tendentes a assegurar este objectivo.

Enunciou, segundo a mesma perspectiva, as garantias que no âmbito do “*e government*” devem ser respeitadas para que este não afecte desproporcionadamente os dados pessoais dos cidadãos administrados.

Voltou a apreciar as vantagens e desvantagens das chamadas “*binding corporate rules*” – declarações unilaterais auto-vinculantes através das quais as empresas (nomeadamente grandes multinacionais dispendo de representações na Europa) se obrigam a assegurar a defesa de dados pessoais nas transferências dos mesmos para países que não proporcionam protecção adequada, sobretudo os EUA. A CNPD – embora intervindo nas discussões – tem-se mantido à margem das tomadas de posição nesta matéria, por se afigurar que, no direito português, declarações deste tipo não podem constituir fonte de obrigações.

Aprovou-se, depois de demorada análise, o primeiro código de conduta submetido à apreciação do Grupo – o da Federação Europeia de Marketing Directo (FEDMA). O cuidado posto no estudo deste instrumento decorreu do propósito de assim se definirem princípios gerais a fazer relevar também em relação a futuros semelhantes textos de auto-regulação.

Tomou-se, enfim, posição acerca duma questão que tem vindo a encontrar soluções diversas consoante os Estados: a da retenção de “dados de tráfego”, de comunicações electrónicas, para efeitos de facturação. Considerou-se ajustado, ponderados os interesses contrapostos em jogo, um prazo de retenção de três e seis meses, e recomendou-se consequentemente aos Estados-membros da UE que assim procedessem.

O Grupo foi, em **2004**, chamado a intervir numa questão em que se patenteou a divergência de perspectivas sobre a protecção de dados pessoais entre a Europa e os EUA. Trata-se da exigência, por parte dos EUA, de as companhias de aviação europeias enviarem aos serviços de fronteiras americanos uma série de informações relativas aos passageiros de voos de e para aquele país.

O parecer do Grupo foi, em larga medida, negativo, por: se considerar excessivo o elenco de dados (alguns sensíveis) pedido; se entender desproporcionado o prazo de conservação desses dados proposto – apesar da sua redução final para 3, 5 anos; se ter por indesejável e perigosa a falta de identificação rigorosa das entidades judiciais e, sobretudo, policiais, às quais os serviços fronteiriços americanos poderiam transmitir as informações em causa.

Como é sabido, a Comissão Europeia não assumiu o essencial deste parecer, tendo emitido uma decisão a qualificar as autoridades fronteiriças americanas como fornecendo protecção adequada para o tratamento destes dados, no que foi seguida pelo Conselho Europeu, que celebrou um acordo com os EUA estipulando as regras do envio dos dados em questão. O problema não está ainda definitivamente resolvido, pois o Parlamento Europeu recorreu destes actos comunitários para o Tribunal de Justiça, estando este processo ainda pendente.

O Grupo elaborou, ademais, pareceres gerais sobre três dos tipos de tratamentos de dados que actualmente têm suscitado mais atenção e, por vezes, controvérsia, a saber:

- a videovigilância, em que procurou sugerir soluções em que devidamente se ponderassem os interesses da segurança de pessoas e bens e os da protecção da imagem enquanto dado pessoal;
- os dados genéticos, a propósito dos quais se realçou a natureza familiar ou grupal que podem assumir, e não puramente individual; e, além disso, se apontou no sentido de, em princípio, não deverem ser utilizados para fins de admissão de trabalhadores e de contratação de seguros;
- os dados biométricos, sobre os quais se ponderou, designadamente, poder a interconexão de diversos tipos de dados desta índole propiciar a configuração de perfis pessoais; e, ainda, que será preferível, como regra, e por razões de segurança, inserir dados deste tipo em cartões de uso individual, em vez de os aglutinar em grandes bases de dados centrais.

Emitiu-se, ainda, uma declaração sobre o terrorismo, salientando que o necessário combate a este fenómeno não deve sacrificar em demasia a defesa dos direitos fundamentais dos cidadãos.

Ao ser chamado, enfim, a pronunciar-se sobre a iniciativa de vários Estados-Membros sobre retenção de dados de tráfego para efeitos de investigação penal, o Grupo afirmou ter por desproporcionada a pretendida retenção da generalidade dos dados dessa natureza, bem como o prazo anual que vinha proposto.

Os pareceres e documentos de trabalho emitidos por este Grupo podem ser consultados em: http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index.en.htm

2.2 Telecomunicações

O Grupo de Trabalho Internacional de Protecção de Dados no sector das Telecomunicações (IWGDPT) existe há mais de 20 anos e reúne autoridades de protecção de dados, representantes de instituições e empresas de todo o mundo. Realiza duas reuniões por ano, uma das quais sempre em Berlim, onde está sediado o secretariado do grupo, com o apoio da autoridade de protecção de dados alemã.

A CNPD participa há muitos anos neste Grupo, que acompanha de perto todos os desenvolvimentos tecnológicos na área das telecomunicações e os problemas de protecção de dados daí decorrentes.

Em **2003**, o IWGDPT debruçou-se, em particular, sobre os sistemas de detecção de intrusão (IDS) e sobre os potenciais riscos associados à introdução do serviço ENUM, tendo adoptado dois documentos de trabalho com recomendações sobre o desenvolvimento de políticas específicas de privacidade e a observação dos princípios de protecção de dados na aplicação destas tecnologias.

O Grupo debateu ainda os serviços de autenticação em linha, as implicações da Convenção do Cibercrime, as comunicações móveis e a utilização de MMS, e reuniu os últimos desenvolvimentos em matéria de *e government*, de legislação de telecomunicações e de *spam*, tendo lançado ainda um questionário aos países participantes sobre os media e a privacidade, no sentido de actualizar a recomendação do Grupo de 1997 sobre essa matéria.

Em **2004**, o IWGDPT aprovou três recomendações relativas ao tratamento de imagens e sons por MMS, à liberdade de expressão e direito à privacidade nas publicações em linha, e à utilização de redes *wireless*.

O Grupo decidiu também fazer alterações à sua Posição Comum sobre privacidade e informação de localização nos serviços móveis de telecomunicações.

Foram ainda analisadas as questões de protecção de dados suscitadas pelas bases de dados *Whois*, pelo *Internet Protocol Version 6 (IPv6)*, pelos direitos de propriedade intelectual, pela videovigilância e pelos identificadores de radiofrequência.

Os documentos do IWGDPT podem ser consultados em http://www.cnpd.pt/bin/actividade/gt_tele.htm

2.3 Workshop sobre Queixas

A CNPD tem participado neste grupo de trabalho, que reúne as autoridades de protecção de dados dos Estados-Membros da UE, da Suíça, da Noruega, da Islândia e, mais recentemente, da Bulgária. Este grupo foi constituído, no âmbito da Conferência Europeia de Comissários de Protecção de Dados, com o intuito de trocar experiências práticas na resolução de casos concretos e reforçar a cooperação no tratamento

de queixas que envolvem mais do que um país comunitário. Neste sentido, a actividade do grupo desenrola-se essencialmente através da rede CIRCA (ver ponto 3.2 deste Capítulo), sendo organizadas, no entanto, duas reuniões anuais para uma discussão mais alargada dos temas e preparação do trabalho futuro.

Em **2003**, decorreram a VII e VIII Workshop, tendo sido debatidos temas como o tratamento de dados relativos ao crédito e solvabilidade; a troca de informações sobre clientes que contratam serviços móveis de comunicação; o tratamento de dados no sector bancário; o tratamento emergente de dados biométricos; e a comparação de legislações quanto aos fluxos internacionais de dados, tendo sido decidido estreitar a cooperação entre autoridades nesta área. Foi ainda abordado o trabalho das autoridades de protecção de dados em matéria de divulgação para o exterior e analisada a aplicação do princípio da proporcionalidade a casos concretos.

Em **2004**, na IX e X Workshop, esteve em destaque o papel dos oficiais de protecção de dados e o regime de notificação nos vários países; a actividade de auditoria e fiscalização, com a apresentação de um projecto de cooperação nórdica; o tratamento de dados pessoais pelos operadores dos serviços telefónicos; a monitorização no local de trabalho e as várias soluções adoptadas na transposição da Directiva das Comunicações Electrónicas.

Este Grupo decidiu também apresentar à Conferência Europeia uma proposta, no sentido de ver alargado o seu mandato, uma vez que, na prática, o seu trabalho há muito que extravasa o âmbito das queixas, tendo-se constituído no dia-a-dia como um verdadeiro centro de intercâmbio de informações quanto aos desenvolvimentos legislativos, mas sobretudo quanto às soluções adoptadas por cada autoridade na resolução de casos práticos. Tal permite, desde logo, uma maior harmonização de entendimentos e uma melhor cooperação perante situações reais, reforçando assim o nível da protecção de dados no espaço comunitário.

3. Cooperação internacional

3.1 Encontros ibéricos

A CNPD manteve, em conjunto com a Agencia de Protección de Datos Española (APDE), a continuidade desta iniciativa de se reunirem anualmente para trocar expe-

riências e informação, discutir questões emergentes na protecção de dados e estabelecer formas de cooperação mais aprofundada.

Iniciados no ano 2000, em Portugal, os encontros ibéricos de autoridades de protecção de dados têm dado frutos muito positivos ao nível da colaboração entre as duas autoridades. Realizam-se alternadamente em cada país, de forma descentralizada.

Assim, em **2003**, realizou-se o IV Encontro Ibérico, que teve lugar na localidade espanhola de Jarandilla de la Vera, onde foram debatidos, nomeadamente, os procedimentos de notificação, a utilização de dados genéticos, a tecnologia de radiofrequência, a transposição e aplicação da directiva de comunicações electrónicas.

O V Encontro Ibérico decorreu no Pinhão – Alijó, em **2004**, tendo as duas autoridades decidido realizar acções de fiscalização simultâneas a alguns sectores específicos de actividade, tais como o financeiro, o energético e o de saúde. Foi ainda decidido promover estratégias conjuntas contra o *spam* e colaboração na resolução de queixas. As duas autoridades acordaram também realizar acções de divulgação dos princípios de protecção de dados nos países ibero-americanos e de língua oficial portuguesa.

As conclusões dos encontros ibéricos podem ser consultadas em <http://www.cnpd.pt/bin/actividade/outros.htm>

3.2 Rede CIRCA

A CNPD participa, desde o ano 2001, com as autoridades europeias suas congéneres, numa rede virtual denominada CIRCA –, da responsabilidade da Comissão Europeia.

Esta rede integra vários grupos de discussão e de trabalho, que, através da Internet, trocam informações entre si. Tem grupos de acesso restrito e um espaço público, acessível em <http://forum.europa.eu.int/Public/irc/markt/Home/main>

A CNPD está presente, como membro, nos dois grupos relativos à protecção de dados: um ligado ao grupo de trabalho de queixas e outro, mais recente nesta rede, referente ao grupo de trabalho do artigo 29.º (Grupo de Trabalho de Protecção de Dados da UE).

A rede CIRCA tem sido um utensílio muito importante de cooperação, uma vez que tem permitido o intercâmbio rápido de informações, a partilha de casos, a difusão de

questionários, a procura de soluções comuns, a divulgação de práticas e de orientações de cada uma das autoridades de protecção de dados.

Nos últimos dois anos, a rede CIRCA tem sido intensamente utilizada, sendo trocada muita informação entre as autoridades dos vários países, designadamente quanto ao cumprimento noutros Estados da União Europeia das disposições de protecção de dados por parte de empresas que possuem mais do que um estabelecimento na UE.

O constante recurso à rede CIRCA demonstra bem as vantagens deste meio de comunicação, que contribui claramente para uma maior harmonização na aplicação das disposições de protecção de dados pessoais e uma melhor colaboração entre as autoridades.

3.3 Grupo tripartido “Spam”

Por iniciativa da Comissão Europeia, foi criado em **2003** um grupo europeu tripartido para discussão das matérias relativas às comunicações electrónicas não solicitadas (*spam*).

Esse grupo de trabalho integra as autoridades de protecção de dados, as autoridades de regulação no sector das telecomunicações e as associações de consumidores.

A CNPD, enquanto autoridade de protecção de dados portuguesa, foi convidada a participar neste grupo. Nesse âmbito, esteve presente, em 2003 e 2004, em três reuniões, em Bruxelas, onde se discutiu, sob diferentes perspectivas, a questão do *spam*. Em análise, estiveram a transposição da Directiva das Comunicações Electrónicas (Directiva 2002/58/CE), os poderes e competências de cada autoridade e a sua coordenação, os regimes sancionatórios, os mecanismos de cooperação entre os Estados na apreciação de queixas internacionais.

Este grupo teve reuniões com o Departamento de Comércio dos Estados Unidos (FTC) e com a Associação Europeia de Fornecedores de Acesso à Internet (Euro ISPA) para discutir o papel desempenhado por cada entidade no combate contra o *spam*, bem como explorar formas de cooperação.

A Comissão Europeia manifesta-se empenhada no combate eficaz ao fenómeno do *spam*, para o qual é necessário fazer convergir esforços, por parte das autoridades de

protecção de dados, das entidades reguladoras das telecomunicações e por parte dos consumidores, e actuar em conjunto, dentro dos Estados e no plano europeu.

3.4 Rede de peritos em TIC

Em **2004**, por proposta da nossa comissão congénere francesa (CNIL), foi criada uma rede informal de peritos das autoridades de protecção de dados em tecnologias de informação e comunicação.

Dado o ritmo das inovações tecnológicas, as competências técnicas das autoridades e o alto nível de *expertise* exigido em todas as áreas, exigia-se criar condições para que os peritos das autoridades pudessem trocar informações e pontos de vista, de modo expedito e prático.

Deste modo, a CNIL promoveu, em Junho do ano passado, uma reunião ao nível europeu para a criação desta rede. A CNPD esteve presente e veio a integrar este grupo, que se debruça sobre as novas tecnologias e os métodos operacionais utilizados no plano da fiscalização, funcionando essencialmente na base do correio electrónico para trocar informações.

3.5 Rede Ibero-Americana

A CNPD participou, pela primeira vez, no Encontro (o 3.º) Ibero-americano de Protecção de Dados de 2004.

Não fora possível participar nos anteriores devido aos constrangimentos financeiros vigentes.

Estes encontros têm-se realizado sob a égide da Agencia de Protección de Datos espanhola, e têm como objectivo principal divulgar o interesse e empenhamento pela protecção de dados nos países latino-americanos.

Neste III Encontro, realizado em Cartagena de Índias (Colômbia), de 25 a 28 de Maio de 2004, participou o Presidente da CNPD.

Nele estiveram representadas as autoridades de protecção de dados de Espanha, Portugal e Argentina.

Em mais nenhum dos países latino-americanos existem, até ao presente, instituições deste tipo – pelo que os intervenientes desses Estados foram universitários e responsáveis dos departamentos oficiais mais interessados neste tipo de problemas.

Foram nomeadamente discutidas matérias relativas à protecção de dados e o sector financeiro; ao chamado “spam”; às transferências internacionais de dados; à Internet.

Reiterou-se a importância da recém-criada Rede Ibero-americana de Protecção de Dados, e criaram-se no seu âmbito vários grupos de trabalho, destinados a aprofundar a abordagem da protecção de dados em termos práticos e funcionais.

3.6 Outras actividades

Em Fevereiro de **2003**, a pedido do Serviço de Estrangeiros e Fronteiras, a CNPD disponibilizou um técnico para integrar, como perito português, a Comissão de Avaliação da Aplicação da Convenção Schengen em Espanha. No primeiro semestre desse ano, Espanha foi sujeita a uma avaliação da União Europeia no âmbito de Schengen. A Comissão de Avaliação é composta por elementos de vários Estados-Membros, que elaboram um relatório final sobre a forma como estão a ser aplicadas as disposições da Convenção Schengen em vários campos.

Em Setembro de **2004**, a CNPD recebeu, nas suas instalações, a visita de uma delegação do Garante per la Protezione dei dati personali, autoridade italiana de protecção de dados. A delegação era constituída pelo vice-presidente Prof. Giuseppe Santaniello, pelo vogal Prof. Gaetano Rasi e pelo Director do Departamento Liberdade e Saúde, Cláudio Fillipi.

Em Outubro de **2004**, realizou-se no Ministério dos Negócios Estrangeiros uma reunião entre o Presidente da CNPD e representantes do departamento de reforma legislativa do Reino Unido, sobre a eventual necessidade de alteração da Directiva de Protecção de Dados (Directiva 95/46/CE).

4. Participação nas conferências de protecção de dados

4.1 Conferência da Primavera

2003

A Conferência da Primavera, que reúne os comissários de protecção de dados europeus, teve lugar em Sevilha, em 3 e 4 de Abril.

Abordaram-se várias questões gerais de relevo para a protecção de dados pessoais, bem como outras, mais específicas, de particular actualidade.

De entre as primeiras, discutiu-se o tema das competências das autoridades de protecção de dados – tendo-se nomeadamente verificado as grandes disparidades a este respeito existentes.

Analisou-se, ainda, a implementação da Directiva 95/46/CE. A representação da Comissão Europeia apresentou a este propósito um relatório, que revelou, por um lado, assinaláveis insuficiências na execução deste instrumento comunitário, e, por outro, as não poucas divergências de interpretação detectadas na sua aplicação.

Quanto aos temas de actualidade, procedeu-se a uma apreciação da situação da protecção de dados pessoais nos países recém-admitidos na UE.

Discutiram-se, ainda, por vezes com veemência, os aspectos positivos e negativos das chamadas "*binding corporate rules*", destinadas a legitimar transferências de dados para países que não propiciem protecção adequada.

Trata-se de declarações unilaterais emitidas por empresas, nomeadamente grandes multinacionais, assegurando garantias relativamente a tais transferências, sobretudo incidentes sobre dados relativos a trabalhadores.

O núcleo da questão é o da natureza vinculativa (ou não) dessas declarações.

2004

A Conferência da Primavera de 2004, realizada a nível europeu, teve lugar em Roterdão, de 21 a 23 de Abril desse ano.

Discutiram-se alguns temas básicos relativos à organização e funcionamento das autoridades de protecção de dados, tendo-se nomeadamente adoptado uma perspectiva comparativa acerca das experiências dessas instituições.

Abordou-se, por um lado, a questão do papel das referidas entidades. Ressaltou, a final, a assinalável variedade das concretas competências das várias autoridades.

A semelhante conclusão se chegou quando se expôs e discutiu o problema da execução das tomadas de posição das autoridades de protecção de dados dos países representados na Conferência.

Quando, de seguida, se abordou a problemática da comunicação das autoridades com o “mundo exterior”, foram patentes as grandes deficiências e limitações que nos vários Estados a este respeito ocorrem.

O representante da Comissão Europeia publicitou, enfim, os resultados do inquérito realizado pelo Euro barómetro acerca da consciência sobre as matérias de protecção de dados revelada pelos cidadãos e responsáveis por tratamentos dos diversos países da UE.

Os resultados do inquérito foram de um modo geral bastante desencorajantes, situando-se Portugal entre os países em que aquela consciência era mais fraca.

4.2 Conferência internacional

A CNPD não participou na Conferência Mundial de 2003, que teve lugar em Sidney (Austrália), em virtude dos encargos que as deslocações envolveriam.

A Conferência Mundial de **2004** ocorreu em Wroclaw (Polónia), de 13 a 16 de Setembro.

A Conferência ocupou-se de algumas questões básicas de protecção de dados pessoais, e, ainda, de certos aspectos de maior actualidade nesta área.

Sob a primeira perspectiva, trataram-se os temas da contraposição entre a privacidade e a defesa da segurança nacional; da cooperação entre as autoridades de protecção de dados; das relações entre os meios de comunicação social e a protecção de dados; do acesso aos arquivos das polícias políticas de regimes autoritários afastados.

No tocante às questões de maior actualidade, abordaram-se, designadamente, as incidências em termos de protecção de dados da identificação por radiofrequência (RFID); da biometria; do “marketing politico” e do controlo das comunicações dos trabalhadores no local de trabalho.

O Presidente da CNPD foi moderador na sessão dedicada ao último dos mencionados temas.

Foi ainda aprovada uma resolução chamando a atenção para a necessidade de a protecção de dados pessoais relevar também na área da cooperação judicial e policial.

Deliberou-se, enfim, admitir como membros da Conferência Mundial a Coreia, a Catalunha e a Autoridade Europeia para a Protecção de Dados.

P A R T E I I
O R I E N T A Ç Õ E S
D A C N P D

2 0 0 3

1 – TRATAMENTO DE DADOS POR PARTE DE PARTIDOS POLÍTICOS

Um partido político solicitou à CNPD autorização para efectuar um tratamento de dados pessoais com a finalidade de proceder ao *registo de militantes com aplicação de número utilizável para envio de correspondência, quotização, realização de eleições e outras actividades internas*.

Os dados pessoais objecto de tratamento eram: *nome, morada, contactos, número de Bilhete de Identidade e data da emissão, número de eleitor, nascimento, naturalidade, habilitações e situação profissional, sindicato, sócio de instituições, autarca, valor da quota e quais as áreas de interesse*.

Quanto ao *número de eleitor*, entendeu a CNPD que as necessidades de organização do procedimento eleitoral, nomeadamente as relativas à designação de elementos que componham as mesas de voto, configuram um caso em que a qualidade dos dados pessoais recolhidos se afigura *adequada, pertinente e não excessiva* (alínea c) do n.º 1 do artigo 5.º da Lei n.º 67/98, de 26 de Outubro). Tendo como condição de legitimidade o consentimento (proémio do artigo 6.º da Lei n.º 67/98, de 26 de Outubro), a CNPD considera que o tratamento do dado pessoal *número de eleitor* não atenta contra a Lei n.º 67/98, de 26 de Outubro.

No entanto, quer a *ficha de adesão*, quer a *ficha de actualização de dados*, indagavam sobre o sindicato em que o militante estava inscrito.

A *filiação sindical*, apesar de ser considerada um dado sensível e proibido o seu tratamento (n.º 1 do artigo 7.º da Lei n.º 67/98, de 26 de Outubro), foi autorizada tratar pela CNPD porque se verificou haver *consentimento expresso do titular dos dados* e porque foram asseguradas garantias de não discriminação e medidas especiais de segurança (n.º 2 do artigo 7.º da Lei n.º 67/98, de 26 de Outubro).

Mas a *filiação sindical*, entendeu a CNPD, não é tratada constitucionalmente como liberdade política. Na óptica da Comissão, a condição de *filiado em partido político* ou de *filiado em sindicato* representavam situações distintas que podiam encontrar-se cumulativamente na esfera jurídica de uma mesma pessoa. Quando assim fosse, entendeu a CNPD ilegítimo que se perguntasse sobre a condição de *filiação sindical*, sem que se fizesse menção a que a pergunta era de resposta facultativa.

Já sobre a qualidade de sócio de alguma associação ou cooperativa, entendeu-se que o tratamento destes dados se revelava *adequado, pertinente e não excessivo* (alínea c) do n.º 1 do artigo 5.º da Lei n.º 67/98, de 26 de Outubro) porque, tendo como condição de legitimidade o consentimento (proémio do artigo 6.º da Lei n.º 67/98, de 26 de Outubro), a CNPD considerou que o tratamento deste dado pessoal não atenta contra a Lei n.º 67/98, de 26 de Outubro (**Autorização 1/2003**).

2 – Tratamento de dados por parte de sindicatos

A relevar a especificidade do tratamento do dados pessoal sensível “*filiação sindical*, na notificação por um sindicato de um tratamento que tinha como finalidade o «registo de imigrantes para ajuda à integração social e profissional em Portugal» e em que os dados tratados eram a “*identificação do imigrante (nome, nacionalidade, idade, sexo, n.º de passaporte), profissão e residência no país de origem e em Portugal, habilitações escolares/profissionais, vínculo laboral, entidade patronal, vencimento, contacto e sindicato que o representa*”, a CNPD exigiu que para ser tratada informação sobre filiação sindical, embora com a perspectiva de encaminhamento do cidadão, devia ser obtido o consentimento do titular dos dados para realizar esse tratamento (cf. Artigo 35.º n.º 3 da CRP e 7.º n.º 3 al. b) da Lei 67/98). Esse direito de informação e o consentimento subsequente deviam ser obtidos no respectivo impresso de recolha. (**Autorização 510/2003**).

Num outro caso, a Comissão Sindical de um banco veio pedir à CNPD a emissão de parecer sobre a seguinte questão: saber se o Sindicato – enquanto responsável pelo tratamento de dados dos seus associados/filiados – podia facultar às Comissões Sindicais de empresa a listagem dos seus filiados.

O contacto entre o sindicato e os seus filiados podia ser realizado através de afixação da informação na empresa (v.g. em locais para esse fim estabelecidos) ou através da *distribuição* pelos associados.

Saber se a distribuição de informação sindical devia ser personalizada e se a Direcção podia facultar a listagem de todos os trabalhadores sindicalizados à Comissão Sindical de Empresa era uma questão que devia ser resolvida em função da *obrigação de informar* – que está atribuída às associações sindicais – e do *direito de ser informado*, que está subjacente aos princípios que regem o exercício da actividade sindical. Estes direitos deviam, ao mesmo tempo, ser compatibilizados com a Lei 67/98, de 26 de Outubro.

A questão que se colocou foi a de saber se, em face das disposições citadas do DL 215-B/75 e dos Estatutos, se podia concluir-se que existia uma «obrigação de comunicação» dos dados de identificação dos associados à Comissão Sindical da Empresa.

Reconheceu-se que a falta de acesso a estes dados, por parte da Comissão Sindical, não inviabilizava, de forma absoluta, o exercício das suas atribuições e competências, nem o exercício da actividade sindical no interior da empresa. Em face do exposto, afigurou-se à CNPD que não havia qualquer disposição que permitisse concluir no sentido de que existia uma «obrigação de comunicação» dos dados dos associados à Comissão Sindical. Por outro lado, importava salientar que a não comunicação da listagem de filiados à Comissão Sindical não inviabilizava o cumprimento da obrigação de informar, nem se apresenta como um obstáculo ao direito de ser informado.

Efectivamente, não sendo a Comissão Sindical um órgão do Sindicato (cf. Artigo 21.º) não podemos deixar de considerar, à luz do artigo 3.º alínea f) da Lei 67/98, que a Comissão Sindical assume a qualidade de «terceiro» em relação ao tratamento de dados da responsabilidade do Sindicato.

Por isso, à luz do artigo 7.º n.º 3 al. b) da Lei 67/98 a Comissão Sindical *só poderá ter acesso à referida listagem se obtiver o consentimento dos titulares dos dados*.

Numa outra perspectiva, importava reconhecer que o «direito de ser informado» tem, igualmente, uma outra vertente que não podia ser desprezada e que, no caso em apreço, devia ser equacionada: a possibilidade de o associado, independentemente de exercer os seus direitos enquanto filiado no sindicato, poder optar pelo «direito de não ser informado».

Neste domínio admitimos, por força do 12.º da Lei 67/98, que os filiados haviam de poder opor-se ao envio de qualquer comunicação que lhe seja endereçada pelo Sindicato ou por alguém em seu nome. Para que o trabalhador se possa opor a tal utilização é necessário que seja informado previamente (cf. Artigo 10.º da Lei 67/98)

sobre todas as finalidades do tratamento e sobre os destinatários ou categorias dos destinatários dos dados.

Em face do exposto, a CNPD considerou que – *na falta de consentimento expresso e informado dos titulares dos dados* – não havia razões legais ou estatutárias que permitissem, à luz da Lei 67/98, de 26 de Outubro, o fornecimento à Comissão Sindical de Empresa de «listagem de trabalhadores no activo no Banco por parte do Sindicato. (**Deliberação 118/2003**).

.....

A Comissão analisou ainda uma outra situação em que um Centro Distrital de Solidariedade e Segurança Social solicitou à CNPD a emissão de parecer sobre a seguinte questão: “O Sindicato dos Trabalhadores da Função Pública requereu uma lista *de todo o pessoal do serviço*» para «actualizar os ficheiros».

Não pareceu ser possível que ao Sindicato pudessem ser comunicados dados pessoais dos trabalhadores, sem que os mesmos tivessem sido informados sobre aquele destinatário e sem que tivessem consentido tal comunicação (cf. Artigo 6.º da Lei 67/98), pelo que a CNPD não autorizou o Centro Distrital de Solidariedade e Segurança Social a facultar ao Sindicato dos Trabalhadores da Função Pública uma lista *de todo o pessoal seu serviço*. (**Deliberação 120/2003**).

3 – ACESSO À BASE DE DADOS DO RECENSEAMENTO ELEITORAL (BDRE)

a) *Por partido político*

Um partido político solicitou à CNPD autorização para que lhe sejam facultadas as moradas dos eleitores, de forma a possibilitar a fiscalização do recenseamento e o contacto com os eleitores, adiantando que se tratava de um «*dado indispen-sável com uma finalidade legítima e de interesse público relevante, não incom-patível com a finalidade que determinou a recolha de dados*».

Entendeu a CNPD que – *para fins de fiscalização do recenseamento* – não existia fundamento legal que permitisse a um partido político ter acesso generalizado às moradas de todos os eleitores. Em situações específicas e concretas, apreciadas

caso a caso pela comissão recenseadora, admite-se que seja pertinente e necessário (cf. Artigo 5.º n.º 1 al. b) e c) da Lei 67/98) o acesso ao dado morada *para instruir a reclamação ou o recurso* – cf. Artigos 57.º, 60.º e 61.º – mas o dado «morada» só poderá ser utilizado para essa finalidade (cf. Artigo 5.º n.º 1 al. b) da Lei 67/98), devendo a mesma ser eliminada logo que seja apreciada a reclamação ou decidido o recurso (cf. Artigo 5.º n.º 1 alíneas d) e e) da Lei 67/98).

Quanto à autorização ao acesso aos nomes e moradas constantes da BDRE para fins de «contacto com os eleitores» residentes em território nacional, considerou a CNPD que se estava perante um caso de utilização de dados pessoais para fins não determinantes da recolha, isto é, com desvio da finalidade.

Como questão prévia, importava saber se a finalidade requerida – «propaganda política» – devia considerar-se incompatível com a finalidade assinalada à BDRE, acima mencionada, visto que, nos termos da alínea c) do n.º 1 do art. 5.º da Lei da Protecção de Dados, os dados pessoais não podem ser tratados de forma incompatível com as finalidades para os quais são recolhidos.

Parece possível delimitar a finalidade (propaganda política) e cingi-la a uma finalidade de propaganda eleitoral, exercida, por isso, num período de tempo delimitado legalmente (campanha eleitoral). O dado morada recolhido para fins de recenseamento eleitoral pode, assim, ser utilizado para uma finalidade ainda conexas com a finalidade de recolha: o exercício da propaganda eleitoral. Mantém-se, por isso, a ideia de que a finalidade da BDRE pode servir o processo eleitoral no seu todo, incluindo, neste caso, a realização da propaganda eleitoral constitucionalmente garantida.

Por se considerar que a finalidade de campanha eleitoral é ainda conexas, e não incompatível, com a finalidade da BDRE, a CNPD pôde autorizar, caso a caso, a comunicação dos dados em causa.

Tendo ficado assente que a finalidade de realização de «contacto com os eleitores» por parte de um partido, em período de campanha eleitoral, representava uma finalidade diversa da determinante da recolha, *ainda que compatível com a finalidade originária*, interessava saber se se justificava que a CNPD, utilizando os poderes que a lei lhe confere (cf. Artigo 23.º n.º 1 alínea c) e artigo 28.º al. d) da Lei 67/98) devia autorizar, *excepcionalmente*, o desvio de finalidade que permitisse a comunicação dos dados «nome» e «morada» de cidadãos eleitores residentes em território nacional, constante da BDRE, aos partidos políticos, para efeitos de propaganda eleitoral durante o período pré-eleitoral de campanha.

Tal como assinalámos, a Lei 13/99, de 22 de Março, só permite aos partidos políticos a obtenção de cópia dos cadernos de recenseamento (artigo 29.º n.º 1 al. c). Estes cadernos de recenseamento, conforme consta do anexo à Lei 13/99 não contêm a morada dos eleitores. Neste contexto, não parece que seja legítimo concluir – contrariamente ao que acontecia para os eleitores residentes no estrangeiro (cf. Artigo 54.º n.º 1 al. c) da Lei 13/99 e artigos 3.º e 4.º do DL 95-C/76, de 30 de Janeiro) – que existe na lei disposição que aponte para a possibilidade de utilização da morada, constante da BDRE, para fins de propaganda política levada a efeito pelos partidos.

A questão que se coloca é de saber se, perante os direitos reconhecidos aos titulares dos dados, há justificação para a CNPD autorizar a cedência da morada dos eleitores residentes em território nacional aos partidos políticos para a referida finalidade.

Dispõe o artigo 35.º n.º 2 da Constituição da República que «a lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado». O artigo 2.º da Lei 67/98 consignou, como princípio geral, que o tratamento de dados «deve processar-se de forma transparente», adiantando o artigo 5.º n.º 1 al. a) que os dados pessoais devem ser tratados «com respeito pelo princípio da boa-fé». Por outro lado, tem sido entendido de forma pacífica que o «direito de informação» é um dever fundamental que impende sobre o responsável do tratamento, o qual deve elucidar os titulares dos dados, no momento da recolha (artigo 10.º n.º 1), quanto às finalidades do tratamento e aos destinatários ou categorias de destinatários dos dados.

Não prevendo a Lei 13/99 qualquer possibilidade de acesso, por parte dos partidos políticos, à morada dos eleitores para fins de contacto no âmbito de campanha eleitoral, teremos que concluir que os titulares dos dados não admitiram que este tipo de utilização pudesse vir a ser considerado pelo responsável pelo tratamento. Ora, nos termos do artigo 12.º al. b) da Lei 67/98, quando estamos perante uma possível utilização de dados para esta finalidade, deve ser reconhecido ao titular – antes da comunicação dos seus dados a terceiros – o direito de oposição em relação à possibilidade de fornecimento dos seus dados a todos ou alguns partidos políticos.

Enquanto este direito de oposição não for assegurado, *nomeadamente por disposição legal ou no momento da recolha de dados*, considera a CNPD que não

deverá autorizar o acesso aos partidos políticos para as finalidades de propaganda política. Não se nos afigura desejável que, sem terem sido assegurados o *direito de informação* (artigo 10.º n.º 1 e 2) e o *direito de oposição* (artigo 12.º da Lei 67/98), que os eleitores sejam confrontados com propaganda política não desejada. Acresce, por outro lado, que a comunicação da morada não se apresenta como «indispensável ao destinatário para cumprimento da finalidade que com eles se propõe atingir na medida em que dispões de outros meios para divulgar a sua mensagem aos eleitores e, assim, «concorrer para a formação da vontade popular».

Em face do exposto deliberou a CNPD não autorizar o fornecimento da morada dos eleitores residentes em território nacional, constante da DBRE. (**Deliberação 97/2003**).

.....

b) *Por motivos de saúde pública*

O Instituto Nacional de Saúde Dr. Ricardo Jorge veio solicitar autorização para acesso à base de dados do STAPE em relação a eleitores de vários concelhos, uma vez que a Resolução da Assembleia da República n.º 34/2001, de 2 de Maio, recomendou ao Governo que tomasse as medidas concretas para “resolver o problema da radioactividade nos resíduos e nas minas de urânio abandonados nos distritos de Coimbra, da Guarda e de Viseu”.

De entre essas medidas foi recomendado que fossem submetidas as comunidades locais a “vigilância epidemiológica activa para garantir uma minimização de riscos, tendo em conta a radioactividade e a poluição química”.

A autorização da CNPD apreciou as condições concretas em que o estudo se iria realizar, designadamente um amplo esclarecimento junto da população e uma selecção aleatória das amostras.

A CNPD considerou que a finalidade não era incompatível com a finalidade que determinou a recolha e acolheu o princípio da justificação social. Neste sentido, autorizou o acesso exclusivamente para as finalidades indicadas, não podendo as informações ser posteriormente tratadas para fins diversos. (**Autorização 6/2003**).

c) *Para processo de inquérito*

A Inspeção Geral da Educação dirigiu-se à CNPD solicitando informação relativa à *morada* de uma ex-aluna, constante da Base de dados do Recenseamento Eleitoral (BDRE).

Invocando o decurso de um *processo de inquérito* numa Escola Profissional, mencionou como fundamento o n.º 2 do art. 36.º do Estatuto disciplinar aprovado pelo DL 24/84 de 16.01 (*“o instrutor poderá ordenar, oficiosamente, as diligências e os actos necessários à descoberta da verdade material”*), o n.º 12 da Portaria 207/98 de 28 de Março, do n.º 1 do art. 2.º do DL 4/98 de 08.01 e do art. 30.º do DL 271/95 de 23 de Outubro.

O pedido da Inspeção-Geral de Educação para identificação da *morada* de uma ex-aluna reuniu, no entender da CNPD, as condições necessárias à comunicação desse mesmo dado por parte do STAPE.

Quando um serviço da Inspeção Geral de Educação pretender instaurar processos de inspecção, e atendendo à abertura do disposto no art.º 30 do Decreto-Lei 271/95 de 23 de Outubro que aprova a Lei orgânica da Inspeção-Geral da Educação, poderá o STAPE comunicar o dado *morada* à Inspeção-Geral da Educação. Dispondo esta de poderes alargados que podem ser utilizados para apurar o correcto funcionamento do sistema educativo, e sendo considerada autoridade pública para efeitos de protecção criminal, permitindo-lhe mesmo solicitar a colaboração de quaisquer entidades públicas, judiciais, administrativas ou policiais, no desempenho de funções inspectivas, por maioria de razão deveria poder ter conhecimento de uma informação não sensível como a *morada*. (**Deliberação 124/2003**).

d) *Para promoção de eventos culturais*

A Câmara Municipal de Portimão pretendeu distribuir aos habitantes com mais de 65 anos, os guias, agendas e panfletos, de divulgação de iniciativas culturais destinados a este grupo populacional. Para esse efeito, veio solicitar autorização à CNPD para consultar a BDRE e fazer uso das *moradas*, a fim de poder endereçar os guias, agendas e panfletos.

Ponderada a pretensão, a Comissão entendeu que o envio de “guias, agendas e panfletos”, ainda que porventura relativos a iniciativas de índole cultural, pode não corresponder necessariamente ao interesse dos cidadãos seus eventuais destinatários.

Não se afigurou, por outro lado, que o acesso proposto fosse indispensável à autarquia requerente para o cumprimento das suas obrigações.

Esta Comissão entendeu, por estas razões, que não devia neste caso usar da faculdade excepcional prevista no art. 28.º, n.º 1, al. d) da Lei n.º 67/98, de 26 de Outubro, pelo que não autorizou o pretendido acesso à BDRE. (**Deliberação 101/2003**).

e) *Para inquérito à população*

A Junta de Freguesia de Nevogilde, pretendia fazer um inquérito à população idosa da Freguesia, com idade igual ou superior a 65 anos, com a finalidade de conhecer as necessidades ao nível da acção social desta camada da população. Para esse efeito veio solicitar autorização a esta CNPD para consultar a BDRE e fazer uso das moradas, a fim de poder endereçar os questionários.

Apurar a morada dos residentes na Freguesia para lhes ser endereçado questionário que seria preenchido de forma anonimizada e se destinava «ao conhecimento real desta população e das suas necessidades de forma a poder estudar serviços e equipamentos em falta na freguesia ou a elaborar protocolos com outras instituições», configurou-se como sendo uma razão de “interesse público” e que decorria do «princípio da justificação social». Neste caso concreto, entendeu a CNPD que o acesso à morada se podia revelar «indispensável ao destinatário para cumprir as suas obrigações legais». (**Deliberação 25/2003**).

4 – TRATAMENTO DE DADOS POR PARTE DE ENTIDADES PÚBLICAS E POLICIAIS

a) *Dados relativos a visitantes de reclusos*

O Estabelecimento Prisional de Santarém veio notificar a Comissão Nacional de Protecção de Dados (CNPD) de um tratamento de dados pessoais relativo a visitantes dos reclusos. A informação recolhida incluía: *nome, estado civil, data de*

nascimento, número do Bilhete de Identidade, data de emissão e arquivo emissor; profissão; morada; número de telefone; filiação; relação ou parentesco com o recluso a visitar. Esta informação serve de base à elaboração de um *cartão de visitante habitual*.

A finalidade determinante da recolha era a *segurança do estabelecimento prisional de molde a processar com maior fluidez as entradas para as visitas*.

O Decreto-Lei n.º 176/79, de 1 de Agosto regula a matéria das visitas a presos, dispondo, designadamente, que o regulamento interno disciplinará tudo quanto respeitar às visitas a estabelecimentos prisionais.

Porém, considerou-se inaceitável que o *cartão de visitante habitual* constitua condição essencial ou obrigatória para visitar reclusos. Esta injunção traduzir-se-ia numa violação às normas de protecção de dados pessoais, por consubstanciar um tratamento de dados pessoais excessivo em relação às finalidades (alínea c) do n.º 1 do artigo 5.º da Lei n.º 67/98, de 26 de Outubro).

Quanto aos dados recolhidos, tendo como propósito a emissão do *cartão de visitante habitual*, entendeu a Comissão que se manifestavam excessivos (alínea c) do n.º 1 do artigo 5.º da Lei n.º 67/98, de 26 de Outubro) os dados que se referiam à *profissão, morada, número de telefone, filiação, relação ou parentesco com o recluso a visitar*. Justificava-se, contudo, a recolha do dado cônjuge. (**Autorização 8 /2003**).

b) Acesso da PJ aos ficheiros da AP Seguradoras

A CNPD recomendou especiais cuidados para que a Associação Portuguesa de Seguradoras facultasse à PJ o acesso directo ao Ficheiro Nacional de Matrículas e ao Ficheiro Nacional de Sinistros e Fraudes Automóveis.

A APS veio solicitar à CNPD autorização para ser facultado o acesso directo à Polícia Judiciária ao Ficheiro Nacional de Matrículas e ao Ficheiro de Sinistros e Fraudes Automóveis no âmbito «da actividade de prevenção e investigação criminal, proceder à detecção de viaturas falsificadas, ou ilicitamente traficadas no estrangeiro, ou utilizadas em fraudes às seguradoras e outras entidades, ou por várias formas assinaladas como intervenientes em práticas criminosas».

Estes tratamentos, cujo funcionamento foi analisado pela CNPD nos termos da Autorização n.º 73/95, encontravam-se notificados. Nos termos da referida autorização apenas existia comunicação às seguradoras aderentes.

Verificou-se que o acesso pretendido consubstanciava um desvio em relação ao princípio da finalidade uma vez que o acesso à PJ não estava previsto, originariamente, nas finalidades destes tratamentos.

Em face das competências da Polícia Judiciária afigurou-se que, embora estivesse em causa a utilização para finalidades diversas, o acesso à informação centralizada pela APS se revelava como «compatível» com a finalidade que presidiu à centralização da informação.

Em face do exposto, autorizou a CNPD o acesso da PJ à informação constante do Ficheiro Nacional de Matrículas e de Sinistros e Fraudes Automóveis.

Pareceu excessivo, no entanto, à CNPD que se admitisse o «acesso ilimitado quanto ao número de utilizadores», devendo, ao invés, serem determinadas quais a pessoas que, de acordo com as funções desempenhadas (v.g. por estarem adstritos às tarefas de prevenção e investigação de crimes ligados ao ramo automóvel e seguros), necessitavam de ter acesso à informação, pois não se vislumbrava que fosse necessário um acesso generalizado a todos os funcionários da PJ.

A CNPD considerou, ainda, desejável que o protocolo especificasse *medidas de segurança que iriam ser adoptadas*, em particular, deveriam ser criados mecanismos específicos de *controlo aos utilizadores do sistema* (v.g. o registo aleatório de algumas consultas) ou a especificação da obrigatoriedade de a PJ – como decorre do artigo 8.º n.º 3 da Lei 67/98 – só fazer o respectivo acesso quando estivesse em causa a «prevenção de um perigo concreto ou repressão de infracção determinada».

Ademais, a informação – que circula na rede – devia estar protegida com sistemas de encriptação, evitando-se a interceptação e acesso por pessoas não autorizadas. **(Autorização 490/2003).**

c) *Introdução de dados no SI Schengen, no âmbito do EURO 2004*

A Polícia de Segurança Pública, no contexto do EURO 2004 e tendo presente a Decisão do Conselho da União Europeia de 25 de Abril de 2002, solicitou a esta Comissão parecer sobre a possibilidade de Portugal, com base no artigo 99.º da

Convenção de Aplicação do Acordo de Schengen (CAAS), inserir no Sistema de Informação Schengen os dados relativos aos adeptos de futebol que o Director da Joint Operational Authority, Sirene UK conhecia como sendo violentos, tendo em conta a necessidade de prevenção da ameaça e segurança pública que eles podiam constituir, no caso de se deslocarem para o nosso território nacional.

Na sequência do pedido, e como questão prévia à sua apreciação, a Comissão solicitou àquela Direcção Nacional informação sobre *«se o conhecimento que o Director da Joint Operational Authority, Sirene UK tem sobre os adeptos de futebol violentos, a serem transmitidos às autoridades portuguesas para serem indicados no Sistema Schengen, resulta de decisão judicial que tenha condenado os respectivos titulares por práticas violentas nesse âmbito ou de decisão administrativa das autoridades policiais?»* e sobre *«a existência, ou não, de acordo bilateral de cooperação entre as entidades policiais de Portugal e o Reino Unido e, em caso afirmativo, os termos do respectivo acordo»*.

Em resposta, e em suma, informaram que o conhecimento sobre os adeptos de futebol violentos a serem transmitidos às autoridades Portuguesas *«resulta da aplicação de decisões judiciais que impuseram interdições de vários tipos a diversos cidadãos do Reino Unido, na sequência de acusações e condenações pela prática de actos ilícitos directamente relacionados com o futebol e quer ocorreram dentro e fora do reino Unido»* e que *«não estando formalizado qualquer acordo bilateral de cooperação nesta matéria específica»*.

O Reino Unido aderiu parcialmente ao acervo de Schengen e a Decisão do Conselho, de 29 de Maio de 2000 (2000/365/CE), reconheceu o direito do Reino Unido participar no conjunto das disposições do acervo de Schengen relativas ao estabelecimento e funcionamento do Sistema de Informação Schengen, exceptuando as disposições relativas às indicações referidas no artigo 96.º da Convenção de 1990 e nas outras disposições a ele relativas (Cfr. artigo 1.º, ponto ii)). A inclusão a existir pretendia-se que fosse feita ao abrigo do artigo 99.º da CAAS.

Decorria do teor do ofício remetido pela Direcção Nacional da PSP que o que se pretendia era a introdução dos *«dados relativos aos adeptos de futebol que conhecem como sendo violentos»*. A CNPD considerou que o fundamento assim invocado era, por si só, insuficiente para justificar a indicação pretendida, uma vez que a inclusão dos dados dos adeptos a existir nos termos do artigo 99.º teria de estar suportada com base nos seguintes fundamentos:

- a) *indícios reais que façam presumir que a pessoa em causa tenciona praticar ou pratica numerosos factos puníveis extremamente graves;*
- b) *quando a apreciação global do visado, tendo especialmente em conta factos puníveis já praticados, permita supor que este praticará igualmente no futuro factos puníveis extremamente graves;*
- c) *ou, ainda sempre que indícios concretos permitam supor que as informações previstas no n.º 4 são necessárias à prevenção de uma ameaça grave pelo visado ou de outras graves para a segurança interna e externa do Estado.*

Era, desde logo, necessário que o facto praticado pelo adepto fosse extremamente grave ou que consubstanciasse uma ameaça grave.

Nesta conformidade, e com vista a prevenir ameaças à segurança pública, considerou a CNPD que o Estado Português poderia (e deveria) socorrer-se de outros instrumentos legais específicos para eventos desportivos da natureza do EURO 2004, sem prejuízo de outros que se quisessem adoptar e que o legitimasse a tratar a informação relativa aos adeptos de risco (Resolução do Conselho de 6 de Dezembro de 2001, a Decisão do Conselho (2002/348/JAI), de 25 de Abril, a Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, de 28 de Janeiro de 1981, a Recomendação n.º R(87) 15 do Comité dos Ministros de 17 de Setembro de 1987, que regulamenta a utilização de dados pessoais no sector da polícia, e a Convenção Europeia de 19 de Agosto de 1995, sobre a violência e os excessos dos espectadores por ocasiões das manifestações desportivas e nomeadamente de jogos de futebol, ratificada pela Resolução da Assembleia da República n.º 11/87, de 10 de Março).

Para fazer face a este tipo de fenómeno (hooliganismo) e sem prejuízo de poder ser utilizada em situações de criminalidade grave desde que verificados os demais pressupostos referidos no artigo 99.º, a CAAS não constitui o meio mais adequado (**Parecer 47/ 2003**).

- d) *Registo de menores estrangeiros em situação irregular no território nacional*

O Governo solicitou à CNPD a emissão de parecer sobre um projecto de Decreto-Lei que criava o registo nacional de menores estrangeiros que se encontrassem em situação irregular no território nacional.

O facto de se tratar de indivíduos menores e que se encontravam em situação irregular mereceu especial cuidado na abordagem do diploma. Mesmo não se tratando de dados pessoais sensíveis, não se pôde ignorar que o registo era de dados pessoais, de menores, em situação irregular, que viviam realidades muitas vezes marginais à sociedade, próximos de práticas e experiências marcadas pela ilicitude e ilegalidade (entrada e permanência irregular no território português por parte dos progenitores e familiares) e, portanto, em contextos já à partida e com frequência excludentes. Ainda que os dados a tratar não revestissem especial sensibilidade, a finalidade da sua recolha e do seu tratamento devia ser precisa e não podia ser de modo nenhum discriminatória.

Por outro lado, o registo destinava-se, nos termos do n.º 1 do art. 2.º do diploma em apreço, *“exclusivamente a assegurar o acesso dos menores ao exercício dos direitos sociais fundamentais, designadamente aos cuidados de saúde e à educação escolar.”*

Aparentemente, esta era a finalidade exclusiva do tratamento dos dados, pois os n.º 2 e 3 do mesmo art. 2.º do diploma em causa impediam a utilização dos dados recolhidos e tratados para fins diferentes, nomeadamente para fins judiciais e administrativos em que os progenitores dos menores estivessem envolvidos.

Porém, o n.º 2 do art. 2.º do Decreto-Lei em estudo fazia, logo no início do preceito, uma ressalva: *“Sem prejuízo do previsto no Decreto Lei n.º 244/98 de 8 de Agosto, republicado pelo Decreto Lei n.º 34/2003 de 25 de Fevereiro, em caso nenhum os elementos constantes deste registo poderão servir de fundamento ou meio de prova para qualquer procedimento, administrativo ou judicial (...)”*.

O Decreto-Lei n.º 244/98 de 8 de Agosto, republicado pelo Decreto-Lei n.º 34/2002 de 25 de Fevereiro, versava sobre uma longa série de matérias atinentes à entrada, permanência, saída e afastamento de estrangeiros do território português, fixando as regras de entrada e saída, nomeadamente de menores e seus familiares – art. 16.º, 56.º e seguintes do Decreto-Lei 244/98.

Tinha, ainda, o Decreto-Lei 244/98 normas de relevância sancionatória administrativa – art. 99.º a 126.º, de relevância jurídico-penal – art. 134.º a 137.º- D e de relevância contra-ordenacional – art. 140.º a 154.º.

Impedir que os dados tratados no registo criado por este diploma fossem fundamento ou meio de prova para qualquer procedimento administrativo ou judicial

em que os menores ou seus familiares fossem intervenientes e, ao mesmo tempo, salvar desse impedimento a matéria disciplinada pelo Decreto-Lei 244/98 de 8 de Agosto pareceu uma contradição que colocava em crise a garantia que a finalidade do tratamento, aparentemente, pretendia oferecer: a de que os dados recolhidos e tratados visavam exclusivamente o exercício de direitos sociais fundamentais e não quaisquer outros.

Pareceu conveniente homenagear a confiança na finalidade do tratamento, esclarecendo inequivocamente que o objectivo do tratamento não passava, nem sequer tangia, outro propósito que não fosse o acesso dos menores que se encontravam em situação irregular no território português ao exercício de direitos sociais fundamentais.

Por isso, a CNPD concedeu parecer favorável ao presente projecto de Decreto-Lei apenas no caso de, sendo eliminada a expressão inicial do n.º 2 do art. 2.º *“Sem prejuízo do previsto no Decreto Lei n.º 244/98 de 8 de Agosto, republicado pelo Decreto Lei n.º 34/2003 de 25 de Fevereiro”*, resultar muito claro que os dados não podiam ser utilizados para outras finalidades diferentes das indicadas no n.º 1 do mesmo preceito.

Quanto ao responsável pelo tratamento, dizia o n.º 2 do art. 3.º do diploma em apreço que *“Compete, com faculdade de delegação, ao membro do Governo responsável pela imigração e minorias étnicas a recolha, o tratamento e a manutenção dos dados recolhidos nos termos do presente diploma”*. Continuava, sob a mesma epígrafe da competência, o n.º 3 da mesma norma: *“Cabe ao Alto Comissariado para a Imigração e Minorias Étnicas, em articulação transversal com os serviços competentes da Administração Pública, garantir que os menores registados acedam ao exercício dos mesmos direitos que a lei atribui aos menores em situação regular no território nacional.”*

Por outro lado, dizia-se no pedido de parecer que o projecto de diploma resultava já de um entendimento final entre o Ministério da Presidência e o da Administração Interna.

Pareceu, pois, que a responsabilidade do tratamento era bipartida, entre o membro do Governo responsável pela imigração – o Ministro da Administração Interna – e o Alto-Comissário para a Imigração e Minorias Étnicas.

Apesar da responsabilidade conjunta pelo tratamento de dados estar prevista no art. 3.º al. d) da LPD, em proveito da transparência da finalidade do tratamento,

considerou a CNPD de todo vantajoso esclarecer a arquitectura que sobressai no presente diploma.

Inequivocamente, a CNPD considerou não ser adequado que o Ministério da Administração Interna, que tutela o Serviço de Estrangeiros e Fronteiras, órgão de polícia criminal com poderes de afastamento de estrangeiros e de instrução de processos administrativos, contra-ordenacionais e criminais, fosse a entidade (co-responsável pelo tratamento dos dados pessoais dos menores aqui em causa. Essa opção clarificava a finalidade e potenciava a confiança na recolha e tratamento dos dados pessoais dos menores que se encontrassem em situação irregular no território português, ficando sob condição dessa consideração o parecer favorável ao presente diploma.

Pareceu, finalmente, à CNPD, igualmente importante que o presente Decreto-Lei fixasse o tipo de dados que visava tratar, identificasse inequivocamente a entidade responsável pelo tratamento, previsse a proibição da comunicação e interconexão de dados (**Parecer 49/2003**).

5 – TRATAMENTO DE DADOS NO ÂMBITO LABORAL

a) *Código do Trabalho*

A Comissão de Trabalho e dos Assuntos Sociais solicitou à CNPD a emissão de parecer sobre o Código do Trabalho.

O artigo 17.º n.º 2, para além de admitir, numa formulação bastante genérica, excepções à não vinculação do trabalhador a fornecer informações sobre o seu estado de saúde – quando verificadas “ *particulares exigências inerentes à natureza da actividade profissional*” – deixava essa decisão «nas mãos» da entidade empregadora, sem que houvesse qualquer referência a uma «intervenção médica» ou enquadramento do pedido no âmbito dos serviços de higiene e saúde no trabalho. Impunha-se que fosse feita uma clarificação no sentido de que a solicitação «por escrito» e «a respectiva fundamentação» fossem subscritas por médico e que, tal como acontece com o n.º 3 do artigo 19.º, ao empregador só fosse revelada a aptidão ou inaptidão para o cargo.

Caso não fosse feita esta precisão, entendeu a CNPD que as disposições do artigo 17.º n.º 1 e 2 do Código contrariavam os artigos 26.º e 18.º n.º 2 da Constituição da República por a limitação da intimidade da vida privada dos trabalhadores se revelar excessiva, não adequada, desproporcionada e desnecessária, traduzindo-se numa efectiva aniquilação de um direito fundamental sem se atender aos princípios da «mútua compressão» que devia nortear a harmonização de direitos fundamentais. Entendeu a CNPD, por outro lado, que deveria ser eliminada qualquer possibilidade, no artigo 19.º n.º 3 *in fine*, de a entidade empregadora ter acesso a dados relativos a testes ou exames médicos, não se apresentando a autorização escrita do trabalhador como um «consentimento livre».

Contrariamente ao que prevê o artigo 19.º n.º 1, entendeu a CNPD que a realização de exames fora do contexto dos serviços de medicina do trabalho apresentava um grande perigo de proliferação de tratamentos de dados de saúde e da vida privada dos trabalhadores, com riscos acrescidos de exames “coercivos” desenquadrados de uma prevenção integrada de promoção e vigilância da saúde do trabalhador. Por outro lado, havia um risco acrescido de interconexão de tratamentos tendentes a integrar «informação exhaustiva» sobre o estado de saúde do trabalhador, na medida em que não estava regulada a relação de interdependência entre os médicos referidos no artigo 19.º n.º 3 e os médicos do trabalho.

Em face da declaração de inconstitucionalidade das normas do artigo 12.º n.º 1 e 2 do DL 231/98, de 22 de Julho, não pôde a CNPD deixar de manifestar a perplexidade pela forma genérica como se legitimava a utilização de «meios de vigilância electrónica», sem a mínima ponderação dos interesses em presença: a segurança de pessoas e bens e a reserva da intimidade da vida privada (direito à imagem/liberdade de movimentos). Por isso, entendeu a Comissão que a Assembleia da República deveria – em termos gerais – legislar sobre a matéria de videovigilância, regulamentando os aspectos enunciados, sendo desejável que o Código do Trabalho fizesse a remissão para o regime geral estabelecido ou consignar disposições específicas em matéria laboral no âmbito da videovigilância compatíveis com o regime geral aplicável.

Atendendo ao disposto nos artigos 17.º e 19.º seria admissível, em face das excepções legalmente estabelecidas, que o empregador exigisse que o candidato prestasse «informações sobre a sua vida privada» ou sobre a sua «saúde» (n.º 1 e 2 do

artigo 17.º) ou submetê-lo a «testes ou exames médicos de qualquer natureza», “quando particulares exigências inerentes à actividade o justifiquem” (n.º 1 do artigo 19.º). Esta formulação, especialmente, a do artigo 19.º pareceu poder legitimar a realização de testes genéticos, solução que, claramente, contrariava os princípios estabelecidos no ponto 2 alínea g) da Resolução da Assembleia da República n.º 47/2001 e violava, frontalmente, o artigo 12.º da Convenção sobre os Direitos do Homem e da Biomedicina, aprovada, para ratificação, pela Resolução da Assembleia da República n.º 1/2001. Por isso, considerou a CNPD que a lei deveria ser expressa e proibir de forma absoluta a realização de testes genéticos prévios à candidatura a emprego, sob pena de violação dos disposto nos artigos 13.º e 26.º da Constituição da República.

O artigo 23.º n.º 2 – norma excepcional em relação ao princípio geral de não discriminação em função do *património genético* contido no n.º 1 – era demasiado vago e permissivo, podendo dar origem a abusos por parte das entidades empregadoras e colocar em causa a autonomia e os direitos de personalidade do trabalhador. O preceito deveria ser compatibilizado com o artigo 12.º da Convenção sobre os Direitos do Homem e da Biomedicina – que apontava para a realização de testes genéticos com «fins médicos» – prevalecendo o interesse da saúde do trabalhador e de terceiros sobre «interesses empresariais» ligados às condições de «exercício da actividade profissional».

Por outro lado, a decisão relativa à necessidade de submissão aos exames genéticos, só admissível para situações muito excepcionais e devidamente fundamentadas, devia ser tomada no âmbito dos serviços de medicina do trabalho, após aconselhamento genético do trabalhador e numa base de voluntariado, com salvaguarda de que o resultado dos exames não deveria ser comunicado, em nenhum caso, à entidade empregadora (**Parecer 8/2003**).

.....

b) Medicina do trabalho antecedentes familiares

Foi solicitada à CNPD autorização para o tratamento de dados pessoais no âmbito da «saúde ocupacional». Além da doutrina da Comissão sobre esta matéria, importa salientar aqui que, em relação aos antecedentes familiares, considerou a

CNPD excessivo e violador da privacidade dos familiares (cf. artigo 1.º da Lei 67/98) a especificação – sem o seu consentimento (cf. artigo 7.º n.º 2 da Lei 67/98) – de dados de saúde de particular sensibilidade. Efectivamente, não se vislumbrou, em relação a certas doenças (v.g. toxicodependência e alcoolismo) a necessidade de as referenciar em relação ao pai, mãe, avós e irmãos. Também não se justificava a especificação do estado de saúde do cônjuge com o detalhe especificado.

Em face do exposto, considerou-se excessivo e desproporcionado o tipo de detalhe em relação a estes dados. **(Autorização n.º 480 /2003).**

6 – TRATAMENTO DE DADOS NO SECTOR DA SAÚDE

a) *Informação genética pessoal*

O Grupo Parlamentar do Bloco de Esquerda solicitou à Comissão emissão de parecer quanto ao Projecto de Lei n.º 28/IX, relativo a informação genética pessoal e informação de saúde.

Resultava do artigo 19.º, n.º 2 e n.º 3 a possibilidade de o consentimento dado pela pessoa junto da qual é obtido o material biológico ser conservado para efeitos de investigação e poder ser retirado e determinada a sua destruição por um seu familiar. Chamou-se a atenção para o facto de tal poder levar a situações que não eram compatíveis, designadamente quando a vontade do titular e da família não coincidiam. Entendeu a CNPD que o consentimento ou a eventual revogação, a existir, seria o da pessoa em causa, devendo este, em caso de conflito, prevalecer sobre o dos familiares.

Admitiu-se que após a morte do titular tal direito pudesse ser exercido pelos familiares, uma vez que a informação genética implicava informações de família. **(Parecer 2/2003).**

b) *Testes genéticos*

O Instituto de Biologia Molecular e Celular notificou o tratamento de dados com a finalidade de gestão de dados de saúde e dados genéticos em relação a pessoas que «hajam requerido consultas de avaliação clínica e aconselhamento genético, avaliação e acompanhamento psicológico e seguimento médico especializado,

com vista à possível realização de testes preditivos e pré-natais no âmbito de doenças neurológicas de início tardio, cancros familiares, hemocromatose e outras doenças hereditárias. O tratamento destes dados visava a melhoria da prestação de cuidados assistenciais mencionados e apoio à investigação clínica e genética destas doenças».

Distinguiram-se duas finalidades: as de diagnóstico e prestação de cuidados de saúde, por um lado, e a investigação clínica e genética de certas doenças, por outro.

Em relação ao tratamento de dados de saúde, admitia o artigo 7.º n.º 4 da LPD o seu tratamento quando fosse necessário para efeitos de “*medicina preventiva, de diagnóstico médico, de prestação de cuidados...* desde que o tratamento desses dados seja efectuado por profissional de saúde obrigado a sigilo profissional ou por outra pessoa igualmente sujeita a segredo profissional” e desde que fossem «garantidas medidas adequadas de segurança da informação».

Em relação à finalidade especificada no artigo 7.º n.º 4 devia ser dada especial atenção à necessidade de assegurar:

- O direito de informação e acesso aos titulares dos dados, nos termos do artigo 10.º e 11.º n.º 5 da lei 67/98);
- A separação lógica entre dados administrativos e dados de saúde (cf. artigo 15.º n.º 3 da Lei 67/98);
- Adopção das medidas de segurança que impedissem o acesso à informação de pessoas não autorizadas. A informação de saúde deveria ser de acesso restrito aos médicos ou, sob a sua direcção e controlo, a outros profissionais de saúde obrigados a segredo profissional (cf. artigo 7.º n.º 4).

O tratamento de dados de saúde e genéticos fora do contexto «assistencial», ou seja, para apoio à investigação clínica e genética devia observar as condições estabelecidas no artigo 7.º n.º 2 da Lei 67/98.

O consentimento teve que ser expresso por uma «*manifestação de vontade*» que materializasse um consentimento para a utilização dos dados para as finalidades de investigação. (**Autorização 495/ 2003**).

.....

C) *DADOS PARA INVESTIGAÇÃO CIENTÍFICA*

Um hospital veio notificar tratamentos de dados. De entre as notificações verificou-se que existiam alguns tratamentos em que os dados pessoais eram utilizados – para além de finalidades de diagnóstico e prestação de cuidados de saúde (cf. artigo 7.º n.º 4 da Lei 67/98, de 26 de Outubro) – para realização de estudos epidemiológicos ou científicos.

A utilização dos dados dos doentes para a realização de estudos epidemiológicos ou científicos – não englobada na previsão do artigo 7.º n.º 4 da Lei 67/98 – só podia ocorrer se fosse obtido o necessário consentimento informado por parte dos titulares dos dados ou dos seus legais representantes se forem menores ou sendo maiores se forem declarados pelo tribunal com incapacidade ou interditos (art.º 7.º n.º 2 da Lei 67/98 de 26.10). A dispensa de consentimento só poderia ocorrer se os estudos a realizar fossem feitos de forma anonimizada, isto é, quando os dados utilizados não permitissem a identificação dos titulares objecto de análise (artigo 35.º n.º 3 da Constituição da República Portuguesa).

Como se estava perante dados de saúde, face aos tratamentos aqui em apreciação, o acesso aos dados clínicos só podia ser facultado a profissional de saúde obrigado a sigilo profissional e desde que apresentasse suficientes garantias de que os dados pessoais dos utentes – que terão dado o seu consentimento – só seriam utilizados para aquela finalidade e que eram anonimizados logo que deixasse de ser necessária a identificação dos titulares dos dados.

Deviam ser criados mecanismos que assegurem a separação de dados clínicos dos restantes, medidas de segurança adequadas e, quanto aos prazos de conservação, deviam ser observados os princípios estabelecidos na Portaria 247/2000, de 8 de Maio. (**Autorização 497/2003**).

Num outro caso, dois médicos hospitalares vieram solicitar autorização para acesso a dados clínicos para realização de estudo epidemiológico, com vista a obter dados sobre a prevalência de neoplasias do tubo digestivo em doentes com doença inflamatória intestinal”. O estudo envolvia um universo de «vários Hospitais do Sul do País».

Tratava-se de um “estudo retrospectivo, baseado em resultados de inquéritos a médicos hospitalares e na colheita de dados em processos clínicos”. Os doentes

eram identificados “por iniciais e datas de nascimento”, não havendo saída nominal de dados pessoais de nenhum doente.

Enquadrando-se esta iniciativa na previsão do artigo 7.º n.º 2 da Lei 67/98, entendeu a CNPD que a utilização dos dados de saúde para finalidades de investigação clínica e epidemiológica subvertia, desde logo, o princípio da transparência e da informação que deve presidir a qualquer tratamento (cf. artigo 2.º e 10.º n.º 1 da Lei 67/98). Por outro lado, e atenta a sua natureza, exigia-se que a utilização destes dados pessoais devia assentar num consentimento expreso e informado dos titulares dos dados (cf. artigo 7.º n.º 2 e 3.º alínea h) da Lei 67/98).

Se for inviável ou impossível a obtenção do consentimento, seria tecnicamente possível transferir para um suporte magnético autónomo a informação pertinente, sem identificação dos doentes (*referenciados por iniciais e datas de nascimento*), não se tendo levantado qualquer objecção em termos de protecção de dados uma vez que o Hospital – enquanto responsável do tratamento – não estava a facultar dados nominativos.

Porém, em relação aos dados incluídos nas *fichas clínicas em suporte de papel* era inevitável que a recolha de dados e a respectiva anonimização para o estudo só pudesse ser efectuada através das fichas clínicas.

Deliberou a CNPD autorizar a recolha de dados, de forma anonimizada, devendo ser observadas as condições acima enunciadas e mediante a seguinte metodologia:

- a) A consulta dos processos clínicos era feita no próprio local onde tais documentos se encontravam, ou seja, no arquivo clínico ou no serviço que os detinha, não podendo ser fotocopiados ou dele ser retirados;
- b) Quaisquer apontamentos deviam ser “despersonalizados” (limitando-se a obter as iniciais do nome e a idade), sendo obrigatório que as conclusões e, em geral, os resultados que se elaborassem e divulgassem não permitissem identificar os titulares dos dados;
- c) O médico ou médicos responsáveis pela consulta do processo clínico deviam subscrever documento em que se identificassem todos os processos a que tivessem tido acesso, listagem que ficaria em poder do respectivo Hospital. (**Deliberação 35/2003**).

A Faculdade de Medicina de Lisboa veio notificar o tratamento relativo à investigação da doença de Parkinson. Nos termos declarados no processo, o tratamento pretendia “constituir uma rede europeia que optimizasse e coordenasse as competências já existentes na área da investigação clínica na doença de Parkinson, implementar a criação de centros de investigação clínica e o desenho e condução de ensaios clínicos no domínio da doença, através de construção de uma plataforma que facilitasse a condução de projectos de investigação multinacionais na Europa”.

Tratava-se, no fundo, de reunir um conjunto de dados clínicos sobre doentes de vários países, para futuro recrutamento de doentes para aderirem a futuros ensaios clínicos.

Analisado o processo verificou-se que o responsável era a Faculdade de Medicina de Lisboa; havia tratamento de dados de saúde recolhidos dos processos de consulta externa de neurologia do Hospital de Santa Maria por parte do médico assistente. Os dados pessoais não eram registados nem transferidos via Internet, só os dados clínicos anonimizados eram introduzidos na central de dados, de forma encriptada para um servidor na Alemanha, junto do coordenador do projecto.

A CNPD autorizou a Faculdade de Medicina de Lisboa a iniciar este tratamento automatizado de dados, nos termos referidos no processo e condicionados por esta deliberação, desde que os órgãos responsáveis pelo Europa ou quaisquer terceiros, não pudessem aceder à identificação dos doentes, a não ser os médicos do serviço de neurologia do Hospital de Santa Maria. (**Deliberação 89/2003**).

.....

Uma outra situação foi igualmente apreciada pela CNPD. Um laboratório farmacêutico veio notificar o tratamento que tinha como finalidade «observar as condições de utilização de um medicamento registando as suas condições de prescrição e o resultado do tratamento, conforme decisão da Agência Europeia do Medicamento».

Para tal, foi concebida uma aplicação informática que tinha como finalidade assegurar a monitorização e segurança do medicamento.

Houve a dizer, em primeiro lugar, que a entidade não tinha necessidade de proceder ao tratamento de dados nominativos dos pacientes para cumprir as exigên-

cias da decisão da Comissão Europeia. Efectivamente, os relatórios a elaborar não continham necessariamente informação nominativa, mas agregada.

O registo de doentes era feito pelo médico prescriptor, ficando os registos automatizados sujeitos às condições de legitimidade estabelecidas no artigo 7.º n.º 4 da Lei 67/98.

Não se enquadrando o tratamento de dados do laboratório no âmbito do diagnóstico, medicina preventiva ou prestação de cuidados de saúde, as condições de legitimidade tiveram de ser enquadradas na previsão do artigo 7.º n.º 2 da Lei 67/98.

Embora se tivesse admitido que as iniciais do nome do doente não permitiam, só por si e ligadas à data de nascimento, identificar o doente, afigurou-se que eram desnecessárias na medida em que a identificação se fazia pelo n.º de identificação do doente. Por isso, em função do disposto no artigo 5.º n.º 1 al. c) da lei 67/98, de 26 de Outubro o laboratório devia abster-se de registar as iniciais do doente.

A declaração de consentimento informado devia manter-se sempre em poder do médico prescriptor ou do estabelecimento de saúde onde este presta serviço, não tendo sido admitido que essa declaração fosse consultada pelo laboratório farmacêutico. (**Deliberação 106/ 2003**).

.....

Uma médica cardiologista veio notificar a CNPD de um tratamento que, numa primeira fase, teria como finalidade avaliar *“os resultados de uma campanha educacional para o controlo da hipertensão arterial”*, adiante designada de *“CERTA”* e, ainda, *“o envio de materiais da campanha (mailings)”* e, numa segunda fase, após anonimização dos dados, a realização de *“um estudo científico da população hipertensa”*.

Uma empresa farmacêutica, com base num protocolo de colaboração com a médica coordenadora da campanha, apoiava logística e financeiramente a campanha *“CERTA”*, disponibilizando os meios materiais e humanos necessários à sua implementação, designadamente procedendo, sob a orientação e direcção da coordena-

nadora, à elaboração dos ditos materiais, bem como procedendo à divulgação daquela junto da classe médica, suportando os custos decorrentes da mesma. Os resultados da campanha e do estudo que a médica pretendia desenvolver eram de reconhecido interesse científico pela empresa farmacêutica, que, entre outras, se dedicava à investigação e comercialização de terapêuticas para a saúde humana, designadamente na área cardiovascular.

A recolha de dados era feita tendo por base dois inquéritos: “*inquérito inicial*” e “*inquérito final*”. De acordo com estes eram recolhidos dados pessoais dos médicos assistentes (nome e centro de saúde) e dos participantes (nome, morada, idade, profissão, escolaridade, peso, altura, tensão arterial, hábitos de vida, tabagismos, exercício físico, consumo de álcool, de sal e de medicamentos, adesão ao tratamento, conhecimentos sobre hipertensão arterial e seu tratamento, satisfação com a campanha).

Os médicos que procedessem ao acompanhamento de doentes hipertensos seleccionavam os doentes os quais, caso concordassem, preenchiam o boletim de inscrição, juntamente com a declaração de consentimento e enviavam-no pelo correio, num envelope pré-pago para o Apartado da empresa farmacêutica patrocinadora do estudo, sendo considerados a partir desse momento como participantes da “*CERTA*”.

Constava da informação dada aos participantes, entre outros elementos, que “*As informações enviadas estão ao abrigo do segredo médico. O tratamento de dados poderá ser feito para fins científicos mas em nenhum caso serão identificados*”.

Importou, desde logo, referir que, pese embora a responsável pelo tratamento pretendesse enquadrar a campanha “*CERTA*” no conceito de medicina preventiva, considerou a CNPD, atendendo ao declarado no formulário de legalização, no protocolo celebrado e nos formulários de recolha, que o tratamento se enquadrava na previsão do artigo 7.º n.º 1 e n.º 2 da Lei acima referida, dado tratar-se de um estudo científico da população hipertensa.

De acordo com o n.º 2 do artigo 7.º, o tratamento de dados de saúde só era legítimo desde que fosse obtido o consentimento expresso dos titulares dos dados e com a adopção das medidas de segurança previstas no artigo 15.º.

Considerando que, no âmbito da campanha “CERTA”, foram recolhidos e processados informaticamente dados pessoais e de saúde relativos aos primeiros inquiridos, sem que os titulares dos dados tivessem dado o seu consentimento, tornou-se indispensável obter, ainda que «*a posteriori*», o consentimento, tendo tido o responsável o dever de proceder à distribuição da declaração de consentimento e de fixar um prazo para os titulares dos dados se pronunciarem, findo o qual, sem que o mesmo tenha sido obtido, os dados pessoais e de saúde relativos a esse(s) “*participante(s)*” deviam ser eliminados.

Atendendo ao facto de, com a campanha, a médica pretender efectuar um estudo sobre a população hipertensa em Portugal, encontrou-se, assim, por justificar designadamente a recolha dos dados relativos aos médicos.

Na medida em que para a realização da campanha em apreço eram recolhidos dados de saúde, considerados estes dados sensíveis, os quais durante o decurso da mesma não se encontravam anonimizados, por motivos de envios dos mailings, impôs-se que fossem adoptadas especiais medidas de segurança do tratamento (Cfr. artigo 7.º e artigo 15.º).

Nesta conformidade, devia ser utilizado um sistema de encriptação dos dados, por forma a que a informação aí processada apenas pudesse ser consultada, alterada, eliminada e utilizada pela médica responsável e/ou a sua colaboradora, através da introdução de uma chave de descriptação. (**Autorização 478/2003**).

d) *Dados relativos à vida privada*

O Serviço de Prevenção e Tratamento de Toxicodependência do Ministério da Saúde (SPTT) veio submeter a autorização da CNPD um tratamento que tinha como finalidade a «adopção de um sistema que visava permitir o tratamento estatístico de dados relativos aos utentes e actividade operativa da Instituição, a todo e qualquer momento, e facilitar a gestão diária dos processos nas unidades especializadas do SPTT».

O acesso difere de utilizador para utilizador do sistema, de acordo com os perfis de três níveis:

- I Os funcionários administrativos podem apenas lidar com a parte administrativa do sistema, ou seja, efectuar marcação de consultas ou alteração das mesmas, e obter as listagens das consultas marcadas para um dado dia;

II No nível intermédio, os técnicos do serviço social, os técnicos psicossociais e os técnico de diagnóstico terapêutico podem aceder, registar e alterar os dados sociodemográficos e de consumo, ficando apenas impedidos de aceder aos dados clínicos;

III Toda a ficha do utente, incluindo os dados clínicos, fica acessível unicamente aos terapeutas.

Havia tratamento de informação sobre a «situação judicial» e que englobava o inte detalhe:

- Julgamentos (S/N);
- Detenções (S/N);
- Processos em curso (S/N);
- Processos suspensos (S/N).

Quanto ao detalhe sobre «situação judicial, não sendo estabelecido um grau de detalhe em relação a julgamentos, detenções ou processos, considerou a CNPD que o seu tratamento devia ser condicionado:

A uma resposta facultativa e informada dos titulares dos dados;

À anonimização da informação a fim de que possa ser utilizada para efeitos de estatísticas e estudos. (Autorização 105/2003).

e) *Carta dos Direitos do Doente Internado*

A Direcção-Geral de Saúde veio solicitar a esta CNPD a emissão de parecer sobre o projecto da «Carta dos Direitos do Doente Internado».

Considerou a CNPD que este direito deveria consignar o princípio do «consentimento esclarecido», devendo ser referido que o doente tinha o direito de retirar, em qualquer altura, o seu consentimento.

Apesar de o conceito tradicional de sigilo médico – que estabelecia uma relação de confiança na relação directa entre a figura do “médico assistente” e o doente – se ter *relativizado* e o sigilo médico assumir, actualmente, como um «segredo partilhado», na medida em que o diagnóstico e a prestação de cuidados de saúde

eram feitos em equipa (grupo de médicos no mesmo serviço) ou através da troca de informações entre profissionais de equipas diferentes (vg. As experiências de telemedicina), a «partilha da informação clínica» devia ser realizada na estrita medida do necessário à prestação de cuidados de saúde.

A circulação de informação deveria, pois, obedecer a um princípio de «confidência necessária» em que seriam determinantes para definir o “âmbito do segredo”, o interesse do doente, a natureza da informação e os reflexos que a sua divulgação trazia para a sua privacidade.

Também em relação às declarações feitas aos órgãos de comunicação social não se vislumbrou que fosse pertinente diferenciar categorias de pessoas (desportistas, políticos e artistas), pois qualquer informação individualizada em relação a diagnósticos, prognósticos só podia ser divulgada se houvesse consentimento do titular dos dados ou se fundamentar, quando aplicável, nas alíneas a) e c) do artigo 7.º n.º 3 da Lei 67/98, de 26 de Outubro.

Não se afigurou admissível que o «médico assistente» se pudesse negar a fazer a «intermediação» para o direito de acesso, nomeadamente nos casos em que o doente não indicasse médico da sua confiança. Neste caso, o estabelecimento de saúde devia diligenciar no sentido de assegurar que o direito de acesso era efectivado.

Para além da consagração do *direito de acesso* entendeu a CNPD que, também de uma forma expressa, deveria ser consagrado um outro direito: «o direito de, por vontade expressa, não ser informado sobre a sua saúde» (**Deliberação n.º 43/2003**).

f) *Acesso a dados clínicos por terceiros*

O Núcleo de Deontologia e Disciplina da Polícia de Segurança Pública do Comando Metropolitano de Lisboa solicitou a um hospital o envio da ficha de admissão de doente respeitante a um agente policial, em virtude de ter sido vítima de agressão e recebido tratamento naquele estabelecimento Hospitalar.

O pedido desta informação destinava-se a documentar o processo de sanidade em curso no referido Núcleo com vista a salvaguardar os interesses da fazenda Pública uma vez que o agente foi vítima de agressão a que se referia o auto de denúncia.

O Hospital solicitou a esta Comissão esclarecimento no sentido de ser informado se poderia dar acesso à informação solicitada.

No âmbito do Decreto-Lei n.º 503/99, de 20 de Novembro, não era permitido ao empregador ou entidade empregadora proceder à recolha de dados que não apresentassem conexão com acidentes de trabalho ou doenças profissionais.

Sobre a participação à entidade empregadora de informações sobre acidentados em serviço, regia o n.º 2 do artigo 9.º do mesmo Decreto-Lei, determinando que os serviços de saúde, públicos ou privados, que tivessem prestado assistência a um acidentado deviam participar a ocorrência à entidade empregadora do mesmo, no prazo de um dia útil, pela via mais expedita.

Esta norma, constituía disposição legal para efeitos do n.º 2 do artigo 7.º da Lei n.º 67/98 de 26 de Outubro, permitindo o tratamento, no domínio da recolha, de dados de saúde dos empregados.

No entanto era referido pela PSP o n.º de processo judicial de investigação criminal que decorria relativamente aos factos que invocou, pelo que os elementos que solicitou, embora se integrassem em disposição legal que permitia o tratamento dos dados de saúde dos empregados, isto é do agente em questão, encontravam-se sob segredo de justiça.

Tal quebra de segredo poderia ser solicitada directamente pela PSP ao Ministério Público ou ao Juiz de instrução nos termos do n.º 4, 5, 7 e 8 do artigo 86.º do Código de Processo Penal, pelo que a CNPD deliberou não autorizar o acesso do Núcleo de deontologia da PSP à ficha de admissão do agente no Hospital, dado tratar-se de informação sob segredo de Justiça. (**Deliberação 69/2003**).

.....

Os Serviços Municipalizados de Água e Saneamento de Sintra solicitaram a esta CNPD, através da CADA, o acesso ao resultado da análise sanguínea de um seu funcionário, envolvido num acidente de viação com o carro de serviço. A fim de verificar o teor de alcoolémia.

Pareceu à CNPD legítimo submeter o trabalhador aos exames necessários no âmbito da alcoolémia, especialmente quando se perspectivem riscos para o trabalhador ou para terceiros.

Nestas circunstâncias, o resultado da análise sanguínea do funcionário revelava-se absolutamente fundamental para determinar uma de duas situações: o arquivamento do processo de inquérito ou a instauração de procedimento disciplinar, pelo que a CNPD autorizou o acesso. (**Deliberação 96/2003**).

7 – TRATAMENTO DE DADOS NO SECTOR FINANCEIRO E DE INFORMAÇÕES DE CRÉDITO

a) *Princípio da actualização dos dados*

A CREDINFORMAÇÕES – Informação de Crédito, Ld.^a veio requerer à CNPD a reapreciação da questão dos prazos de conservação, fixados nas Deliberações n.º 90/95 e 19/97, no sentido de “permitir a conservação em ficheiro dos dados de incidentes de crédito de cada titular até 2 anos após a cessação de todos os incidentes que lhe respeitem”.

Existia, ainda, uma comunicação da Credinformações em relação à possibilidade de os titulares dos dados poderem exercer o direito acesso e rectificação, na sequência do direito de informação, junto de um apartado.

Importava que a Credinformações estabelecesse uma metodologia rigorosa que permitisse à CNPD assegurar, com rigor, o cumprimento da obrigação de actualização consignado no artigo 5.º n.º 1 al. d) da Lei 67/98, de 26 de Outubro) e o direito de rectificação (art. 11.º n.º 1 al. d) da Lei 67/98).

A CNPD entende que a Lei 67/98, de 26 de Outubro, não trouxe alterações substanciais à fixação do prazo de conservação de dados. O artigo 5.º n.º 1 al. d) da Lei 67/98 não tem qualquer efeito nos princípios que foram definidos na Deliberação n.º 19/97, de 5 de Junho. Efectivamente, e em face do disposto neste preceito, mantêm-se válidos os seguintes princípios em matéria de actualização de dados:

1. *“O tempo de conservação dos dados deve ser definido e limitado à finalidade do ficheiro;*
2. *Os dados respeitantes a um incidente de crédito só devem ser conservados enquanto este se verificar;*
3. *Logo que tenha cessado o incidente as empresas participantes devem comunicar essa ocorrência à Credinformações a qual, imediatamente, procede à eliminação do incidente («informação negativa»).*

A única alteração da Lei 67/98, de 26 de Outubro, foi a de atribuir à CNPD uma competência específica para «fixar prazos de conservação dos dados pessoais em função da finalidade» (cf. artigo 23.º n.º 1 al. f). Porém, a CNPD não viu que houvesse razões objectivas – quer de facto quer de direito – para alterar os prazos de conservação estabelecidos no caso em apreço. As condições estabelecidas pela autorização n.º 118/96, com as precisões definidas pela Deliberação n.º 19/97 e 36/97, de 23 de Outubro, são aquelas que melhor se adequam aos princípios estabelecidos pelo artigo 5.º n.º 1 alíneas d) e e) da Lei 67/98.

Em face do exposto, considerou a CNPD que não havia razões para alterar os prazos de conservação anteriormente estabelecidos.

Quanto ao direito de acesso, a questão que se colocava era a de saber se a Credinformações podia assegurar o direito de acesso mediante solicitação escrita dos interessados dirigida a um Apartado. A Credinformações informou que pretendia que fosse assegurada a possibilidade de a correspondência dos titulares dos dados poder «ser remetida para um apartado postal, independentemente do direito de acesso e rectificação poder ser exercido somente por escrito ou também presencialmente».

A CNPD não viu que existisse qualquer objecção a que a correspondência fosse endereçada para um Apartado. Efectivamente, considerou a CNPD que o direito de acesso, correcção e rectificação de dados, bem como a correspondência endereçada dos titulares dos dados podia ser endereçada para um Apartado.

Tinham chegado à CNPD algumas queixas apresentadas por titulares dos dados que pretendiam ver actualizados os seus dados pessoais, nomeadamente na sequência de liquidação de créditos em dívida.

A Autorização 90/95 estabelecia o seguinte: «a actualização é efectuada com base nos dados fornecidos pelas entidades que concedem o crédito. A actualização é feita mensalmente» (ponto 8, pág. 7). Esta formulação tem suscitado algumas dificuldades na medida em que, em alguns casos, a informação tem sido mantida no sistema (sem estar actualizada) por períodos superiores a 30 dias.

Havia situações em que o titular comprovava – junto da Credinformações – que tinha efectuado a liquidação da dívida. Nestes casos o titular esperava e reclamava, nos termos do artigo 11.º da Lei 67/98, a actualização imediata dos dados.

A Credinformações aguardava, em regra, que a entidade participante lhe comunicasse a alteração da situação. Porém, esta solução podia, em alguns casos, conter com os princípios de rectificação consignados no artigo 11.º da Lei 67/98. Efectivamente, caso o titular comprovasse que os dados já não eram exactos (artigo 11.º n.º 1 al. d) da Lei 67/98) assistia-lhe o direito de os ver actualizados. Em face do exposto a CNPD deliberou a CNPD que a Credinformações devia tomar todas as medidas para assegurar que a actualização dos dados fosse feita *no prazo máximo de 30 dias sobre a data dos factos determinantes da actualização*. (**Deliberação 122/2003**).

.....

b) Exercício do direito de acesso junto do Banco de Portugal

O Banco de Portugal veio, na sequência do disposto no artigo 3.º n.º 5 do DL 454/91, de 28 de Dezembro, na redacção introduzida pelo DL 83/2003, de 24 de Abril, solicitar a emissão de parecer sobre a Instrução que visava regular “a forma e termos de acesso às informações” constantes do tratamento de utilizadores de cheque que ofereciam risco, quando estas se destinavam à avaliação de riscos de crédito por parte das instituições financeiras. A CNPD considerou que o projecto de Instrução devia, em termos globais, merecer uma apreciação favorável uma vez que estavam regulados com precisão os aspectos fundamentais a considerar em matéria de acesso à informação.

Entendeu, não obstante, que havia *dois aspectos* que deveriam merecer alguma reflexão e que, de acordo com os procedimentos a adoptar e com as disponibilidades técnicas do Banco de Portugal, poderiam ter uma melhor concretização.

Quanto aos mecanismos de controlo em relação aos procedimentos de consulta realizados pelas instituições financeiras (especialmente aquelas que, até à entrada em vigor do DL 83/2003, não tinham acesso à informação) era necessário que estivessem previstas «grelhas de consulta» (vg. necessidade de indicação do n.º de BI, nome do titular dos dados e data da formalização do pedido de concessão de crédito), sendo as pesquisas registadas pelo Banco de Portugal – durante um certo período (v.g. 1 ano) – com o objectivo de realização de auditorias. A possibilidade de realização destas auditorias deveria constar da Instrução.

Quanto à preocupação legal, expressa no artigo 3.º n.º 6, de *assegurar a actualização da informação*, a lei estabelece que as informações recebidas “devem ser eliminadas...logo que cesse o período de permanência de dois anos, haja decisão de remoção da listagem ou se verifique o termo de decisão judicial, excepto se o titular nisso expressamente consentir”.

Daqui decorre que deviam ser criados todos os mecanismos necessários a assegurar, de forma efectiva, as condições que permitissem às instituições financeiras proceder à actualização da informação, nos termos das disposições combinadas do artigo 3.º n.º 6 do DL 454/91 (redacção do DL 83/2003) e artigo 5.º n.º 1 al. d) da Lei 67/98.

Se para as instituições financeiras que podiam celebrar convenções de cheque não se levantavam problemas – porque o Banco de Portugal lhes comunicava as decisões de remoção – já quanto às demais instituições o mesmo não parecia estar assegurado. Efectivamente, não pareciam estar asseguradas as condições objectivas que permitissem às instituições financeiras que consultavam o sistema do Banco de Portugal, e registavam a informação obtida no seu sistema, garantir a actualização dos dados quando houvesse remoção ou reabilitação judicial antes do prazo fixado. Admitir, como o fazia o projecto de Instrução, que só podia haver eliminação quando as instituições financeiras «*possam ter de algum modo conhecimento*» das razões determinantes da actualização/eliminação de dados traduzia-se numa situação incerteza que representava uma frontal violação dos princípios da actualização de dados. Ao não serem adoptados mecanismos que iam permitir a actualização imediata dos dados por parte de algumas instituições financeiras – aspecto que tinha sido objecto de apresentação de múltiplas queixas dos cidadãos em relação ao regime anterior – abria-se caminho à existência de tratamentos da responsabilidade das instituições financeiras, mantidos com violação do artigo 5.º n.º 1 alíneas d) e e) da Lei 67/98. Esta insuficiência ia permitir às instituições de crédito a manutenção da informação desactualizada com a alegação de «*não terem conhecimento da remoção ou reabilitação*», facto que tinha consequências visíveis em relação à privacidade dos titulares dos dados.

Entendeu a CNPD que o Banco de Portugal deveria informar as instituições financeiras que consultavam o sistema do Banco de Portugal – servindo-se do «registo das consultas» efectuado (acima proposto) – sempre que esses registos fossem

actualizados (v.g. na sequência de remoção da listagem antes do prazo inicialmente estabelecido ou da reabilitação judicial).

Este último aspecto foi decisivo para a CNPD emitir um parecer favorável ao projecto de Instrução. (**Parecer 37/2003**).

.....

O Banco de Portugal veio, na sequência do disposto no artigo 3.º n.º 5 do DL 454/91, de 28 de Dezembro, na redacção introduzida pelo DL 83/2003, de 24 de Abril, solicitar a emissão de novo parecer sobre a Instrução que visava regular “a forma e termos de acesso às informações” constantes do tratamento de utilizadores de cheque que ofereciam risco, quando estas se destinam à avaliação de riscos de crédito por parte das instituições financeiras.

O Banco de Portugal fez alterações ao projecto inicial, em particular em relação aos aspectos relativos à *actualização da informação*. Foram estabelecidas exigências em relação ao registo de dados por parte das instituições financeiras, consignando-se, nomeadamente, que não poderão ser guardadas informações negativas no caso de «a proposta de concessão de crédito ter sido recusada».

Da metodologia aprovada no projecto de Instrução resultava claro que as instituições financeiras que consultavam o sistema eram responsáveis pelos tratamentos que realizassem na sequência de consulta ao Banco de Portugal. Isso implicava que deviam fazer a respectiva notificação do tratamento à CNPD (nos termos do artigo 27.º da Lei 67/98) e comprovar que tomavam as medidas adequadas para manter actualizada a informação negativa (cf. artigo 5.º n.º 1 alíneas d) e e) da Lei 67/98). (**Parecer 48/2003**).

.....

c) *O consentimento no âmbito das cláusulas contratuais gerais*

Um cidadão solicitou a intervenção da CNPD relativamente a uma cláusula contratual – artigo 14.º inserida por uma entidade bancária nas “Condições Gerais de Utilização de Cartões VISA e Eurocard/Mastercard e serviço MBNet”.

Referiu a reclamante, cliente da instituição bancária, que a imposição ao cliente

por parte do Banco dos seus «*dados pessoais para finalidades diversas daquelas que respeitam à respectiva recolha constitui violação do Direito vigente*».

O artigo 14.º das “Condições Gerais de Utilização de Cartões VISA e Eurocard/Mastercard e serviço MBNet” tinha por objecto *dados pessoais informatizados*, dispondo o seguinte:

- a) *os dados pessoais recolhidos para execução do presente contrato ou no âmbito da contratação de produtos e serviços com ele relacionados são susceptíveis de serem transmitidos ou processados automaticamente, destinando se ao estabelecimento de relações comerciais personalizadas com o Banco e com as instituições a ele coligadas;*
- b) *é assegurado nos termos legais o direito de informação, correcção, aditamento ou supressão dos dados, mediante contacto pessoal ou por escrito junto de qualquer sucursal do Banco;*
- c) *o Titular autoriza a recolha, transmissão e processamento adicionais de dados obtidos junto de Repartições Públicas ou empresas especializadas, para a confirmação dos dados e a obtenção dos elementos necessários à relação contratual, no quadro actual vigente.*

Indagado, pela ora reclamante, sobre a eliminação desta cláusula, o Banco emitiu a seguinte declaração: *declaramos para os devidos efeitos que não é possível retirar a cláusula 14 Dados pessoais informatizados das “Condições Gerais de Utilização de Cartões VISA e Eurocard/Mastercard e serviço MBNet”.*

No que respeitava à protecção de dados pessoais, entendeu-se que o problema devia ser estudado da seguinte forma:

- a) O contrato denominado “Condições Gerais de Utilização de Cartões VISA e Eurocard/Mastercard e serviço MBNet” era composto por cláusulas contratuais gerais *elaboradas sem negociação prévia individual* (art.º 1, n.º 1 do anexo ao Decreto-Lei n.º 220/95, de 31 de Janeiro);
- b) O n.º 14 do contrato revelava o consentimento do titular no que respeitava à cedência dos dados a instituições coligadas ao Banco e a repartições Públicas ou empresas especializadas, para a confirmação dos dados e a obtenção dos elementos necessários à relação contratual, no quadro actual vigente;

- c) O consentimento era uma condição de legitimidade idónea nos termos dos artigos 6.º da Lei n.º 67/98, de 26 de Outubro;
- d) Nos termos do artigo 3.º, alínea h) da Lei n.º 67/98, de 26 de Outubro, por consentimento devia entender-se *qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objecto de tratamento*;
- e) Um dos traços fundamentais do regime jurídico do consentimento consistia na sua *revogabilidade*;
- f) Previa a Constituição que *“é proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei”* (artigo 35.º, n.º 4), o que, evidentemente, não exclui o consentimento.

Afigurou-se a esta Comissão meridiano que cláusulas contratuais gerais enxertadas em instrumentos contratuais limitam ou eliminam a capacidade negocial de um dos contraentes, no caso a reclamante.

Assim, tutelando a Lei n.º 67/98, de 26 de Outubro a *liberdade* do acto de consentimento, considerou-se que esta não é obtida em instrumentos contratuais como o apreciado.

Desta forma, as cláusulas contratuais gerais que envolvam cedência de dados pessoais, a empresas de um grupo, sem admitir a revogação do consentimento, em contratos como o apreciado, consideraram-se nulas nos termos gerais (artigo 294.º do Código Civil), por envolverem a violação do artigo 6.º da Lei n.º 67/98, de 26 de Outubro).

A CNPD considerou que o conteúdo da alínea c) da cláusula devia ser interpretado em conformidade com a alínea e) do artigo 6.º da Lei n.º 67/98, de 26 de Outubro, no segmento em que refere a *prossecação dos interesses legítimos do responsável pelo tratamento*.

A CNPD não dispunha de competência para declarar a nulidade de cláusulas contratuais, devendo, todavia, exercer as suas competências enquanto *autoridade nacional que tem como atribuição controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de protecção de dados* (artigo 22.º, n.º 1 da Lei n.º 67/98, de 26 de Outubro).

Neste sentido, a CNPD podia, nos termos do alínea b) do n.º 3 do artigo 22.º da Lei n.º 67/98, de 26 de Outubro, *proibir, temporária ou definitivamente, o tratamento de dados pessoais*.

Em face do exposto, a CNPD determinou a proibição do Banco fornecer os dados pessoais da reclamante a empresas do grupo, efectuados em execução da cláusula 14 das “Condições Gerais de Utilização de Cartões VISA e Eurocard/Mastercard e serviço MBNet”. (**Deliberação 149/ 2003**).

.....

d) *Circulação de informação bancária para efeitos de luta contra o branqueamento de capitais e financiamento do terrorismo*

Uma entidade bancária veio informar que tinha em curso um projecto de controlo e circulação de informação de clientes ao nível mundial, nomeadamente com o objectivo de poder responder às exigências legais impostas pelos diversos estados ao nível de branqueamento de capitais e da luta contra o financiamento do terrorismo e corrupção.

Para assegurar a realização dessa finalidade o Banco propôs-se obter o *consentimento dos titulares dos dados*. Essa declaração de consentimento, necessariamente genérica, estabelecia o seguinte: “autorizo a transmissão... tanto em Portugal como no estrangeiro de quaisquer documentos ou informações que em qualquer momento estejam na vossa posse ou sejam do vosso conhecimento e que digam respeito à nossa pessoa e/ou às nossas relações bancárias... para as seguintes finalidades:

- (i) ... no quadro das obrigações decorrentes de qualquer lei ou regulamento referente a branqueamento de capitais e à luta contra o financiamento do terrorismo e contra a corrupção, aplicável em qualquer país em que se situe qualquer entidade pertencente ao mesmo Grupo e em que qualquer entidade do mesmo Grupo possa ser inquirida, sob qualquer forma, por autoridade judicial, fiscal, administrativa, reguladora ou outra espécie, revelação essa que compreendemos e aceitamos;
- (ii) Estabelecer e manter procedimentos de centralização de gestão de risco e/ou sistemas internos de venda cruzada (*cross selling*) do Grupo.

As comunicações referidas – nomeadamente as finalidades de informação sobre branqueamento de capitais – eram objecto de previsões legais, quer no nosso direito interno quer no direito de outros países, que impunham uma obrigação legal de comunicação a determinadas entidades. Não obstante, para a referida finalidade o Banco obtinha o consentimento dos titulares dos dados. Por uma questão de rigor, o Banco devia certificar-se que as entidades que solicitavam as referidas informações eram as entidades competentes, nos respectivos países, para poderem solicitar a informação.

Em relação à utilização dos dados no âmbito dos riscos de crédito (cf. artigo 83.º do DL 298/92) considerou a CNPD que deviam ser indicadas as entidades aos seus titulares, ou seja, devia o BNP identificar as empresas do Grupo junto da CNPD e indicar a respectiva sede (**Autorização 477/ 2003**).

e) *Cedência de dados pessoais*

Uma instituição bancária concretizou uma operação de cessão de créditos a uma entidade com sede em França, a qual envolveu a cedência de créditos nos termos do artigo 586.º do Código Civil.

A questão que se colocou relacionou-se com a cedência de dados a «entidade terceira» – uma sociedade financeira.

A cedência de dados era feita no âmbito de um contrato celebrado. As informações a prestar estavam protegidas por segredo bancário.

A legitimidade para o tratamento – na vertente comunicação – podia derivar de três fundamentos possíveis:

- Através de consentimento inequívoco por parte dos titulares (corpo do artigo 6.º);
- Através da inclusão de cláusula contratual estabelecida entre o Banco e os titulares dos dados (art. 6.º al. a);
- No âmbito da “prossecação de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados” (art. 6.º al. e).

Quando se verificasse o fundamento indicado na alínea e) – nomeadamente em relação aos contratos já celebrados – o Banco deveria informar os titulares dos dados da possibilidade de comunicação de informação no âmbito de cessão de

créditos (cf. art. 10.º n.º 1 da Lei 67/98). Só depois de assegurado o direito de informação os titulares estariam em condições de, eventualmente, poderem exercer o “direito de oposição” (cf. art. 12.º al. a) ou invocar a “prevalência de interesses ou direitos” consignados no artigo 6.º al. e) da Lei 67/98.

Em face do exposto, a CNPD autorizou a cedência dos dados pessoais indicados, desde que a cedência respeitasse um dos condicionalismos acima estabelecidos. O direito de informação deveria ser assegurado pelo Banco em momento anterior à ocorrência do evento que irá desencadear todo o processo, por forma a assegurar que, em relação àqueles a quem foi reconhecido o «direito de oposição» (art. 12.º al. a) da Lei 67/98), não houvesse a inclusão dos seus dados pessoais na disquete ou – se for o caso – não fosse celebrado o contrato. (**Autorização 2/2003**).

f) *Concessão de crédito ao consumo*

Uma entidade bancária veio informar a CNPD que encetou uma nova parceria comercial com diversas empresas, com vista ao financiamento dos bens adquiridos nos seus estabelecimentos.

Recolhendo aquelas empresas dados pessoais dos clientes que pretendem comprar bens a crédito – impresso anexo ao formulário – pretendia a requerente, nesse contexto, transmitir dados pessoais (nome, NIF, morada, nacionalidade, BI, data de nascimento, telefone, sexo, estado civil, n.º de dependentes, nome da empresa, profissão, salário, tipo de contrato, outros rendimentos, tipo de cartão de crédito, tipo de habitação, encargos mensais e demais elementos do contrato) às empresas.

A cláusula 2 das condições gerais estabelecia o seguinte: «*os mutuários autorizam expressamente o banco e o fornecedor dos seus dados de natureza pessoal com vista à gestão do presente financiamento e para efeitos publicitários...*».

Importava saber se esta cláusula é bastante para legitimar o tratamento/comunicação de dados às empresas fornecedoras.

Caso se pretendesse a comunicação de dados aos fornecedores para estes os tratarem de forma autónoma e, nomeadamente, fazerem prospecção comercial dos seus produtos ou contactos com os clientes este procedimento teria de obedecer a todas as exigências da Lei 67/98. Em particular:

- a) Não se vislumbrava, em função da finalidade, que os dados a comunicar aos fornecedores fossem necessários e pertinentes. Pelo contrário, revelavam-se excessivos na medida em que para a finalidade de prospecção é desproporcionada a recolha de todos os dados indicados;
 - b) O texto incluído na cláusula 2.1. não permitia o «direito de oposição» consignado no artigo 12.º al. b) da Lei 67/98, vinculando todas as pessoas que celebrassem contratos a facultar os seus dados aos fornecedores;
 - c) Nenhuma das empresas indicadas tinha o seu tratamento notificado junto da CNPD, nomeadamente para a finalidade aqui delineada. Não estavam, igualmente, autorizadas a tratar todos aqueles dados. Enquanto isso acontecesse, não pôde o Banco comunicar dados a essas entidades. (**Autorização 509/2003**).
- g) *Gestão de programa de cartões de débito*

Um Banco veio notificar o tratamento cuja finalidade era a «gestão de programas de cartões Visa Electron pré-pagos. Em determinados programas havia partilha de dados do registo de clientes com parceiros de negócio».

No formulário de recolha de dados referia-se que o Banco podia transmitir os dados a uma operadora de telecomunicações, “bem como a outros parceiros.

De acordo com os elementos constantes do processo os titulares dos dados autorizavam, expressamente, o fluxo de dados para os EUA.

Em relação ao *direito de informação* – no caso de o titular dos dados ser menor – entendeu a CNPD que era obrigatória a indicação do e-mail ou outro contacto dos pais a fim de ser assegurado o direito de informação.

Por outro lado, o Banco, na qualidade de sociedade financeira, encontrava-se vinculado ao sigilo bancário nos termos do artigo 78.º da Lei das Sociedades Financeiras. A libertação do sigilo só podia tornar-se efectiva se os titulares dos dados, ou os seus legais representantes no caso de serem menores, dessem o seu consentimento.

O disposto na alínea h) do artigo 3.º da Lei 67/98, pressupunha um consentimento que se concretizasse mediante uma «*manifestação de vontade*, livre, específica e informada, nos termos da qual o titular aceitava que os dados pessoais fossem objecto de tratamento».

Por isso, o consentimento tinha de ser expresso por uma «manifestação de vontade» – vg. através de uma “quadrícula ou *icon*” – que materializasse a vontade de ceder os dados e a que entidades.

Não foi admissível qualquer «consentimento presumido» no âmbito deste programa na medida em que, em termos de protecção de dados, o consentimento envolve sempre uma «manifestação de vontade» (veja-se o artigo 3.º alínea g) da Lei 67/98).

Por outro lado, não pôde ser aplicável a este tratamento o sistema de «*opting out*», sendo sempre necessária uma manifestação de consentimento.

Quanto à transferência de dados para os EUA – plataforma informática que gere a informação e transacções dos cartões – verificava-se que a empresa realizava esta actividade na qualidade de sub-contratante (era responsável pela administração da base de dados) e decorrendo o fluxo de *consentimento* e de *cláusula contratual* necessária à execução do contrato e uma vez que se encontrava assegurada a confidencialidade da informação, tendo-se comprometido o sub-contratante a utilizar os dados de acordo com as instruções do responsável, entendeu-se que devia ser autorizada a transferência, nos termos do artigo 20.º n.º 1 e n.º 1 alínea b) da Lei 67/98.

Envolvendo o tratamento de dados a realização de perfis de consumo em função dos «hábitos de compras individuais» entendeu a CNPD, desde logo, que esta informação devia constar de forma expressa e autónoma, no formulário de recolha de dados, pois esse tipo de tratamento consubstanciava uma acentuada invasão da esfera privada. Acresceu, ainda, que a simples atribuição de benefícios (pontos ou prémios – ofertas) sem informação clara e esclarecida podia integrar uma recolha violadora dos princípios da boa-fé (cf. art. 5.º n.º 1 al. a) da Lei 67/98) e da transparência (art. 2.º da Lei 67/98), para além de não satisfazer as condições de legitimidade do corpo do artigo 6.º da Lei 67/98 quando exigia um consentimento dado «de forma inequívoca». (**Autorização 16/2003**).

.....

h) Transferências internacionais de dados

Uma entidade bancária veio solicitar o fluxo transfronteiriço de dados para «estruturas de representação do Banco no estrangeiro».

A transferência era «*necessária para a execução de contratos de abertura de conta e doutros contratos associados à prestação de serviços financeiros entre os clientes e o Grupo*».

Havendo fluxo de dados para países terceiros, o Banco remeteu a esta CNPD cláusulas contratuais a fim de serem consideradas. Estas cláusulas contratuais eram muito similares àquelas que estavam estabelecidas na Decisão da Comissão n.º 2001/497/CE, de 15/6/2001, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros.

Mesmo assim, entendeu a CNPD que se tornava mesmo assim necessário estabelecer a garantia adicional de que não haveria qualquer transferência subsequente de dados pessoais do importador de dados para outro responsável estabelecido em país terceiro sem o acordo/autorização prévia do Banco». Ou seja, deveria ser adoptada uma formulação similar à que consta da cláusula 6 do Apêndice 2 da Decisão 2001/497/CE.

A adopção de cláusulas contratuais-tipo era uma das formas possíveis de permitir o fluxo transfronteiras para países que não ofereciam garantias adequadas. A solução contratual apareceu, assim, como «*um meio através do qual o responsável pelo tratamento fornece garantias adequadas à pessoa em causa aquando da transferência dos seus dados para fora da comunidade, mais concretamente, para um país terceiro no qual o nível geral de protecção não é adequado. Para poder cumprir essa função, as cláusulas contratuais terão de compensar de forma satisfatória a ausência de um nível geral de protecção adequado, através da inclusão de elementos essenciais de protecção omissos numa determinada situação concreta*».

Cabia à CNPD, nos termos do artigo 20.º n.º 2 da Lei 67/98, de 26 de Outubro, autorizar uma transferência ou conjunto de transferências, verificando se o responsável assegura mecanismos suficientes – *v. g. mediante cláusulas contratuais* – de garantia de protecção da vida privada e dos direitos e liberdades fundamentais das pessoas.

Sendo as cláusulas apresentadas muito similares àquelas que constam no Anexo à Decisão 2001/497/CE, a CNPD entendeu que seria de autorizar o fluxo trans-fronteiras desde que fossem feitas algumas alterações:

- A Cláusula 4 (b) devia ser alterada na medida em que não era claro que deveriam sempre «prevaler» as disposições sobre cumprimento de obrigações legais ou de dispensa do direito de informação. Entendeu a CNPD que deveria ser eliminada a expressão «prevalência» e que a cláusula poderia ter a seguinte redacção:...” *sem prejuízo das disposições que prevêem o cumprimento de obrigações legais e a dispensa do direito de informação*”;
- Na Cláusula 4 (d) seria desejável, em vez de se referir um «prazo razoável», que o mesmo fosse especificado. Sugeriu-se a possibilidade de fixar um prazo geral *10 dias*, o qual poderia ser prorrogado por mais 10 dias sempre que fossem invocadas razões atendíveis que justificassem tal prorrogação;
- Quando estivesse em causa a resposta a pedido formulado pelo titular dos dados, tanto o exportador (cláusula 4.^a al. d) como o importador (cláusula 5.^a al. c), deviam informá-lo no prazo de 10 dias das diligências efectuadas e das razões da respectiva prorrogação;
- As «transferências subsequentes» só deviam ser feitas com o consentimento quando envolvessem categorias especiais de dados ou mediante informação clara e inequívoca sobre as suas finalidades, devendo ser assegurada a oportunidade de o titular dos dados poder exercer o direito de oposição. (**Autorização 501/2003**).

8 – TRATAMENTO DE DADOS NO ÂMBITO DO MARKETING

a) Perfil de utilizador

Uma empresa veio notificar a CNPD de um tratamento de dados pessoais com a finalidade de *gestão de clientes e serviços, acções de marketing de novos produtos e serviços, promoções, estudos de mercado, adaptação da oferta de produtos e serviços*.

Os dados recolhidos eram os seguintes: nome (nome próprio e apelidos), endereço electrónico, palavra-passe, perfil do utilizador, morada, telefone e data do nascimento.

Entendeu-se que o *perfil do utilizador* se reconduzia à categoria dos dados pessoais prevista na alínea a) do artigo 3.º da Lei n.º 67/98, de 26 de Outubro. Daqui resultava que as operações de determinação do *perfil do utilizador* não podiam ser realizadas pelo responsável pelo tratamento sem consentimento do titular, não havendo que admitir qualquer forma de *consentimento tácito*.

Esta Comissão entendeu que uma *pergunta tipo* sobre a prestação de consentimento devia ser formulada de forma a que o titular pudesse expressá-lo – por exemplo através das declarações *autorizo* ou *aceito*, explicitando que o tratamento em causa respeitava à *determinação de perfis* e indicando que os *perfis* assentavam no tratamento de dados relativos a hábitos que resultavam da utilização dos serviços da empresa. (**Autorização 5/2003**).

.....

b) *Direito de informação tipo de letra*

Num outro caso relativo ao tratamento de dados pessoais, a partir de um inquérito ao consumo para fins de “*análise comportamental de clientes, à efectivação de listagens e à cedência de dados para fins de marketing directo*”, a CNPD chamou a atenção para que, no texto de prestação das informações ao titular dos dados, o tamanho da letra fosse em tudo idêntico ao utilizado no questionário.

Por outro lado, a CNPD não aceitou que, nas situações em que o inquérito é feito com intervenção do entrevistador não constasse o texto relativo ao direito de oposição.

Na verdade, e como se reconhecerá, nada impede que o titular dos dados aceite prestar ao entrevistador as respostas tidas por adequadas e, simultaneamente, exerça o seu direito de oposição quanto à cedência a outras entidades para fins de marketing, ofertas de produtos ou serviços responder às questões colocadas.

Mesmo que o entrevistador pudesse – leia-se, devesse – informar o titular, constando expressamente o mesmo do respectivo impresso será mais uma garantia de que o mesmo pode ser lido e conhecido, prevenindo até eventuais esquecimentos daquele. Face à ausência quer do respectivo texto informativo, quer da correspondente quadrícula para assinalar a competente oposição, não se via, até, como, em caso de conflito, pudesse o mesmo ser devidamente comprovado. (**Autorização 494/2003**).

.....

c) *Direito de informação e direito de oposição na Internet*

Uma empresa veio notificar um tratamento cuja finalidade era a «identificação de características de grupos de utilizadores de um site e envio de promoções por correio normal ou e-mail para esses mesmos utilizadores.

Verificava-se que a entidade responsável pretendia recolher dados na Internet. Os dados tratados eram o nome, morada, sexo, data de nascimento, ocupação, n.º de contribuinte, e-mail, receber mail em html (S/N), *username* e *password*. Para além destes dados o responsável informou que fazia *perfis de utilizadores* elaborados a partir de informação obtida a partir dos dados pessoais referidos e de «informação relativa a navegação e utilização dos serviços, como sejam: conteúdos visualizados ou pesquisados e/ou conteúdos colocados pelo próprio utilizador». O site registaria apenas o acesso a outros sites cujos *links* fossem disponibilizados.

A CNPD impôs que o formulário de recolha de dados fosse alterado, no sentido de assegurar o direito de informação e o direito de oposição em relação a quaisquer acções promocionais, criando para o efeito uma quadrícula ou ícone para que os utilizadores pudessem manifestar essa sua escolha. Quando os titulares se opusessem a realizações de acções de *marketing* ou de campanhas promocionais devia o responsável incluir os utilizadores em «lista de recusas» e abster-se de lhes enviar qualquer publicidade.

A elaboração de «perfis», em termos de legitimidade, e tendo em atenção o disposto no artigo 6.º da Lei 67/98, passava, necessariamente, pela obtenção do consentimento dos utilizadores. (**Autorização 498/2003**).

.....

d) *Código de Conduta do Marketing Directo*

A Associação Portuguesa de Marketing Directo (AMD) solicitou à Comissão Nacional de Protecção de Dados (CNPD) parecer sobre o novo Código de Conduta das Empresas de Marketing Directo.

A CNPD observou que o novo projecto de Código de Conduta não fazia referência à recolha e tratamento de dados pessoais a partir de meios electrónicos, tendo considerado que seria sumamente vantajosa a inclusão de regras que disciplinassem a actividade de marketing directo exercida com recurso ao correio electrónico.

A CNPD considerou que a fórmula *dados portugueses* contida no preâmbulo tinha de ser esclarecida, pois não se sabia se eram dados pessoais relativos a portugueses, independentemente do país da recolha, ou de dados recolhidos sobre portugueses em Portugal, ou, ainda, de qualquer outra hipótese.

O n.º 2 do artigo 2.º tinha por objecto dados pessoais não recolhidos directamente, mas através de *documentos acessíveis ao público, objecto de publicação ou por via de terceiros*. A CNPD considerou que o facto de o titular figurar numa lista pública não legitima que seja os seus dados sejam transmitidos pelo responsável pela recolha, no caso de ter sido exercido o *direito de oposição* (artigo 12.º da Lei n.º 67/98, de 26 de Outubro). Assim, as fórmulas *documentos acessíveis ao público* e *objecto de publicação* podiam legitimar a consulta e a actividade de *marketing directo*, desde que não envolvesse a comunicação de dados de titulares a que a tal se houvessem oposto aquando da recolha junto do responsável por esse tratamento.

A rectificação e actualização de dados, enunciadas no artigo 3.º do Código de Conduta, estavam conformes com a Lei n.º 67/98, de 26 de Outubro. A CNPD considerou, porém, excessivo o período de 120 dias como prazo máximo para a eliminação do nome de uma lista destinada a marketing directo.

A CNPD considerou vantajoso que o Código de Conduta contivesse o compromisso de não *recolher conservar ou utilizar quaisquer dados pessoais sensíveis*. Mais acrescentou que na jurisprudência firme desta Comissão encontrava-se fixado o entendimento que o tratamento de dados pessoais sensíveis carecia de autorização prévia da CNPD e que, além disso, se devia mostrar uma relevante pertinência e adequação, considerando a sua finalidade. (**Parecer 44/2003**).

.....

e) *Comunicações electrónicas*

Sobre os tratamentos de dados pessoais através de meios electrónicos, a CNPD emitiu diversos pareceres a diplomas legais que transpuseram as Directivas Comunitárias sobre o Comércio Electrónico e sobre a Privacidade nas Comunicações Electrónicas, respectivamente, a Directiva 2000/31/CE do Conselho e do Parlamento de 8 de Junho de 2000 e a Directiva 2002/58/CE do Conselho e do Parlamento, de 12 de Julho de 2002. (**Parecer 6/2003, Parecer 12/2003, Parecer 20/2003, Parecer 45/2003**).

9 – TRATAMENTO DO DADO “RAÇA”

Foi notificado à CNPD um tratamento relativo aos dados de natureza clínico-laboratorial relativos à observação de doentes de consulta de um estabelecimento hospitalar. Estes dados tinham implicação no plano da programação de actos terapêuticos no âmbito da especialidade.

Este tratamento fazia o registo da «raça». A questão que se colocava era a de saber se o registo da raça era possível no nosso ordenamento jurídico.

Tanto a CRP (art. 35.º n.º 3) como o artigo 7.º n.º 1 e 2 da Lei 67/98 estabeleciam que o tratamento da raça ou etnia só podia ser feito se houvesse disposição legal que o admitisse ou consentimento dos titulares dos dados.

O artigo 6.º da Convenção n.º 108 do Conselho da Europa, ratificada pelo Dec. do Presidente da República n.º 21/93, de 9 de Julho, estabelecia que estes dados só podiam ser objecto de tratamento caso «o direito interno preveja garantias adequadas».

Não existia qualquer disposição legal no nosso ordenamento jurídico que permitisse o tratamento destes dados no âmbito do diagnóstico, gestão ou prestação de cuidados de saúde.

Assim, o tratamento destes dados só seria possível se houver *consentimento expresso* do titular dos dados (cf. art. 35.º n.º 3 da CRP e art. 7.º n.º 1 e 2 da Lei 67/98) e quando houvesse garantias de não discriminação e medidas de segurança adequadas.

A CNPD só poderia autorizar o tratamento desta informação se a mesma se revelasse pertinente, necessária e não excessiva em relação à finalidade declarada (cf. o artigo 5.º n.º 1 al. c) da Lei n.º 67/98).

Não foi possível obter uma conclusão pacífica e uniforme sobre a necessidade e imprescindibilidade do tratamento da raça ou etnia para efeitos de medicina preventiva, diagnóstico ou prestação de cuidados de saúde.

Admitiu-se, por outro lado, que o registo desta informação sensível pudesse ser dispensável em certo tipo de tratamentos. Isto é, a necessidade de registo não se colocava com igual acuidade e pertinência, podendo variar em função das sintomatologias e doenças, bem como da finalidade dos tratamentos. Parecia pacífico que a recolha sistemática deste dado (vg. em sede de tratamento do “*dossier clínico geral*” de doentes) se podia revelar excessiva.

Em Espanha admitia-se o tratamento da etnia e da raça quando houvesse consentimento dos titulares dos dados.

Em França, a CNIL tinha vindo a aceitar ou a não autorizar a recolha e processamento da raça em função do tipo de tratamento que lhe era apresentado. Não autorizou o tratamento de dados que pudessem identificar a raça dos jovens inadaptados acolhidos em estabelecimentos especializados, no âmbito de inquérito relativo à gestão administrativa e médico-social. Aceitou o tratamento da origem racial no âmbito de um estudo científico específico sobre a SIDA, com o objectivo de “*permettre éventuels relacionamentos entre esta informação e as manifestações clínicas do vírus*”. Por outro lado, não admitiu o tratamento da nacionalidade no projecto de informatização dos *dossiers* de vítimas de contaminação por HIV, na sequência de transfusões para servirem de base ao arbitramento de indemnizações, na medida em que este dado não se revelava necessário à finalidade e poderia, eventualmente, ser fonte de discriminação na atribuição das indemnizações. Da análise das decisões da CNIL verificava-se, porém, que não existia uma oposição sistemática ao registo daquela informação.

A CNPD entendeu que o tratamento da raça só poderia ocorrer em casos excepcionais, devidamente justificados e em que o responsável invocasse motivos atendíveis e ponderosos para fundamentar a referida excepção (vg. quando estivessem em causa motivos de investigação antropológica ou epidemiológica). Ainda assim, o trata-

mento só seria possível quando houvesse consentimento expresso dos titulares dos dados (cf. art. 7.º n.º 2 da Lei 67/98).

O requerente informou a CNPD que o tratamento da raça era de importância inequívoca por duas ordens de razões:

- *“Contribuir, numa perspectiva nacional, para o estudo da frequência dos diferentes grupos sanguíneos, permitindo contornar o recurso habitual a dados obtidos no estrangeiro;*
- *“Seleção criteriosa, na fase prévia à execução de provas de compatibilidade, das unidades de sangue destinadas a doentes com grupos sanguíneos raros, os quais são sabidamente mais frequentes em determinadas raças, contribuindo deste modo para um incremento na segurança transfusional”.*

A CNPD foi sensível às preocupações manifestadas em matéria de «segurança transfusional». A CNPD considerou que, a título excepcional e exclusivamente no âmbito do serviço de Imuno-hemoterapia, estavam suficientemente explicitadas as razões que permitiam fundamentar uma autorização excepcional do tratamento da raça. **(Autorização 491/2003).**

.....

Num outro caso, um hospital veio proceder à notificação dos tratamentos realizados no âmbito da actividade desenvolvida naquele estabelecimento de saúde.

Havia dois tratamentos – o arquivo de dados clínicos (no serviço de nefrologia) e a gestão clínica e laboratorial no âmbito do serviço de dermatologia – que procediam ao tratamento da «origem étnica» dos doentes.

O serviço de dermatologia considerou que a informação referente à “coloração cutânea” era indispensável para a actividade clínica. «A referência à “etnia” poderia ser substituída por fototipo cutâneo, uma classificação que se baseava na raça e ainda na pigmentação cutânea, cor de pele, cor de cabelo, cor dos olhos, sendo o registo efectuado numa classificação de I a VI».

A verdade é que o tratamento destes dados não pode deixar de merecer alguma reflexão e determinar medidas que evitem que o processamento não pertinente possa originar a realização de discriminações que, para além do art. 35.º n.º 3 da CRP e da

Lei 67/98, a Lei n.º 134/99, de 28 de Agosto, veio proibir de forma expressa no âmbito da saúde.

O Hospital pretende apenas tratar dados relativos ao fototipo cutâneo, informação que num serviço de dermatologia se revela pertinente.

A CNPD considerou que nos dois tratamentos notificados deviam ser observados os seguintes princípios:

1. O Hospital podia proceder ao tratamento da etnia de forma não nominativa, isto é, de modo a que a origem étnica não pudesse ser relacionada com a identificação dos titulares dos dados;
2. O dado raça devia ser eliminado do tratamento relativo ao serviço de nefrologia;
3. Admitiu-se o tratamento de informação relativa ao «fototipo cutâneo» no serviço de dermatologia;
4. Uma vez que as tabelas de «fototipo cutâneo» podiam evidenciar informação sobre o tratamento do dado raça, deve ser obtido o consentimento dos titulares para o referido tratamento. (**Autorização 504/2003**).

.....

Também outro estabelecimento hospitalar procedia ao tratamento do dado “raça” em várias aplicações: *Serviço de Gastroenterologia, Medicina 1 e Cirurgia 1*.

O Hospital apresentou um documento subscrito pelos médicos responsáveis dos respectivos serviços que referia o seguinte:

- a) Considerava-se que a raça era parte integrante da História Clínica do doente;
- b) Não sendo necessário esse registo sistemático, «*é útil que figure nos dados clínicos do doente internado ou de consulta externa*»;
- c) O registo era feito pelo médico e não pelo administrativo;
- d) A raça era informação «*necessária, frequentemente, no diagnóstico diferencial e é informação imprescindível em muitos estudos epidemiológicos*».

Não foram apresentados fundamentos científicos relevantes para, naqueles serviços em concreto, considerar o tratamento daquele de dado como imprescindível ao diagnóstico e prestação de cuidados de saúde. Pelo contrário referiu-se que o seu

registo é «útil», facto que foi insuficiente para fundamentar o tratamento de um dado pessoal que só em casos excepcionais devia ser autorizado.

O tratamento destes dados só poderia ser feito com o consentimento expresso e informado dos interessados, os quais poderiam – em qualquer momento – retirar esse consentimento.

Assim, a CNPD entendeu que o tratamento da raça só poderia ocorrer em casos excepcionais, devidamente justificados e em que o responsável invocasse motivos atendíveis e ponderosos para fundamentar a referida excepção (vg. quando estejam em causa motivos de investigação antropológica ou epidemiológica ou quando, em serviço ambulatorio, haja necessidade de saber a raça para realizar exames e não esteja presente o doente). Ainda assim, o tratamento só seria possível quando houvesse consentimento expresso dos titulares dos dados (cf. art. 7.º n.º 2 da Lei 67/98).

No caso dos autos não foram apontadas razões clínica e cientificamente relevantes que permitam à CNPD pronunciar-se favoravelmente àquele tratamento nos serviços indicados. (**Autorização 532/2003**).

.....

Num outro contexto, uma entidade veio notificar um tratamento cuja finalidade era a gestão de recursos humanos, quer da empresa, quer do grupo empresarial americano de que a requerente era subsidiária. O tratamento era feito, ainda, para fins de contabilização e pagamento de quaisquer formas de remuneração e para cumprimento de obrigações legais e fiscais. Nesse âmbito, a entidade propunha-se tratar o dado “raça”.

Na sequência de pedido de informação da CNPD sobre a necessidade e finalidade de tratar tal dado, a requerente informou que renunciava à pretensão do tratamento do dado raça, pelo que este não será tratado. (**Autorização 492/2003**).

10 – VIDEOVIGILÂNCIA EM PARQUES NATURAIS

O Instituto da Conservação da Natureza (ICN) veio notificar a Comissão Nacional de Protecção de Dados (CNPD) de um «sistema de televigilância do Parque Natural da Arrábida e Reserva Natural do Estuário do Sado». O sistema instalado – «Sistema

CICLOPE» – era composto por um conjunto de 10 pontos de captação de imagens, um ponto retransmissor e um Centro de Gestão e Controlo.

A finalidade declarada pelo responsável foi a seguinte: *«vigilância e detecção de fogos florestais, obras de construção ilegais, caça furtiva, depósito de entulhos, alterações de morfologia do solo, actividades interditas (nomeadamente motorizadas em locais inadequados, pesca ilegal) e monitorização em várias áreas científicas».*

Para assegurar o direito de informação foi afixado um aviso nas entradas rodoviárias do Parque Natural da Arrábida e Reserva Natural do Estuário do Sado, nos seguintes termos: *«para sua protecção, este território dispõe de um sistema de videovigilância».*

A CNPD proferiu projecto de autorização em que constavam como conclusões fundamentais *“não autorizar o tratamento, tal como está concebido, na medida em que não existe fundamento legal, à luz da Lei n.º 67/98, que permita legitimar a sua realização (cf. artigo 28.º, n.º 1, alínea a) da Lei n.º 67/98, determinando-se que o ICN deverá propor novas soluções técnicas que assegurem a preservação do direito à privacidade das pessoas residentes e que frequentem a «área vigiada».* A CNPD decidiu, também, *que não podemos deixar de reconhecer que o direito de informação se encontra assegurado de forma manifestamente insuficiente”.*

A CNPD nunca colocou em causa o valor e a riqueza do património natural, nem questionou a necessidade de o preservar em face dos riscos a que está sujeito.

Não havendo em Portugal legislação específica sobre a utilização de videovigilância para as finalidades requeridas, foi para a CNPD pacífico que as condições de tratamento de imagem – ao qual é aplicável o artigo 4.º n.º 4 da Lei 67/98 – só podiam ser apreciadas à luz da Lei 67/98, não se colocando problemas de inconstitucionalidade orgânica. Isto é, a CNPD podia proibir o tratamento de dados quando houvesse violação dos princípios relativos à “qualidade dos dados” (artigo 5.º da Lei 67/98): quando se revelasse estarem a ser recolhidos de forma ilícita (v.g. gravação de imagem ao nível das actividades de detectives privados), quando se revelassem excessivos e desproporcionados ou quando não houvesse fundamento legítimo que justificasse o tratamento.

No caso em apreço o responsável, que se limitava a afixar nas entradas rodoviárias do parque Natural da Arrábida e da Reserva Natural do Estuário do Sado um aviso, propôs-se a colocar *“editais em locais públicos bastante frequentados nas zonas onde*

os equipamentos se encontram instalados”. Embora a proposta apresentada pudesse ser insuficiente para assegurar o direito de informação, admitiu que fosse possível encontrar uma metodologia que permitisse assegurar, minimamente, o direito de informação a uma grande parte da população, sendo certo que seria impossível fazer chegar a «mensagem» a todas as pessoas visadas.

Em relação às *condições de legitimidade* para o tratamento, não pôde a CNPD deixar de integrar esta operação na previsão do artigo 7.º da Lei 67/98, de 26 de Outubro.

Não havendo *consentimento das pessoas* (o que se torna claramente inviável) nem disposição legal em que pudesse assentar este tratamento, interessava apurar se a CNPD poderia considerar que estava perante um tratamento de dados que estava fundamentado num «*interesse público importante*» que se apresentava como «*indispensável ao exercício das atribuições legais ou estatutárias do seu responsável*».

Interpretando, desta forma, o n.º 2 do artigo 7.º, à CNPD cabe, nesta fase, verificar se existe uma correcta ponderação entre os direitos fundamentais em presença.

O princípio da proporcionalidade do n.º 2 do artigo 18.º da CRP, representava, aquando do recurso à actividade de videovigilância, a necessidade de apreciar a idoneidade do meio utilizado, bem como a sua consideração ao abrigo de um princípio de intervenção mínima.

O princípio da intervenção mínima obrigava, necessariamente, a que, em cada caso concreto, se ponderasse entre a finalidade pretendida e a necessária compressão de direitos fundamentais, aqui concretamente o direito à privacidade e à imagem. Não pôde a CNPD olvidar, por outro lado, que o «olhar indiscreto» e bastante intrusivo – dotado de técnicas de *zooming* e de tratamento digital – estava direccionado, também, para uma região com uma população significativa. Esta grande «capacidade de vigiar» podia causar alguma desconfiança, mal-estar e alarme social nas populações, em face da possibilidade de o sistema poder ser utilizado para o controlo de movimentos de pessoas e se apresentar como susceptível de violar o seu direito à imagem e à privacidade.

Assim, a CNPD considerou que “*podem ser implantados sistemas de vigilância em patrimónios naturais, ainda que dessa actividade possa resultar uma limitação da privacidade de moradores e visitantes.*”

A Comissão Nacional de Protecção de Dados deliberou autorizar o tratamento declarado relativamente à finalidade de *vigilância e detecção de fogos florestais*, desde que:

- a) o ICN introduzisse no sistema de vigilância as alterações necessárias – na terminologia adoptada na resposta *correções, aperfeiçoamentos com vista ao ajustamento ao sistema* para que a actividade de videovigilância respeitasse o direito à privacidade das pessoas residentes ou que frequentavam a «área vigiada»;
- b) o ICN conservasse as gravações durante o período de 30 dias, de forma a garantir uma actividade fiscalizadora eficaz desta Comissão. (**Autorização 496/2003**).

11 – TRATAMENTO DE DADOS NO ÂMBITO DE PROGRAMAS TELEVISIVOS

Uma produtora televisiva veio notificar um tratamento de dados com vista à selecção de concorrentes para participação em programa televisivo.

Eram tratados dados pessoais relativos a: Aspectos Gerais; Família e Estilo de Vida; Estado de Saúde e Criatividade.

Tratando-se de recolha de dados sensíveis, designadamente de dados de saúde, sexuais e da vida privada, importava aferir das condições de legitimidade do seu tratamento e das condições de segurança.

Relativamente ao «consentimento expresso», exigido pelo n.º 2 do artigo 7.º, considerou-se o mesmo obtido em face da parte inicial do texto da declaração da qual resultava que o titular dos dados *“autoriza, expressa e inequivocamente, que todos os dados pessoais a mim referentes, e por mim fornecidos de livre vontade, incluindo de natureza sensível, sejam recolhidos e tratados pela Endemol Portugal Ld.ª, incluindo todos os seus funcionários, empregados ou auxiliares, para efeitos de selecção dos concorrentes ao programa”*.

Contudo, no que às «medidas de segurança» diz respeito, houve de proceder a alterações do tratamento. Isto porque, não se vislumbraram que medidas, das indicadas no artigo 15.º da Lei n.º 67/98, foram, em concreto, adoptadas. Com efeito, não foram estabelecidos níveis de acesso à informação, sendo possível a todos os funcionários, sem excepção, aceder a dados da vida sexual, de saúde e vida privada dos candidatos.

Ora, considerando-se excessivo que todos, sem excepção, tivessem acesso à informação, devia o acesso e a sua utilização ser restrito ao pessoal que dela necessitasse para seleccionar o candidato. Assim, apenas aos elementos da equipa que tivessem responsabilidade e poder de decisão na escolha dos concorrentes ao programa podiam ter acesso à informação. (**Autorização 511/2003**).

.....

Num outro caso semelhante, considerando que quer o processo de selecção para o reality show quer a emissão do programa já tinham terminado, devia o responsável, em cumprimento dos princípios em matéria de protecção de dados constantes do artigo 5.º da Lei n.º 67/98, designadamente da licitude e da finalidade do tratamento, proceder à eliminação de toda e qualquer informação de natureza pessoal recolhida no âmbito do citado programa.

Nas situações em que, após a emissão do programa e em condições de liberdade, os concorrentes e suplentes tivessem autorizado expressamente a conservação dos seus dados, o responsável deveria submeter a autorização desta CNPD tal possibilidade, porquanto a finalidade na conservação seria, pelos motivos acima expostos, necessariamente diferente da que determinou a recolha (Cfr. artigo 28.º n.º 1, al. d) da Lei n.º 67/98). (**Autorização 506/2003**).

.....

12 – DIFUSÃO DE DADOS NA INTERNET

A CNPD recebeu uma queixa de uma mãe e encarregada de educação de aluno sobre a divulgação dos nomes dos alunos – listados por turmas – e as respectivas fotografias, no site da Internet do estabelecimento de ensino, o que não tinha autorizado.

A CNPD, após ter investigado o caso, verificou que eram publicitados no *site*, estando acessíveis ao público, as várias turmas e os nomes dos alunos; era possível visualizar, imprimir e copiar a fotografia de cada aluno; o *site* disponibilizava, ainda, uma «galeria de fotografias» que documentava várias realizações levadas a efeito na esco-

la, algumas das quais de índole religiosa; o tratamento destes dados não se encontrava notificado à CNPD.

A disponibilização pública dos dados pessoais dos alunos, nas circunstâncias descritas e sem qualquer controlo da CNPD, apresentava um grande risco para a sua privacidade, para além de violar o direito à imagem.

A CNPD entendeu que se justificava, no caso em apreço, uma *medida cautelar de bloqueio temporário do site* até que fosse comprovada junto desta Comissão, por parte do estabelecimento de ensino a observância de todos os princípios da Lei 67/98. (**Deliberação 32/2003**), bem como foi aplicada posteriormente uma coima (**Deliberação 64/2003**).

Num outro caso, a CNPD recebeu uma queixa de encarregado de educação de aluno, na qual referia que o *site* da Internet de um estabelecimento de ensino divulgava os nomes dos alunos – listados por turmas – e as respectivas notas de avaliação, categorias de faltas.

A CNPD verificou então que:

1. Eram publicitados no *site*, estando acessíveis ao público, os nomes dos alunos das várias turmas do 2.º e 3.º ciclo do ensino básico e do ensino secundário, bem como as notas por disciplina, as faltas (injustificadas e justificadas), a exclusão por faltas, as transferências dos alunos;
2. Uma vez posicionados na página referida – que apresentava a *listagem de alunos que integram cada turma* – era possível visualizar, imprimir e copiar os mapas das notas de cada aluno e por turma;
3. O tratamento destes dados não se encontrava notificado à CNPD.

A CNPD entendeu, também aqui, que se justificava uma medida cautelar de remoção da informação dos alunos do referido *site* até que fosse comprovada junto desta Comissão, por parte da escola, a observância de todos os princípios da Lei 67/98. (Deliberação 47/2003) e a posterior aplicação de uma coima (Deliberação 78/2003).

2 0 0 4

I – DADOS SENSÍVEIS

1 – DADOS DE SAÚDE

a) *Saúde Escolar*

1.a.1. – No âmbito das suas competências, a CNPD deliberou sobre o fornecimento de dados pessoais dos alunos de estabelecimentos de ensino aos Centros de Saúde insertos em Sub-Regiões de Saúde.

Considerou a CNPD que, porque está em causa uma “missão de interesse público” (cf. artigo 6.º alínea d) da Lei 67/98) e os dados pessoais – embora não sejam sensíveis (dados de saúde) – se destinem a fazer o levantamento da população escolar, com o objectivo de vir a realizar acções com finalidades de medicina preventiva ou diagnóstico (cf. artigo 7.º n.º 4 da Lei 67/98), os dados devem ser fornecidos ao Centro de Saúde.

O seu fornecimento ao Centro de Saúde, entendeu ainda a CNPD, exclusivamente para a finalidade indicada (valorização dos cuidados antecipatórios como factor de promoção da saúde e de prevenção da doença, nomeadamente facultando aos pais os conhecimentos necessários ao melhor desempenho da sua função parental; detecção precoce e encaminhamento de situações passíveis de correcção e que possam afectar negativamente a saúde da criança; apoio e responsabilização progressiva e auto-determinação em questões de saúde das crianças e jovens), não apresenta qualquer perigo de discriminação ou violação da privacidade (cf. artigo 2.º da Lei 67/98), tanto mais que o Centro de Saúde já detém, na generalidade dos casos, estes dados.

No entanto, a CNPD entendeu que só poderão ser fornecidos os seguintes dados: o **nome do estabelecimento de ensino**, o **nome do aluno**, **data de nascimento**, **Centro de Saúde a que pertence** e **n.º de Utente**.

Isto é, para a CNPD, tendo em vista a finalidade prosseguida pelos Centros de Saúde e pelas respectivas Sub-Regiões de Saúde, **os dados relativos à identificação do médico de família e do pediatra, bem como a idade, ano de escolaridade, morada e filiação são excessivos para face à finalidade visada.**

1.a.2. – Por outro lado, a CNPD teve conhecimento, através da comunicação social, de que *“há Centros de Saúde que enviam para as escolas a ficha médica das crianças com registo de todas as doenças crónicas”*.

Foi referido por instituições com responsabilidade nas áreas concretas em questão que *“os exames de saúde globais que terminam numa ficha de medicina familiar são informações técnicas, que são entregues pelos médicos de família aos técnicos de saúde escolar. É assim em todo o país”*.

A CNPD, observando a Lei de Bases da Saúde – Lei 48/90, de 24 de Agosto (e também tendo em conta o Programa da Saúde Escolar) – verificou que *“deve ser promovida uma intensa articulação entre os vários níveis de cuidados de saúde, sendo de garantir a circulação recíproca e confidencial da informação clínica relevante sobre os utentes”* (Base XIII, n.º 2). Por isso, de entre os **direitos dos utentes**, assume particular relevância a obrigação de *“respeito pela confidencialidade sobre os dados pessoais revelados”* (Base XIV, alínea d).

Assim, considerou a CNPD que a inclusão de dados de saúde detalhados, conforme ficou comprovado, integra uma comunicação excessiva de dados, desproporcionada à finalidade prosseguida e, como é óbvio, susceptível de gerar discriminação dos alunos. Perante a posição das escolas – que consideram necessária a apresentação da cópia de “ficha de ligação” como condição para a aceitação da matrícula – ficam os pais confrontados perante a impossibilidade de guardarem reserva em relação a alguns dados inseridos na referida ficha.

A CNPD considerou que os procedimentos denunciados e verificados nas escolas – em que as “fichas de ligação” estão integralmente preenchidas e com inclusão de dados de saúde susceptíveis de discriminar os alunos – são violadores da sua privacidade, por consubstanciarem uma divulgação indevida e desproporcionada de dados de saúde.

Determinou, por isso, que devem cessar, de imediato, tais procedimentos.

b) *Acesso a Dados de Saúde*

1.b.1. – A CNPD tomou a Deliberação n.º 51/2001 sobre o acesso a dados de saúde em diversos casos, sendo a orientação dessa Deliberação seguida nas decisões da Comissão.

Casos tem havido, nesta matéria de acesso a dados de saúde que, sem qualquer desvio dessa Deliberação, têm conhecido decisões deliberativas e autorizantes da CNPD que merecem assinalar.

A CNPD foi chamada a pronunciar-se sobre um pedido de acesso à informação clínica de um indivíduo, pedido esse apresentado por uma Companhia de Seguros junto de um Hospital.

Em concreto, a Companhia pretendia informação sobre o grau de alcoolémia que o seu segurado era portador à data do sinistro automóvel de que foi vítima, e em resultado do qual veio a falecer, por forma a determinar se haverá lugar ao pagamento do capital por morte no âmbito do seguro de acidentes pessoais com aquele contratado.

O interesse invocado pela Companhia de Seguros foi o seguinte: nos termos do ponto 1 do artigo 6.º das condições gerais da apólice de seguro *“Ficam sempre excluídas da cobertura do presente contrato os sinistros consequentes de a) Acção ou omissão de Pessoa Segura sob o efeito de álcool ou de bebida alcoólica que determine grau de alcoolémia superior a 0,5 gr por litro”*. Impedia, pois, sobre a companhia de seguros a demonstração desse facto, demonstração que pretendia efectuar através do acesso solicitado aos dados de saúde do seu segurado.

No entanto, a CNPD não autorizou o acesso

Para a CNPD, com a publicação do Acórdão n.º 6/2000, de 28 de Maio desse ano, do Supremo Tribunal de Justiça, foi fixada jurisprudência nos seguintes termos: *“A alínea c) do artigo 19.º do Decreto Lei 522/85, de 31 de Dezembro, exige para efeitos de procedência do direito de regresso contra o condutor por ter agido sob influência do álcool o ónus da prova pela seguradora do nexo de causalidade adequada entre a condução sob o efeito do álcool e o acidente”*.

Resultou, assim, do referido acórdão, no entendimento da CNPD, que a Companhia de Seguros só poderia exercer o direito de regresso no caso do seu segu-

rado ter tido um acidente quando conduzia sob o efeito de álcool se demonstrar a relação causa-efeito entre a condução no referido estado e o acidente.

Ora, no acesso pedido, o fundamento da Companhia de Seguros foi pretender não pagar o capital coberto pelo seguro em virtude da obtenção da informação relativa ao grau de alcoolémia do seu segurado.

Tal fundamento, porém, no entender da CNPD, não era legal.

Assim, e considerando que dos autos não resultou que a Companhia de Seguros pretendesse saber qual o grau de alcoolémia, com vista à interposição de uma acção judicial para efeitos de exercício do direito de regresso, esta Comissão deliberou negar o acesso à informação pretendida, sem prejuízo da Companhia de Seguros vir demonstrar o contrário.

Ainda que o segurado tivesse dado o consentimento para a Companhia de Seguros aceder aos seus dados pessoais complementares constantes de entidades públicas, para efeitos de gestão do contrato, considerou-se que tal declaração não consubstanciava uma manifestação de vontade livre, específica e informada conforme é exigido pela Lei n.º 67/98 (Cfr. artigo artigo 3.º alínea h), uma vez que o segurado, desde logo, não conhecia, em pormenor, porque omissa na declaração, quais “os dados pessoais complementares necessários à gestão contratual”, que poderiam ser solicitados “junto dos organismos públicos”, faltando, assim, o “consentimento expresso” exigido pela lei no acesso a esta informação (Cfr. artigo 35.º da Constituição da República Portuguesa e artigo 7.º, n.º 2 da Lei n.º 67/98).

Pelo exposto, a CNPD deliberou não autorizar o acesso à informação sobre o grau de alcoolémia de um segurado para efeitos de pagamento do capital de risco.

2 – DADO PESSOAL “VIDA PRIVADA”

a) Videovigilância

2.a.1. Após a declaração de inconstitucionalidade orgânica do Decreto-Lei 231/98 de 22 de Julho⁽¹⁴⁾, ficaram pendentes diversos pedidos de autorização de

⁽¹⁴⁾ Acórdão do Tribunal Constitucional de 12 de Junho de 2002, publicado na 1.ª Série A do Diário da República de 8 de Julho de 2002, pag. 5237.

tratamento de dados pessoais através de captação de imagem e som, com e sem gravação, genericamente designados de tratamentos de videovigilância.

Procedendo a aturada análise do regime vigente para a videovigilância, apelando à experiência comparada de outras entidades de diferentes países, a CNPD extraiu algumas conclusões que se converteram em importantes pressupostos, critérios e instrumentos de deliberação neste domínio.

Assim e em primeiro lugar, apesar de existir a possibilidade de fundamentar e legitimar o tratamento de videovigilância em disposição legal ou consentimento (cf. artigo 7.º n.º 2 da Lei 67/98), na protecção de interesses vitais⁽¹⁵⁾ (art. 7.º n.º 3 alínea a) ou no exercício e defesa de um direito em processo judicial (art. 7.º n.º 3 alínea d), importa não perder de vista que a esmagadora maioria dos pedidos de notificação tem como finalidade assegurar a “**protecção de pessoas e bens**”, tendo como pano de fundo a utilização das imagens como prova das infracções criminais praticadas, em observância das disposições processuais penais.

Ora, estando em causa objectivos relacionados com a prevenção de crimes, entendeu a CNPD que o fundamento de legitimidade poderá, nestes casos, ser encontrado na previsão do artigo 8.º n.º 2 da Lei 67/98, de 26 de Outubro. A autorização da CNPD (cf. artigo 28.º n.º 1 alínea a) terá que respeitar os diversos pressupostos estabelecidos naquele preceito.

Muito embora o artigo 8.º n.º 2 se refira ao tratamento relativo a “*suspeitas de actividades ilícitas, infracções penais, contra ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias*”, não pôde a CNPD deixar de considerar que as tarefas de recolha e tratamento de informação no contexto da *prevenção criminal* se devem enquadrar neste preceito⁽¹⁶⁾.

Sendo pressuposto que as imagens recolhidas possam servir de prova em processo penal (cf. o artigo 13.º n.º 2 do DL 35/2004) não pôde, ainda, a CNPD deixar de considerar esta finalidade e englobar a recolha de dados, bem como a obtenção

⁽¹⁵⁾ Um exemplo do recurso a sistemas de videovigilância em ambiente hospitalar será o controlo e monitorização de doentes (v.g. cuidados intensivos).

⁽¹⁶⁾ Deve anotar se que o artigo 11.º n.º 2 da Lei 67/98, que estabelece condicionantes em relação ao direito de acesso, limita o exercício do direito de acesso quando estão em causa finalidades relativas à “*prevenção ou investigação criminal*”.

dos meios de prova, numa estratégia integrada que visa a protecção de pessoas e bens. Ou seja, a informação recolhida pode vir a ser utilizada como prova da infracção.

Por isso, não será legítimo defender que todas as pessoas que frequentam os locais públicos sujeitos a videovigilância se apresentam como “potenciais suspeitos”. O que está em causa na utilização destes meios é assegurar a dissuasão, **sempre com o conhecimento das pessoas e com protecção dos seus direitos fundamentais**⁽¹⁷⁾, bem como registar e documentar a eventual prática de infracções. O tratamento de som ou imagem e a finalidade delineada pelo responsável, porque assume objectivos primordialmente preventivos e dissuasores, não tem que “situar-se, necessariamente, a montante de qualquer actividade delituosa”⁽¹⁸⁾ ou pressupor a existência de suspeitas concretas sobre a generalidade das pessoas em relação às quais são captadas as imagens.

As imagens só têm relevância e só são “pertinentes” (cf. artigo 5.º n.º 1 alínea c) da Lei 67/98) quando ocorrer algum facto com relevância em sede de investigação criminal. Neste caso serão as imagens encaminhadas para a autoridade competente.

Aliás, na linha do que dispõe o artigo 13.º n.º 2 do DL 35/2004, as imagens só podem ser utilizadas nos termos da lei processual penal.

Em face do exposto a CNPD propôs-se autorizar o tratamento de som e imagem quando, observados os princípios relativos à qualidade dos dados (artigo 5.º), o direito de informação (artigo 10.º), as “condições de legitimidade” (artigo 7.º e 8.º n.º 2) e demais princípios da Lei 67/98 que, no caso concreto, forem exigíveis.

⁽¹⁷⁾ O artigo 8.º n.º 2 obriga, como condição a ponderar pela CNPD, a que “não prevaleçam os direitos, liberdades e garantias dos titulares dos dados”. Em geral, o êxito das diligências de observação e vigilância está dependente da ignorância por parte do visado do facto de que está a ser objecto de escutas, de gravação de som e imagem. A doutrina do Tribunal Europeu dos Direitos do Homem, relativa às escutas telefónicas e à possível violação do artigo 8.º da CEHD, salientou que “a natureza secreta desta modalidade de diligência apresenta riscos de abusos e, por conseguinte, a intervenção realizada só pode considerar-se ‘necessária numa sociedade democrática’ se o sistema de vigilância se rodear de garantias suficientes” (Caso Malone de 2 de Agosto de 1984). Para maior desenvolvimento veja-se José Francisco Etxeberria Guridi “La Protection de los Datos de Carácter Personal en el Ámbito de la Investigación Penal”, 1998, pág. 291.

⁽¹⁸⁾ Veja-se, em relação à actuação policial, Marcello Caetano “Manual de Direito Administrativo”, Coimbra, 9.ª Edição, II Vol. pág. 1145.

2.a.3. – Entre as condições a observar importava conferir particular atenção – quando aplicável o artigo 8.º n.º 2 da Lei 67/98 – aos pressupostos em que assentava o tratamento e à sua determinação pela necessidade de “execução de finalidades legítimas do seu responsável”. Para além disso, era exigível que, por força desse tratamento, “não prevaleçam os direitos, liberdades e garantias do titular dos dados.

O tratamento a realizar e os meios utilizados devem ser considerados os **necessários, adequados e proporcionados** com as finalidades estabelecidas: a protecção de pessoas e bens.

O princípio da intervenção mínima obriga, necessariamente, que, em cada caso concreto, se pondere entre a finalidade pretendida e a necessária violação de direitos fundamentais, aqui concretamente o direito à privacidade e à imagem.

Deverá mesmo pressupor-se que, no caso concreto, o risco a prevenir deverá ser de todo razoável⁽¹⁹⁾ e proporcionado quando comparado com os direitos fundamentais de terceiros que são afectados com a utilização destes meios.

Por isso, em cada caso concreto e de acordo com os princípios acabados de enunciar, a CNPD deverá limitar ou condicionar a utilização de sistemas de videovigilância quando a utilização destes meios se apresentem como excessivos e desproporcionados aos fins pretendidos e tenham consequências gravosas para os cidadãos visados.

2.a.4. – Sendo patente que os sistemas de videovigilância estão direccionados para o desempenho de finalidades relativas à “protecção de pessoas e bens”, apresentando-se como medida preventiva e de dissuasão em relação à prática de infracções penais e podendo, ao mesmo tempo, servir de prova nos termos da lei processual penal, é imprescindível que – de acordo com o *princípio da necessidade* – o acesso às imagens seja restrito às entidades que delas precisam para alcançar as finalidades delineadas. Uma vez detectada a prática de infracção penal, a entidade responsável pelo tratamento deve – com a respectiva participação – enviar ao órgão de polícia criminal ou à autoridade judiciária competente as imagens recolhidas. Não há qualquer justificação para a visualização das imagens por parte das entidades responsáveis, por duas ordens de fundamentos:

(19) Veja se a Deliberação n.º 98/2002, de 21 de Maio.

- a) Caso não tenha sido praticada qualquer infracção penal ou procedimento que atente contra as pessoas e bens, a visualização de imagens não tem qualquer sentido útil, sob pena de violação do disposto no artigo 5.º n.º 1 alínea b) da Lei 67/98, de 26 de Outubro;
- b) Caso tenha sido praticada infracção penal as imagens devem, necessariamente, ser canalizadas para a autoridade competente.

Quando estiverem em causa imagens que servem de prova em processo criminal – imagens necessariamente sujeitas às regras do segredo de justiça – é aplicável o disposto no artigo 11.º n.º 2 da Lei 67/98 (prevenção ou investigação criminal), razão pela qual os pedidos de acesso devem ser encaminhados para a CNPD⁽²⁰⁾. Admite-se, excepcionalmente, a visualização das imagens quando – *não haven do qualquer infracção penal* – os titulares dos dados tenham solicitado o “direito de acesso”, nos termos do artigo 11.º da Lei 67/98. O responsável do tratamento não está dispensado de assegurar o direito de acesso⁽²¹⁾, razão pela qual lhe é exigível que procure a imagem captada em relação à pessoa visada que exerceu aquele direito.

No entanto, e porque o exercício do direito de acesso por parte de determinado interessado pode envolver o acesso a dados de terceiros, o responsável do tratamento deve tomar todas as medidas técnicas necessárias para ocultar/anonimizar as imagens de terceiros.

2.a.6. – Será admissível, igualmente, que determinadas pessoas – que não sejam os responsáveis pelos tratamentos – possam solicitar, no âmbito de processo criminal, o acesso às imagens para assegurar o “exercício ou defesa de um direito em processo judicial” e exclusivamente para essa finalidade (cf. artigo 7.º n.º 3

⁽²⁰⁾ Solução idêntica foi adoptada no direito francês, que admite a recusa do direito de acesso quando fundamentada em razões de segurança do Estado, da defesa e segurança pública ou de direitos de terceiros (artigo 10.º V da Lei 95 73, de 21 de Janeiro).

⁽²¹⁾ No direito francês o artigo 10.º da Lei 95 73, de 21 de Janeiro, estabelece que qualquer interessado pode dirigir-se ao responsável do tratamento de videovigilância para obter um acesso aos registos que lhe dizem respeito ou de verificar a sua destruição no prazo previsto. Também o Decreto n.º 96 926, de 17 de Outubro, estabelece que o pedido de autorização prévia à instalação de um sistema de videovigilância deve especificar as modalidades do direito de acesso por parte do interessado (artigo 1.º n.º 10).

alínea d) da Lei 67/98). Isto é, determinado cidadão ou entidade que tenha sido lesado por determinada actuação ou procedimento captado por sistemas de videovigilância não estará inibido, com base no preceito citado, de poder beneficiar da prova captada para exercício dos seus direitos no contexto de participação criminal. Neste caso as imagens serão enviadas à autoridade judiciária ou órgão de polícia criminal competente.

b) *Videovigilância nos estádios*

2.b.1. Foi solicitada à CNPD autorização para serem recolhidas imagens no âmbito de eventos desportivos a realizar em Portugal, nomeadamente no EURO 2004, sendo as imagens e som captados nos locais públicos onde se concentrarão os adeptos, bem como nas imediações e interior dos recintos desportivos

2.b.2. Tendo por base, quer a *Resolução da Assembleia da República n.º 11/87, de 10 de Março*, que aprovou, para ratificação, a Convenção Europeia sobre a Violência e os Excessos dos Espectadores por Ocasão das Manifestações Desportivas e nomeadamente de Jogos de Futebol, quer a Lei n.º 38/98, de 4 de Agosto, que estabeleceu “medidas preventivas e punitivas a adoptar em caso de manifestações de violência associadas ao desporto”, verifica a CNPD que apenas o artigo 11.º deste diploma obriga os responsáveis de recintos desportivos onde se disputem competições profissionais a **“dispor de um sistema de vigilância e controlo por circuito fechado de televisão a fim de permitir o controlo visual de todo o recinto desportivo”**. Não foi, porém, nesta Lei e no domínio do **“acompanhamento e vigilância de grupos de adeptos”**, estabelecida qualquer possibilidade de utilização de sistemas de videovigilância. Por outro lado, o nosso ordenamento jurídico não tem disposições legais que permitam a recolha de imagens na via pública para fins de prevenção criminal, prevenção da violência ou recolha de prova. Entendeu a CNPD, por outro lado, que as autoridades policiais só podem recolher imagens no **“recinto desportivo”** quando se verificar que o sistema do organizador do espectáculo desportivo se revela insuficiente para zelar pela segurança do espectáculo desportivo. Neste caso, não estão estas autoridades dispensadas de notificar este tratamento.

2.b.3. Na apreciação dos tratamentos que envolvam o processamento de dados pessoais de som e imagem a CNPD tem sempre em atenção a jurisprudência mais recente do Tribunal Constitucional. O Acórdão de 12 de Junho de 2002⁽²²⁾ declarou, com força obrigatória geral, a inconstitucionalidade orgânica dos n.ºs 1 e 2 do artigos 12.º do DL 231/98.

2.b.4. – Para a CNPD foi pacífico que o pedido formulado não pôde enquadrar-se na previsão da *Lei n.º 38/98, de 4 de Agosto*, na medida em que esta previsão só pode integrar, no entendimento que tem sido dado pela CNPD, a vigilância feita às zonas de acesso e interior do recinto desportivo.

A recolha de imagens em locais públicos por parte das autoridade policiais não consta de qualquer disposição legal. Pelo contrário, diversa legislação limita a recolha de imagens por parte das autoridades policiais:

2.b.5. – Por isso, não tendo sido obtido **consentimento expresso dos titulares dos dados** (cf. artigo 7.º n.º 2 da Lei 67/98, de 26 de Outubro) – situação que se vislumbra inviável – a CNPD não viu que tal procedimento pudesse estar fundamentado em qualquer disposição legal, razão pela qual não autorizou a recolha de imagens.

c) *Autorizações de videovigilâncias nos estádios*

2.c.1. – Foi a CNPD notificada da recolha de imagens no estádio de futebol, com vista à segurança das instalações e protecção de pessoas e bens.

A CNPD proferiu uma decisão que fixou as condições em que considera legítimo o tratamento requerido por videovigilância nos estádios de futebol, nomeadamente com vista à realização do EURO 2004.

2.c.2. – Os aspectos relativos à prevenção da criminalidade (da qual não pode ser afastada a realização de actos terroristas) – em particular no âmbito da realização do EURO 2004 – foram equacionados em termos dos sistemas de segurança. Por

⁽²²⁾ Publicado na I.ª Série A do Diário da República de 8 de Julho de 2002, pág. 5237. Abordaremos, oportunamente (Capítulo III, ponto II), as implicações da declaração de inconstitucionalidade destes preceitos.

isso, o tratamento de dados foi também ser visto à luz do disposto no artigo 8.º n.º 2 e 3 da Lei 67/98, de 26 de Outubro.

A Assembleia da República – na Lei 38/98 – obrigou os organizadores de competições desportivas a dotarem os seus recintos de sistemas de videovigilância, sem que tivesse feito uma delimitação específica dos interesses conflitantes que podem decorrer da adopção desses sistemas. Por isso, o tratamento destes dados no caso em apreço está fundamentado em disposição legal (cf. artigo 7.º n.º 2 da Lei 67/98 e artigo 11.º da Lei 38/98, de 4 de Agosto).

A utilização de sistemas de videovigilância, à semelhança do que acontece noutros sistemas jurídicos, foi submetida à condição de observar o princípio da proporcionalidade “numa dupla versão de idoneidade e de intervenção mínima”⁽²³⁾.

2.c.3. – A capacidade dos sistemas instalados, pelas potencialidades que apresentavam em captar e tratar imagem com particular precisão nas zonas limítrofes e ao ponto de captar imagens nos prédios contíguos (**se isso acontecer**), obrigou a CNPD a perguntar se os meios utilizados, em face dos riscos que apresentam para os direitos das pessoas aí residentes e que frequentam aquelas zonas, podiam ser considerados os **necessários, adequados e proporcionados** com as finalidades do tratamento.

A CNPD considerou, em face da grande capacidade do sistema de videovigilância, dos riscos que apresentava para a invasão da privacidade das pessoas visadas, da natureza desproporcionada dos meios utilizados (violadores do princípio da “intervenção mínima”), que este tratamento de imagem, tal como estava concebido no momento da sua notificação, era violador dos princípios estabelecidos no artigo 2.º da Lei 67/98, não se apresentando como legítimo, à luz do artigo 7.º da Lei 67/98, de 26 de Outubro. Por outro lado, as pessoas visadas nem sequer seriam informadas que podiam ser vigiadas, facto que violava o disposto no artigo 10.º da Lei 67/98.

⁽²³⁾ Requisitos estabelecidos no artigo 6.º da lei espanhola (Ley Orgánica 4/1997, de 4 de Agosto). A idoneidade determina que “só poderá empregar se a camera de vídeo quando seja adequado, numa situação concreta, para a manutenção da segurança do cidadão, em conformidade com o disposto na lei” (n.º 2 do artigo 6.º). A intervenção mínima exige “a ponderação, em cada caso, entre a finalidade pretendida e a possível afectação, pela utilização da camera de vídeo, do direito à honra, à própria imagem e à intimidade das pessoas” (n.º 3).

2.c.4. – Pelas mesmas razões entendeu a CNPD que não era legítimo o tratamento à luz do artigo 8.º n.º 2 da Lei 67/98 na medida em que este preceito obriga a confrontar as finalidades estabelecidas com os direitos, liberdades e garantias do titular dos dados. Ora, porque se estava perante um conflitos de direitos fundamentais, afigurou-se à CNPD que, **caso fosse feito um tratamento na forma e amplitude que permitisse a recolha de imagens em residências contíguas (a existirem)**, havia uma violação dos artigos 26.º e 18.º n.º 2 da Constituição da República por a limitação da intimidade da vida privada das pessoas se revelar excessiva, não adequada, desproporcionada e desnecessária⁽²⁴⁾, traduzindo-se numa efectiva *aniquilação de um direito fundamental* sem se atender aos princípios da “mútua compressão” que deve nortear a harmonização de direitos fundamentais.

2.c.5. – Por isso, considerou a CNPD que, se isso acontecesse, ***deviam ser realizadas as alterações técnicas que evitassem a captação de imagens nas zonas limítrofes que excedessem os “perímetros de acesso” e nas habitações circundantes, através de uma das seguintes metodologias ou outras que se considerassem adequadas:***

- a) Limitação técnica – se o software o permitisse – da captação/recolha de imagem a partir de determinados ângulos de alcance das câmaras;
- b) Colocação de uma “malha” ou “grelha” que impedisse a recolha de imagens nas zonas limítrofes que excediam os “perímetros de acesso” e nas habitações circundantes;
- c) Substituição, em determinados locais, de câmaras móveis por câmaras fixas.

Ficou claro que as imagens não podiam ser comunicadas a terceiras entidades (vg. Imprensa, Federação ou Liga) na medida em que a finalidade de recolha era a protecção de pessoas e bens, bem como a prevenção e obtenção de prova ligada

(24) Cf. neste sentido o Acórdão do Tribunal Constitucional n.º 394/93, de 16 de Junho, in DR I.ª Série A, n.º 229, de 29 de Setembro de 1993.

ao espectáculo desportivo (cf. artigos 8.º n.º 2 e 5.º n.º 1 alínea b) da Lei 67/98, de 26 de Outubro, e artigo 11.º da Lei n.º 38/98, de 4 de Agosto).

Para além das situações em que se verificariam ocorrências – e que as imagens seriam entregues às autoridades policiais – não houve razão para permitir a conservação das imagens por períodos superiores a 30 dias. A CNPD, no âmbito dos poderes que lhe são conferidos pelo artigo 23.º n.º 1 alínea f) da Lei 67/98, fixou em 30 dias o prazo máximo de conservação das imagens recolhidas pelo sistema em apreciação.

2.c.6. – *Desde que fossem asseguradas as alterações propostas*, a CNPD autorizou a recolha e gravação de imagens e som.

d) *Videovigilância nas serras*

2.d.1. – Foi a CNPD notificada da intenção de proceder a um tratamento de televigilância composto por uma câmara de vídeo e por uma câmara de infravermelhos instaladas no posto de vigia de uma Serra, especificando a notificação que foram contempladas as possibilidades de definição de zonas cegas, não se permitindo a identificação, nem das pessoas objecto de visionamento, nem das matrículas dos veículos também observados.

2.d.2. – A CNPD já tinha dado uma autorização semelhante, desde que se garantisse que não se procedia a qualquer captação de imagens nas áreas urbanas ou de habitações, devendo estas encontrar-se cobertas por *blank zones*, não se permitisse a identificação das pessoas objecto de visionamento, nem das matrículas dos veículos também observados e as gravações fossem conservadas durante um período de 30 dias, de forma a garantir uma actividade fiscalizadora eficaz desta Comissão.

2.d.3. – Não havendo consentimento das pessoas (o que se tornava claramente inviável) nem disposição legal em que pudesse assentar este tratamento, interessava apurar se a CNPD poderia considerar que estava perante um tratamento de dados que estivesse fundamentado num “interesse público importante” que se

apresentasse como “indispensável ao exercício das atribuições legais ou estatutárias do seu responsável”, para aplicação do n.º 2 do artigo 7.º da LPD ⁽²⁵⁾.

2.d.4. – Relativamente à interpretação a fazer do n.º 2 do artigo 7.º da Lei n.º 67/98, de 26 de Outubro, considerou a CNPD que a fórmula legal “*indispensável*” devia valer com o sentido de “*contribuir relevantemente para o exercício de atribuições legais ou estatutárias*”. Assim, indispensável não se assumiu como sinónimo de único meio apto para o exercício de determinadas funções.

2.d.5. – Coube, por sua vez, à CNPD verificar se existe uma correcta ponderação entre os direitos fundamentais em presença.

A capacidade do sistema instalado obrigou a CNPD a perguntar se os meios utilizados, em face dos riscos que apresentavam para os direitos das pessoas, podiam ser considerados os necessários e adequados para o exercício das atribuições do ICN. A CNPD considerou que a tarefa de concordância prática entre direitos fundamentais não podia conduzir, no caso concreto, a soluções extremadas que implicassem a efectiva aniquilação do direito fundamental à reserva da intimidade da vida privada. Porém, considerou-se que, num espaço protegido, devia ser avaliado o perigo da destruição irremediável de um património natural especialmente valioso. Assim, a CNPD considerou que podiam ser implantados sistemas de vigilância em patrimónios naturais, ainda que dessa actividade pudesse resultar uma limitação da privacidade de moradores e visitantes.

2.d.6. – A Comissão Nacional de Protecção de Dados autorizou o tratamento notificado sem deixar de sublinhar a necessidade de estar garantido que:

- Não se procedesse a qualquer captação de imagens nas áreas urbanas ou de habitações, devendo estas encontrar-se cobertas por *blank zones*;

⁽²⁵⁾ Admitindo que possa existir uma desconformidade do n.º 2 do artigo 7.º da Lei n.º 67/98, de 26 de Outubro com o n.º 3 do artigo 35.º da Constituição, a CNPD já suscitou ao Provedor de Justiça que suscitasse a fiscalização sucessiva abstracta da inconstitucionalidade da norma. Em decisão aprovada por maioria, a CNPD já decidiu, no Processo n.º 2218/02, que não dispõe de competência para não aplicar normas legais com fundamento na sua inconstitucionalidade.

- Através das gravações e da visualização não se permitisse a identificação das pessoas objecto de visionamento, nem das matrículas dos veículos também observados;
- No prazo de 60 dias fosse implantada a *funcionalidade* que permitisse que as gravações fossem conservadas durante um período de 30 dias, de forma a garantir uma actividade fiscalizadora eficaz desta Comissão.

e) *Videovigilância nas creches*

2.e.1. – Uma empresa proprietária de uma creche e jardim de infância notificou a CNPD de um tratamento de dados pessoais mediante captação de imagens, sem gravação, com 5 ou 6 câmaras fixas, nas salas de actividades e nos refeitórios onde se encontram crianças até aos 5 anos de idade, com a finalidade de permitir à Direcção e aos pais das crianças supervisionar as actividades das ditas crianças.

2.e.2. – O fundamento de legitimidade do tratamento, declara a responsável, reside no consentimento dos titulares – dos representantes legais das crianças – conjugado com a inexistência de risco de intromissão na vida privada ou de discriminação.

Apenas a Direcção da empresa responsável e os pais e representantes legais das crianças, mediante “*password*” própria, podem aceder às imagens.

2.e.3. – Justifica a empresa, ainda, que o tratamento permite aos pais e representantes legais saber exactamente como os seus filhos estão a ser cuidados e avaliar a qualidade dos serviços, sendo que o tratamento só iniciaria com o consentimento de todos os pais e representantes legais.

2.e.4. – O tratamento pretendido incide sobre a vida privada das pessoas, logo, só poderia inserir-se nos casos previstos nos n.º 2 a 4 do artigo 7.º da LPD.

É notório que não tem, o presente tratamento, cabimento nos n.º 2 e 3 do artigo 7.º. Importa, pois, aferir da aplicabilidade do número 2 do mesmo artigo.

2.e.5. – Em primeiro lugar, o tratamento de captação de imagens sem gravação, com acesso pela Direcção da empresa e pelos pais e representantes legais das crian-

ças, abrangeria sempre, inevitavelmente, os trabalhadores da creche e do jardim de infância. Essa eventualidade ofenderia o n.º 1 do artigo 20.º do Código do Trabalho que proíbe a vigilância à distância nos locais de trabalho. Ainda que essa vigilância dos trabalhadores não seja a finalidade directa do tratamento, a sua utilização para esse fim é inelutável. Mas, também, o possível consentimento dos trabalhadores para a captação e visualização das imagens, ainda que informado, não seria um consentimento passível de ser considerado inteiramente livre, dada a posição de dependência do trabalhador na relação laboral. Aliás, existe mesmo o entendimento, não contestado, de que a proibição legal de vigilância à distância, como forma de salvaguardar a intimidade e a imagem do trabalhador, sobre-põe-se sobre as manifestações de assentimento do próprio trabalhador que derrogassem essa proibição.

Por fim, o acesso de terceiros em face da relação laboral – pais e representantes legais das crianças – às imagens dos trabalhadores, acesso incontornável também, não encontraria suporte legal.

2.e.6. – Por outro lado, o controlo das crianças mediante a captação de imagens afigurou-se à CNPD excessivo e desproporcional, não pertinente mesmo tendo em vista a confiança na acção pedagógica e acompanhamento que os pais e representantes legais depositam na empresa quando nela colocam as crianças.

2.e.7. – O facto de as imagens serem divulgadas pela empresa através da Internet, às quais os pais e representantes legais acedem por *password*, comporta sempre o risco de intrusão por terceiros não autorizados a aceder.

2.e.7. – O tratamento pretendido de captação e visualização (sem gravação) das imagens das crianças da creche e jardim de infância significa um constrangimento injustificado do direito à intimidade das crianças. O direito à intimidade não deve sofrer qualquer restrição, como também não conhece qualquer dilatação, em função da idade. Quer a Constituição, quer o Pacto Internacional de Direitos Civis e Políticos, quer ainda a Convenção Europeia dos Direitos Humanos e, ainda, a Convenção sobre os Direitos das Crianças da ONU.

2.e.8. – Pelas razões expostas, a CNPD negou a autorização ao tratamento pretendido de captação sem gravação das imagens das crianças da creche e jardim de infância e o seu acesso pela Direcção da responsável e pelos pais e representantes legais.

f) *Tratamento do dado pessoal “imagem”*

2.f.1. – Foram publicitadas na Internet cópias de cheques emitidos por uma empresa, com indicação do nome do subscritor, incluindo uma fotografia sua, num sítio electrónico.

Efectivamente, na página da Internet referida existia uma página intitulada de *“pessoas e empresas de cobranças difícil”*, na qual estava acessível uma fotografia associada à pessoa queixosa bem como um conjunto de cheques sem cobertura que alegadamente o queixoso terá passado ao responsável pela página da Internet.

2.f.2. – A divulgação da imagem é um tratamento de dados pessoais nos termos do artigo 4.º, n.º 4, da Lei n.º 67/98. Além do mais, porque se encontra associada à passagem de cheques sem cobertura, passa a consubstanciar um tratamento de dados pessoais relativos à solvabilidade, sujeitos a controlo prévio pela CNPD. (Cfr. artigo 3.º, n.º 1 alínea b) e artigo 28.º).

Acresce que com tal divulgação pretendeu o responsável que fosse formado no meio comercial um juízo de valor negativo quanto à capacidade patrimonial do titular queixoso em pagar as suas dívidas.

2.f.3. – Não estando em causa a veracidade dos factos subjacentes a este tratamento, a verdade é que foi violado o “direito à imagem” do titular, consagrado no artigo 26.º da CRP e artigo 79.º do Código Civil (C.C.), uma vez que da divulgação da sua fotografia via Internet resultou prejuízo para a honra e reputação da sua pessoa.

De igual modo, foi atingido o direito ao “bom nome”, também consagrado no artigo 26.º da CRP, e no artigo 72.º do CC, na medida em que o uso foi ilícito, ao divulgá-lo via Internet e associando-o à passagem de cheques sem cobertura.

Com efeito, a imagem do titular na Internet foi obtida num outro contexto e com uma outra finalidade, sem que para tal tivesse obtido o seu consentimento para a divulgação com os propósitos descritos.

2.f.4. – Tal conduta é punível com contra-ordenação, nos termos da lei.

3 – DADO PESSOAL “RAÇA”

3.1 – Foi a CNPD notificada de um tratamento pretendido efectuar no âmbito do exercício da actividade de organização e manutenção actualizada da informação necessária à promoção e dádiva de sangue, bem como de coordenação da acção dos serviços integrantes da rede nacional de transfusão de sangue. A finalidade do tratamento prendia-se, pois, com a necessidade de recolher e manter actualizada a informação relativa aos dadores de sangue, às actividades de promoção e dádiva de sangue e ao reforço da segurança transfusional.

3.2 – Os dados pessoais abarcados pelo tratamento requerido eram: o nome de cada dador, o seu estado civil; a nacionalidade; o sexo; a data de nascimento; a profissão; a residência; o cartão nacional de dador de sangue; o número de dador de sangue; **a “raça”**; *os dados relativos ao seu estado de saúde* e dados de natureza laboratorial.

3.3 – Resulta dos autos que um dos dados pessoais que pretendido recolher e tratar é o da “raça”, bem como os dados relativos ao estado de saúde do respectivo dador. Indagado sobre a necessidade da recolha do elemento “raça”, o **responsável pelo tratamento** referiu, a este propósito, que:

“É necessário o tratamento da raça/etnia de forma nominativa, justificando se tal procedimento pelo facto de que “só se encontra sangue compatível para os doentes de determinado grupo étnico em indivíduos desse mesmo grupo”.

Sabe-se que “dos estudos realizados por investigadores estrangeiros, que há níveis de anticorpos do sistema ABO em diferentes populações e que os mesmos variam consoante a população seja de raça branca ou negra”.

Assim, por exemplo, “os níveis de anti A e anti B são geralmente mais altos nos indivíduos de raça negra do que nos de raça branca”. E os próprios sistemas de coagulação e hemorragia sanguíneas variam de acordo com os grupos a que pertencem.

Daí que o requerente e responsável pelo tratamento conclua afirmando, de forma categórica, que é necessário efectuar o tratamento da raça/etnia, sendo o conhecimento da raça dos dadores de sangue de extrema importância.

3.4 – O tratamento da raça ou etnia só pode ser feito se a CNPD autorizar o tratamento desta informação ou se, *in casu*, se verificar qualquer das restantes condições legais exigidas pelo n.º 2 do art.º 7.º da Lei n.º 67/98.

Assim sendo, e tendo em atenção a finalidade específica e fundamentada para o tratamento destes dados – que se prende com razões de interesse público – e apesar dos mesmos serem qualificados como sensíveis, por força dos normativos ínsitos na Lei de Protecção de Dados (cf. art. 7.º, n.º 1, da Lei n.º 67/98, de 26 de Outubro), **entendeu a CNPD que desde que o tratamento dos dados se faça de forma anónima, isto é, sem estabelecer a identificação nominativa entre o sangue obtido e o seu dador, nada obsta a que seja autorizado.**

Porém, no caso de o requerente e responsável se ver confrontado, ao pretender desenvolver a sua actividade, bem como para efectuar investigação científica, com a impossibilidade de anonimizar os dados recolhidos, ou então verificar que carece da referência nominativa dos titulares dos dados, impôs-lhe a CNPD a obrigação de, nesse caso, recolher previamente o consentimento expresso dos titulares desses dados, tendo em atenção essa finalidade específica.

Situação em que o consentimento funcionaria como factor legitimante da recolha desse elemento, nos termos do n.º 2 do art.º 7.º da Lei n.º 67/98.

Nesta circunstância, o Requerente devia diligenciar no sentido de tal consentimento ser prestado de forma inequívoca.

4 – DADO PESSOAL “FILIAÇÃO SINDICAL”

4.1 – Uma empresa decidiu elaborar um “estudo e pré-análise de perfis profissionais” no âmbito da “avaliação dos seus trabalhadores”, através da adjudicação dos serviços a uma outra empresa, com a qual contratou para esse fim.

No contrato assinado entre as duas entidades não existiam cláusulas sobre protecção de dados pessoais, apenas sobre confidencialidade.

4.2 – Durante uma acção inspectiva levada a cabo pela CNPD verificou-se que os procedimentos da empresa contratada incluíam o tratamento do dado pessoal “filiação sindical” referente aos trabalhadores.

Só é permitido o tratamento do dado pessoal “filiação sindical” nas condições seguintes (Lei n.º 81/2001 de 28 de Julho):

- a) A entidade empregadora utilize o dado pessoal “filiação sindical” exclusivamente no processamento do sistema de cobrança e entrega de quotas sindicais;
- b) A entidade empregadora obtenha autorização expressa (ou o trabalhador tenha expressamente pedido) para essa cobrança e entrega de quotas.

4.3 – A empresa adjudicante procedeu ao tratamento do dado pessoal “filiação sindical” através da comunicação desse dado à empresa contratada (artigo 3.º alínea b) da LPD), sem ter dado informação dos trabalhadores titulares desse dado pessoal nem obtido o consentimento prévio (artigo 3.º alínea h) e artigo 7.º n.º 2 da LPD). O consentimento dos titulares, bem como o dever de os informar e de obter os consentimentos prévios respectivos, são exigidos porque, sendo legítimo à empresa responsável pelo tratamento – aqui, a adjudicante – proceder ao tratamento do dado pessoal “filiação sindical” para a finalidade de cobrança e entrega de quotas, tendo para esse efeito obtido o consentimento/pedido expresso dos titulares, já o tratamento desse dado para a finalidade de “estudo e pré-análise de perfis profissionais” no âmbito da “avaliação dos seus trabalhadores” configura um evidente desvio face àquela finalidade. Aliás, o dado pessoal “filiação sindical” revela-se excessivo, desproporcionado e não necessário ao “estudo e pré-análise de perfis profissionais” no âmbito da “avaliação dos seus trabalhadores, pelo que não deve ser realizado o seu tratamento, seja através de comunicação (artigo 5.º n.º 1 alínea c) da LPD).

4.4. – Também a empresa contratada, aqui referida como adjudicatária, tratou o dado pessoal “filiação sindical” sem que a empresa adjudicante tenha solicitado esse tratamento ou tenha sequer fixado qualquer instrução para esse tratamento (v. artigo 14.º n.º 3 e artigo 16.º da LPD). Daí que o tratamento efectuado pela empresa contratada configura um tratamento de dados pessoais com autonomia e independência, sob sua exclusiva responsabilidade.

A empresa adjudicatária obteve o dado pessoal “filiação sindical” e desenvolveu os procedimentos do seu tratamento sem consentimento dos titulares e em frontal violação pelo artigo 7.º n.º 2 da LPD.

4.5. – Por esses motivos, ambas as empresas foram sancionadas com coimas em processo de contra-ordenação.

II – TRATAMENTO DE DADOS PESSOAIS RELATIVOS A ÓRGÃOS DE POLÍCIA CRIMINAL E A PREVENÇÃO, INVESTIGAÇÃO E REPRESSÃO CRIMINAL (V. Fluxos transfronteiriços de dados pessoais)

III – DADOS RELATIVOS À SITUAÇÃO FINANCEIRA, AO CRÉDITO E À SOLVABILIDADE

1 – TITULARIZAÇÃO DE CRÉDITOS

1.1 – Foram colocadas à consideração da CNPD algumas questões relativas à operação de titularização de créditos.

A questão fundamental que se coloca no âmbito da comunicação de dados no contexto de um contrato de “titularização de créditos” prende-se, no entender da CNPD, com o direito de informação que a Lei 67/98, de 26 de Outubro impõe a todos os responsáveis do tratamento. O “direito de oposição” só se coloca num momento subsequente, isto é, depois de os titulares dos dados terem conhecimento sobre as entidades a quem são comunicados os dados. O “direito de oposição” está subjacente a qualquer tratamento, mas não significa que o titular dos dados tenha sempre legitimidade para exercer o direito de oposição.

1.2 – Em termos de protecção de dados, há duas questões fundamentais que merecem especial referência num contrato de titularização de créditos:

- a) As condições de legitimidade;
- b) O direito de informação.

1.3 – Em relação às condições de legitimidade – na vertente do tratamento por comunicação – entendeu a CNPD que a comunicação de dados possa ser fundamentada em vários pressupostos. O que é necessário é que o responsável verifique, no momento do contrato (ou mesmo posteriormente), se pode comunicar os dados a uma entidade terceira. O responsável pode:

- a) Obter um **consentimento expresso** para a comunicação de dados. Não se torna necessário que haja uma autorização expressa sobre transmissão de dados no âmbito de operações de titularização, bastando que *se admita essa possibilidade* (vg. autoriza-se a comunicação de dados a terceiros, nomeadamente para a celebração de contratos de seguros de créditos ou operações de titularização);
- b) Através da inclusão no contrato de **cláusula contratual**, similar à que consta do número anterior, que *admita* tal possibilidade de comunicação de dados.

1.4 – Porém, se não houver qualquer consentimento ou cláusula expressa sempre se poderá entender que a operação de titularização de créditos é legítima, na confrontação do DL 453/99, de 5 de Novembro, com o regime do Código Civil relativo à cedência de créditos, entendendo-se que a cedência de dados corresponde à “prosecução de interesses legítimos do responsável pelo tratamento ou de terceiros a quem os dados são comunicados”. Neste caso deve entender-se que os direitos, liberdades e garantias do titular dos dados” (cf. parte final da alínea e) da Lei 67/98) não prevalecem sobre aquele interesse legítimo.

1.5 – No entanto, quando o tratamento se fundamenta no “interesse legítimo do responsável ou de terceiros”, o grande problema que se coloca é o de saber como é assegurado o **direito de informação**, princípio básico subjacente a qualquer tratamento de dados. Esta informação pode ser assegurada em dois momentos, em função da forma como os dados são recolhidos: directamente junto do titular (recolha directa – n.º 1 do artigo 10.º) ou recolhidos junto de terceiros (recolha indirecta – n.º 3 do artigo 10.º).

Embora a lei da titularização de créditos nada tenha dito em relação ao “direito de informação” – e sendo posterior à Lei 67/98 – não se pode concluir, de forma alguma, que os responsáveis estejam dispensados de assegurar o direito de informação. O artigo 10.º n.º 5 impõe que seja a lei ou a CNPD, em circunstâncias concretas e

quando se verifiquem certos requisitos, a dispensar a obrigação de informação. Logo, a omissão do DL 453/99 em relação ao direito de informação não implica a sua dispensa, mas a obrigatoriedade de respeitar as obrigações estabelecidas no artigo 10.º n.º 1 a 4 da Lei 67/98.

1.6 – Já quanto ao ***direito de oposição*** o problema é mais abrangente. Saber se deve ser reconhecido o “direito de oposição” é um problema que – como se infere da formulação legal (artigo 12.º alínea a) da Lei 67/98) – a sua apreciação em relação ao exercício desse direito terá de ser feita caso a caso e numa ponderação dos interesses em presença: os do responsável e os do titular dos dados. Por força do regime traçado pelo DL 453/99 e pelo artigo 577.º do Código Civil, é claramente defensável que, *em geral*, existem obstáculos legais em relação ao exercício do “direito de oposição”. Isto é, o regime da titularização de créditos aponta, em termos gerais, no sentido de que os interesses do titular dos dados podem ter que ceder perante os interesses do responsável.

Concluindo, mantém-se a necessidade de assegurar o “direito de informação”, como resulta do artigo 10.º da Lei 67/98, de 26 de Outubro, não havendo qualquer fundamento para a sua dispensa e, em relação ao “direito de oposição – quando for invocado – deverão os seus pressupostos ser apreciados caso a caso, tendo em atenção o disposto no DL 453/99 e artigo 577.º do Código Civil.

2 – COBRANÇA DE DÍVIDAS

Foi pedida autorização para tratamento de dados pessoais relativos ao crédito e solvabilidade, concretamente para efeitos de cumprimento de obrigações contratuais relativas ao serviço de cobrança de dívidas.

Na decisão da CNPD, foram analisados alguns princípios básicos da protecção de dados pessoais, constantes quer da Lei de Protecção de Dados, quer da Constituição da República Portuguesa (CRP), princípios esses que se mostraram atinentes à pretensão de tratamento em causa.

Em primeiro lugar, entendeu a CNPD que o facto de o profissional de cobranças se apresentar junto do titular da dívida que pretendia cobrar munido de agenda, caderno, carro e uniforme, todos distintivos da empresa massivamente divulgados, bem como

as práticas inquisitórias e persecutórias para apuramento da situação económica e financeira do devedor, violam o direito ao bom nome e reputação consagrados no artigo 26.º n.º 1 da CRP.

Em segundo lugar, o tratamento por parte da requerente, empresa de cobrança, deve ser considerado legítimo, independentemente do consentimento do titular (devedor), se o tratamento visar a prossecução de interesses de terceiros (credor) aos quais os direitos do titular não devem prevalecer. Importa, no caso, portanto, aferir da origem e prevalência do crédito, pois pode acontecer, caso esse crédito não deva prevalecer sobre os direitos fundamentais do titular, que integrem as práticas do responsável comportamentos sancionáveis contra-ordenacional e criminalmente.

Em terceiro lugar, a CNPD considerou que alguns dados pessoais – altura, peso, idade, complexão, familiares solventes – são excessivos face à finalidade prosseguida de cobrança de dívidas. Também alguns tratamentos – recolha de dados sobre os “implícados na dívida”, recolha de dados através de vizinhos e porteiros ou através de sujeitos de relações comerciais e financeiras – têm por objecto dados pessoais excessivos face à finalidade do tratamento sob autorização.

Por fim, pretende a responsável pelo tratamento proceder a tratamento de dados tendente a demonstrar e sustentar a existência da dívida que pretende cobrar. Ora, entendeu a CNPD que essa era uma finalidade dos tribunais, que a requerente não pode prosseguir em termos que fundamentem o tratamento de dados pessoais requerido.

IV – ACESSO A DADOS PESSOAIS CONSTANTES DE REGISTOS PÚBLICOS E INTERCONEXÃO DE DADOS PESSOAIS

1 – ACESSO A DADOS PESSOAIS CONSTANTES DE REGISTOS PÚBLICOS

a) Acesso às Bases de Dados dos Registos, Direcção Geral dos Impostos (DGCI) e Segurança Social

1.a.1. – Foi pedido à CNPD que se pronunciasse sobre a possibilidade de, no âmbito dos processos pendentes num Centro de Arbitragem, este poder aceder aos dados existentes nas bases de dados dos serviços de identificação civil, da

segurança social, da Direcção-Geral dos Impostos e da Direcção-Geral de Viação com vista à localização do citando.

Foi o pedido fundamentado na aplicação aos tribunais arbitrais do regime previsto no artigo 244.º n.º 1 do Código de Processo Civil.

1.a.2. – Estava-se perante o acesso directo (acesso em tempo real) a dados pessoais. Nesta matéria interessou, desde logo, considerar que o artigo 35.º n.º 4 da Constituição da República estabelece que “*é proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei*”. Em face da definição de “terceiro” constante do artigo 3.º alínea f) da Lei 67/98, de 26 de Outubro, o Centro da Arbitragem era, necessariamente, um terceiro na medida em que não é responsável.

Conforme decorria do acórdão do STJ de 18 de Maio de 1999, “a arbitragem voluntária é contratual na sua origem, privada na sua natureza, e, porque o Estado quebrou o monopólio do exercício da função jurisdicional por reconhecer a sua utilidade pública, jurisdicional na sua função e pública no seu resultado”. Em face das características dos tribunais arbitrais não parece que seja admissível aceitar a aplicação subsidiária dos artigos 238.º e 244.º do Código de Processo Civil.

Efectivamente, a previsão constante dos preceitos citados do CPC – que levantou algumas objecções à CNPD – só pode ser considerada como previsão legal de acesso (cf. artigo 35.º n.º 4 da CRP) em matéria de processo judicial. Será excessivo e desproporcionado, em face da natureza do processo do tribunal arbitral, admitir o acesso directo às bases de dados referidas.

Deliberou a CNPD pronunciar-se no sentido de que não será admissível – por aplicação dos artigos 238.º e 244 do CPC – o acesso directo às bases de dados de Identificação civil, da segurança social, da DG dos Impostos e da DGV por parte dos tribunais arbitrais.

b) Colaboração dos Registos Públicos, DGCI e Segurança Social

1.b.1. – Diferente foi o caso de os Registos Públicos, DGCI e Segurança Social prestarem a colaboração a um Centro de Arbitragem,, fornecendo-lhe os elementos das moradas das pessoas demandadas.

1.b.2. – Os tribunais arbitrais estão previstos na CRP (artigo 209.º n.º 2) e asseguram o acesso ao direito e a tutela jurisdicional efectiva.

1.b.3. – O fornecimento dos dados pelos Registos Públicos, DGCI e Segurança Social a um Centro de Arbitragem é feito na prossecução de um interesse legítimo deste Centro, interesse esse que é relevante e digno de protecção, não prevalecendo sobre eles os direitos, liberdades e garantias dos titulares, pelo que o desvio da finalidade do tratamento daqueles Registos, DGCI e Segurança Social não obsta a esse comunicação, sendo ela permitida.

c) Acesso dos Advogados aos Dados da Segurança Social

1.c.1. – Um advogado solicitou à Segurança Social informação sobre os descontos de um cidadão efectuados pela entidade patronal, para efeitos de requerer a penhora sobre o vencimento deste beneficiário. A CNPD foi chamada a pronunciar-se sobre esse acesso.

1.c.2. – Entendeu a CNPD que, se por um lado, o artigo 268.º n.º 2 da CRP permite a todos os cidadãos o acesso aos arquivos e registos administrativos, por outro, no artigo 18.º n.º 2 impõe que a lei só pode restringir os direitos, liberdades e garantias dos cidadãos nos casos expressamente previstos na Constituição, devendo essas restrições limitar-se ao necessário para a salvaguarda de interesses e direitos constitucionalmente protegidos.

1.c.3. – O artigo 76.º da Lei de Bases da Segurança Social dispõe sobre a confidencialidade da informação sobre os cidadãos e o direito destes de não verem a informações que lhes respeitam indevidamente divulgadas.

1.c.4. – O requerente dispõe da faculdade da lei processual civil para satisfazer a sua pretensão de nomear bens à penhora, pelo que a CNPD refutou o pretense acesso aos dados da segurança social.

2 – INTERCONEXÃO DE DADOS PESSOAIS

2.1 – O Instituto de Solidariedade e Segurança Social (ISSS) requereu à CNPD a admissibilidade da troca recíproca de informações entre o próprio ISSS, os Centros de Emprego, o Instituto de Emprego e Formação Profissional (IEFP) e o Instituto de Informática e Estatística de Solidariedade (IIES), todos do Ministério da Solidariedade e Segurança Social.

2.2 – Alegou, como finalidade dessa interconexão, a optimização do controle e combate na atribuição do Rendimento Social de Inserção (RSI). Para mais, alegou ainda, a atribuição do RSI requer a informação actual e rigorosa sobre os beneficiários.

2.3 – Muita informação sobre as condições e requisitos de atribuição do RSI – bem como da atribuição do subsídio de desemprego – encontra-se depositada nos Institutos que visam trocar, reciprocamente, a informação. A legislação em vigor implica já a obrigação de comunicação recíproca das informações.

2.4 – Atenta a finalidade, mostrou-se à CNPD que a interconexão dos dados entre os organismos enunciados era pertinente, adequada e legítima, pelo que foi autorizada.

V – IDRF, TELECOMUNICAÇÕES E COMÉRCIO ELECTRÓNICO

a) IDRF

A CNPD emitiu uma deliberação sobre Identificação por RadioFrequência (IDRF), considerando que está perante um sistema automático de identificação que possibilita a transmissão de dados recorrendo a marcas/identificadores (*tags*) portáteis para leitores com a capacidade de processar tais dados.

As marcas, considerou ainda a CNPD, são *microchips*, de dimensões muito reduzidas, por vezes microscópicas, que se encontram conectados a uma antena e que possuem a capacidade de transmitir informação de identificação – tipicamente, um código único universal. Os sinais enviados/recebidos pelas marcas de radiofrequência (RF) são, assim, univocamente identificáveis.

Verificou a CNPD que os dados transmitidos pelas marcas de radiofrequência (RF) podem incluir informação sobre a identificação ou a localização, bem como outra relativa às características (propriedades) do produto etiquetado. A transmissão da informação pode ser iniciada/interrompida remotamente sem que o portador da marca disso se aperceba.

A CNPD não questiona as vantagens da utilização desta tecnologia, bastante útil para finalidades bem definidas. Mas sendo possível associar esse código identificador único a informação pessoal, a IDRF potencia, na óptica desta Comissão, os eventuais perigos da sua utilização de forma ilegítima. Por outro lado, a possibilidade de leitura e activação remotas das marcas RF, sem conhecimento prévio das pessoas que as possuem, inviabilizando, assim, quaisquer oportunidades de o titular dos dados influenciar e/ou controlar o processo coloca, na perspectiva da protecção de dados, preocupações adicionais.

Perante a massificação da tecnologia de IDRF sem que os cidadãos estejam alertados para os riscos que tal acarreta para a sua privacidade, torna-se necessário, para a CNPD, que os fabricantes dos produtos RF estejam sensibilizados para a necessidade de encontrar soluções tecnológicas que compatibilizem os interesses económicos com os direitos dos cidadãos. De igual modo, os responsáveis pelos tratamentos deverão ter consciência das suas obrigações legais nesta matéria.

Em conclusão, a CNPD considera que sempre que o recurso à tecnologia de IDRF implica a interconexão com informação de carácter pessoal se está em presença de um tratamento de dados pessoais (nos termos da alínea b) do artigo 3.º da Lei 67/98 de 26 de Outubro) e delibera que as normas de protecção de dados devem ser pontualmente cumpridas.

b) Telecomunicações e Comércio Electrónico

Por uma queixa apresentada em virtude de correspondência de marketing não solicitada, via telecópia, verificou-se que os faxes foram endereçados a uma sociedade comercial. Com a entrada em vigor do Decreto-Lei n.º 7/2004, de 7 de Janeiro, foi alterado o regime vigente em matéria de “comunicações não solicitadas”. Contrariamente ao que acontecia com o artigo 12.º da Lei 69/98, de 28 de Outubro (que não fazia distinção de regimes entre pessoas singulares e sociedades e obrigava ao “consentimento prévio do assinante chamado”), o artigo 22.º n.º 2

estabelece agora que – **para as pessoas colectivas** – as mensagens publicitárias por fax devem deixar de ser enviadas quando a empresa (destinatária) recorra ao “sistema de opção negativa”.

Isto é, em relação ao envio de faxes a pessoas colectivas não é exigível o consentimento prévio, devendo estas exercer o direito de oposição quando não pretendam receber acções/mensagens de marketing directo através dos meios referidos no artigo 22.º n.º 1 do DL 7/2004.

Em face do exposto, a CNPD deliberou arquivar as queixas uma vez que os factos participados ocorreram na vigência do DL 7/2004, de 7 de Janeiro.

VI – FLUXOS TRANSFRONTEIRIÇOS DE DADOS PESSOAIS

1 – COMUNICAÇÃO DE DADOS PESSOAIS DE ADEPTOS DE FUTEBOL PELA PSP

1.1 – A PSP pretendeu introduzir os dados relativos a adeptos do futebol, nomeadamente para responder às exigências de segurança do Euro 2004. Considera a PSP que, de acordo com o artigo 8.º n.º 2 e 3 da Lei 67/98, de 26 de Outubro, tem legitimidade para introduzir estes dados no seu sistema de informação.

A Decisão 2002/348/JHA do Conselho, de 25 de Abril de 2002 (JO L 121 de 8 de Maio de 2002, p. 1), estabeleceu disposições sobre a segurança por ocasião de jogos de futebol com dimensão internacional. A decisão n.º 2003/C 24/05 (JO de 31/1/2003 – C) fixou quais os “pontos de informação sobre o futebol dos Estados da União Europeia”.

Em Portugal tal tarefa ficou a cargo da Direcção Nacional da Polícia de Segurança Pública.

1.2 – Nos termos do Decreto Regulamentar n.º 5/95, de 31 de Janeiro, a PSP dispõe de uma base de dados que tem por finalidade organizar e manter actualizada a informação necessária ao exercício das missões da PSP que a respectiva Lei Orgânica lhe comete (cf. artigo 1.º n.º 2).

O tratamento da informação e a prevenção de infracções ligadas ao desporto apresenta-se como necessária ao exercício das missões da PSP, verificando-se que estão

reunidas as condições estabelecidas pelo artigo 8.º n.º 2 da Lei 67/98, pelo que a CNPD autorizou o tratamento dos dados por parte da PSP, enquanto “ponto nacional de informações sobre futebol”, nos termos do artigo 8.º n.º 2 e 3 da Lei 67/98.

2 – TRANSMISSÃO TRANSFRONTEIRIÇA DE DADOS PESSOAIS DURANTE O EURO 2004

A Sociedade Euro 2004 veio solicitar a tomada de posição da CNPD acerca de três questões relativas a transmissão ou comunicação de dados pessoais integrados em tratamentos relacionados com o evento que lhe cabe organizar.

Tratou-se da transmissão de dados às forças de segurança, às federações nacionais de futebol dos países participantes no Euro 2004 e ao Serviço de Estrangeiros e Fronteiras.

Foi autorizado o acesso, com respeito das regras de segurança estabelecidas nos artigos 14.º e 15.º da Lei n.º 67/98, dos órgãos de polícia criminal, através do Grupo de Validação, aos dados a que esta se refere, às seguintes entidades policiais, e para as finalidades indicadas:

- Polícia Judiciária (criminalidade da sua competência exclusiva);
- SIS (ameaça terrorista; actos violentos de extremismo; criminalidade organizada);
- Serviço de Estrangeiros e Fronteiras (legalidade da permanência em território nacional; medidas cautelares; criminalidade organizada);
- Polícia de Segurança Pública (criminalidade da sua competência; protecção de altas individualidades).

Foi autorizada a comunicação, com respeito das regras de segurança adequadas, ao Serviço de Estrangeiros e Fronteiras, para efeito de concessão de vistos, de dados de pessoas que irão exercer funções oficiais no Euro 2004.

Com dispensa, ao abrigo do artigo 10.º, n.º 5 da Lei n.º 67/98, da informação dos titulares dos dados sobre essa transferência, foi autorizada, com base no artigo 20.º, n.º 1, alínea a) da Lei n.º 67/98, a transferência, para as Federações de futebol dos países participantes na fase final do Euro 2004, de dados das pessoas nestes residentes às quais foram atribuídos bilhetes na primeira fase de vendas.

3 – CLÁUSULAS CONTRATUAIS GERAIS E FLUXOS TRANSFRONTEIRIÇOS DE DADOS PESSOAIS

3.1 – Foi requerido um tratamento de dados pessoais no qual se pretendia proceder ao envio (fluxo) de dados pessoais para os EUA, no âmbito de um contrato de gestão de ficheiros, cujo conteúdo era, no que ao fluxo de dados pessoais respeita, muito semelhante às cláusulas contratuais estabelecidas na Decisão da Comissão n.º 2002/16/CE, de 27/12/2001, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para sub-contratantes estabelecidos em países terceiros.

3.2 – Estas cláusulas contratuais-tipo ofereciam garantias adequadas à protecção da vida privada e dos dados pessoais dos cidadãos titulares.

3.3 – Com a adopção destas cláusulas contratuais-tipo (ou outras em tudo semelhantes), ficavam garantidos os procedimentos e resultados satisfatórios em matérias de protecção de dados pessoais, pelo que o fluxo pretendido foi autorizado.

VII – PROTECÇÃO DE DADOS PESSOAIS NO LOCAL DE TRABALHO

1 – PRIVACIDADE NO LOCAL DE TRABALHO: A UTILIZAÇÃO DA BIOMETRIA

A CNPD, sobre a utilização dos dados biométricos no local de trabalho, entendeu que:

1. As características biométricas não deixam de representar uma parte da individualidade das pessoas, estando ligadas intrinsecamente à própria pessoa;
2. A introdução do sistema na empresa deverá procurar obter o consenso dos trabalhadores e não ser imposto;
3. Os equipamentos biométricos devem registar, normalmente, uma representação digital (*template*) e não uma amostra biométrica passível de ser reproduzida, ou seja, o *template* armazenado não tem utilidade nenhuma noutros sistemas e não pode ser usado para reproduzir os dados biométricos originais;

4. O sistema biométrico que, através do processo de algoritmização, gerou o *template* que representa numericamente a característica biométrica captada, não deve permitir fazer a reversão e, por conseguinte, descodificar e reproduzir, de forma digitalizada, a imagem da característica biométrica (v.g. representação digitalizada da impressão digital, da íris, da geometria da mão ou da geometria facial);
5. O responsável do tratamento não deve dispor, por isso, de uma base de dados de características biométricas, mas de uma lista estruturada e numeralizada dessas características;
6. A centralização das características biométricas em bases de dados apresenta perigos acrescidos para a privacidade, razão pela qual não é admissível o seu relacionamento com outro tipo de tecnologias (v.g. videovigilância);
7. Esse relacionamento não prejudica a possibilidade de utilização de “sistemas multimodais”, caracterizados pelo recurso a mais de uma característica biométrica para conferir uma maior eficácia e rigor às operações de reconhecimento ou autenticação;
8. O *template*, que representa a característica biométrica do indivíduo, pode ser gravado ou memorizado no sistema central, em terminais ou num suporte que o seu titular traz consigo (v.g. um cartão, um equipamento ou um código de barras);
9. Um sistema biométrico que não é fiável cumpre de forma deficiente as finalidades que se propõe atingir, correndo o risco de tratar – especialmente em “sistemas de identificação” – informação desactualizada;
10. A existência de uma grande probabilidade de “falsos utilizadores” poderem ser aceites permite que – no contexto de uma empresa onde o sistema visa controlar o horário de trabalho – as apontadas deficiências no desempenho potenciem a troca de identificação de alguns trabalhadores (eventualmente com características semelhantes) e a consequente anotação de atrasos, faltas ou presenças de forma indevida;
11. A aquisição de sistemas biométricos deve passar pela adopção de soluções alternativas para suprir as suas insuficiências, especialmente as que resultam das taxas de falsas rejeições, aceitações ou impossibilidade temporária de o trabalhador apresentar o seu dado biométrico para autenticação ou reconhecimento;

12. O titular tem o direito de saber se a sua característica biométrica se encontra armazenada e obter a respectiva comprovação, nomeadamente através do desencadeamento da operação de reconhecimento ou de autenticação;
13. A operação de recolha das características biométricas com a finalidade de controlo do horário de trabalho não envolve uma violação da integridade física do trabalhador, do seu direito à privacidade ou da sua intimidade;
14. Independentemente da autorização da CNPD, o titular dos dados pode, em abstracto, por força do artigo 12.º alínea a) da Lei 67/98, opor-se ao tratamento sempre que haja “razões ponderosas e legítimas relacionadas com a sua situação particular” e que se apresentem com relevância para fazer prevalecer o seu direito sobre os interesses da entidade empregadora;
15. Os dados em si mesmo (impressão digital, geometria facial, íris ou retina) não se enquadram no conceito de “vida privada”, nem as finalidades prosseguidas permitem um enquadramento dessas categorias de dados na previsão do artigo 7.º n.º 1 da Lei 67/98;
16. As “condições de legitimidade” do tratamento só poderão ser enquadradas numa das previsões do artigo 6.º da Lei 67/98;
17. Será de afastar o consentimento como “condição de legitimidade”, em face da posição em que o trabalhador se encontra;
18. Será de afastar, igualmente, a aplicação da alínea b) do artigo 6.º na medida em que, perante a omissão do Código do Trabalho em relação à possibilidade de controlo por meio de sistemas biométricos, não é possível concluir – perante disposições da lei do trabalho tão genéricas sobre “registo de horas de trabalho prestadas pelo trabalhador” – que se tenha pretendido neles fundamentar qualquer forma de controlo deste tipo;
19. Se não for estabelecido contratualmente o tratamento de dados biométricos por razões inerentes e determinadas pela especial natureza do contrato (v.g. entrada em locais de “alta segurança”), a mera celebração do contrato não determina, só por si, uma legitimação para o tratamento destes dados;
20. A legitimidade para o tratamento de dados com a finalidade de controlo do horário de trabalho (assiduidade) só poderá ter como fonte a previsão do artigo 6.º alínea e) da Lei 67/98, uma vez que o tratamento é feito na “prosecução de interesses legítimos do responsável”;

21. O artigo 6.º alínea e) da Lei 67/98 obriga a CNPD, em cada caso concreto, a apurar se “não prevalecem os interesses ou os direitos liberdades e garantias dos titulares dos dados” sobre o interesse legítimo invocado pela entidade empregadora;
22. Este procedimento ajusta-se à aplicação do princípio da proporcionalidade e que, por isso, o tratamento deve deixar de ser feito quando se revele injustificado, por ser desajustado e excessivo, ou quando – pela sua falta de fiabilidade – comprometa a finalidade determinante do tratamento;
23. O princípio da proporcionalidade constitui, igualmente, o critério determinante das decisões relativas ao tratamento de dados biométricos tomadas pelas autoridades de protecção de dados;
24. A operação de captação de dados biométricos – que implica a cooperação/anuência do trabalhador através da “exposição” da respectiva parte do seu corpo (dedos, mão, olho ou rosto) para tratamento das características físicas ou morfológicas da sua identidade pessoal que se pretendem coligir para fins de identificação ou autenticação – não pode ser realizada com violação da sua identidade pessoal (art.26.º da CRP), com lesão da sua integridade física (art. 25.º n.º 1 da CRP) ou com intromissão na intimidade da vida privada (artigo 16.º do CT);
25. A simples operação de recolha, em exclusivo, para fins de controlo da assiduidade do trabalhador não afecta o direito à identidade pessoal e da intimidade da vida privada, garantidas constitucionalmente no artigo 26.º da CRP;
26. Em geral, a submissão à operação de recolha não se poderá traduzir numa discriminação ou violação do dever de respeito e dignidade do trabalhador, nem afectar o recato ou pudor que a sua condição supõe, tanto mais que a finalidade que está subjacente à captação destes dados não envolve, por princípio, qualquer discriminação ou desconfiança em relação ao trabalhador;
27. Não é o dado biométrico em si mesmo que pode afectar o direito à privacidade da pessoa, mas a finalidade com que é utilizado e os riscos que apresenta para a própria pessoa (risco de discriminação ou de cruzamento com outros sistemas, conseqüências produzidas em razão da sua falta de fiabilidade, efeitos na sua esfera pessoal no caso de falsificação ou usurpação da característica biométrica);

28. Se justifica alertar para a aplicação, com especial pertinência, do princípio contido no artigo 13.º da Lei 67/98 que proíbe a tomada de decisões com base, exclusivamente, em tratamento automatizado;
29. O princípio da proporcionalidade “impõe que qualquer tratamento de dados pessoais, atenta a sua finalidade concreta, deva ser avaliado em termos de idoneidade e de intervenção mínima”, o que envolve uma ponderação, casuística, entre a finalidade visada e o risco de utilização indevida dos dados para outras finalidades.

A CNPD deliberou que irá observar os seguintes princípios em relação à apreciação dos tratamentos de dados biométricos para controlo de assiduidade:

- I O tratamento de dados biométricos, porque estamos perante dados pessoais, deve respeitar todas as condições estabelecidas na Lei 67/98, nomeadamente, no requerimento de notificação serem indicadas, com detalhe, as características do sistema biométrico, as condições de tratamento e outras condições que permitam à CNPD apreciar o pedido em termos de necessidade e de proporcionalidade;
- II A preocupação primeira em relação à utilização de dados biométricos passa pela ponderação, no caso concreto, da idoneidade e da necessidade daquele meio e da conformidade dos motivos apresentados com o princípio da proporcionalidade;
- III A finalidade do tratamento insere-se no âmbito do exercício de poderes de controlo conferidos legalmente à entidade empregadora, correspondendo a uma “actividade legítima” do responsável;
- IV O controlo da assiduidade com recurso a dados biométricos apresenta-se como um meio adequado por corresponder a uma “finalidade legítima”, razão pela qual o controlo de assiduidade terá que ser enquadrada na previsão do artigo 6.º alínea e) da Lei 67/98;
- V A CNPD deverá verificar, numa ponderação dos interesses em presença e em cada caso concreto, se “não prevalecem os interesses ou os direitos liberdades

e garantias dos titulares dos dados” sobre o “interesse legítimo” invocado pela entidade empregadora;

- VI A recolha de dados biométricos – normalmente a impressão digital, geometria da mão ou da face, padrão da íris ou reconhecimento da retina – não tem qualquer implicação com a integridade física do trabalhador, não afectando, igualmente, o seu direito à identidade pessoal e à intimidade da vida privada, garantidos constitucionalmente no artigo 26.º da CRP;
- VII Em geral, a operação de recolha e comparação das características biométricas não constitui factor de discriminação ou violação do dever de respeito, nem afecta o recato ou pudor do trabalhador;
- VIII Se a inserção das características biométricas em cartão que o trabalhador traz consigo tem a vantagem de sossegar o trabalhador em relação ao não fornecimento da sua característica biométrica à entidade empregadora e de lhe permitir um controlo sobre a utilização dos seus dados biométricos, a verdade é que tem o inconveniente de exigir que o trabalhador tenha sempre o cartão consigo, obrigando o responsável a produzir novo cartão em caso de extravio ou mau estado de conservação;
- IX Não estando afastados riscos efectivos de falsificação ou “apropriação” das características biométricas, aspecto que tem consequências imprevisíveis para os titulares nomeadamente se caminharos para a utilização generalizada destes meios, a CNPD seguirá com atenção os novos desenvolvimentos tecnológicos;
- X A utilização de sistemas com deficiente grau de desempenho ou de performance (v.g. uma elevada taxa de falsas aceitações ou de falsas rejeições) podem comprometer a finalidade do tratamento – o controlo de entradas e saídas – e criar dificuldades acrescidas ao trabalhador, que se reflectem no exercício dos seus direitos, tal como estão delineados na Lei 67/98 e, em certa medida, no Código do Trabalho;
- XI Se houver este risco, deve entender-se que o sistema não reúne as condições legais para desempenhar as finalidades de controlo uma vez que, para além de a informação se encontrar desactualizada, é um factor de grande instabilidade e de falta de confiança no sistema, colocando aos trabalhadores grandes difi-

- culdades de prova em relação à comprovação da “falsa entrada” que lhes foi atribuída pelo sistema;
- XII Se isso acontecer, verifica-se que o tratamento das características físicas intrínsecas do trabalhador contribuem para violar os princípios da qualidade dos dados e, em particular, o princípio da actualização, subjacentes à previsão do artigo 5.º da Lei 67/98;
- XIII Este aspecto, que é uma “condição de licitude do tratamento”, condicionará o sentido da decisão da CNPD;
- XIV Por isso, impõe-se que a entidade empregadora não encare, sem qualquer flexibilidade, a introdução destes novos sistemas como instrumentos “infalíveis” em termos de reconhecimento, devendo abordar com realismo as situações em que o trabalhador questiona a sua eficácia;
- XV Na linha do que dispõe o artigo 17.º n.º 4 do Código do Trabalho, deve ser reconhecido ao trabalhador o “controlo sobre o tratamento dos seus dados pessoais” colocando ao seu alcance mecanismos para verificar – no momento da sua identificação/autenticação – se o sistema fez o seu reconhecimento (ou se fez um “falso reconhecimento”);
- XVI A utilização para finalidade não determinante da recolha carece, necessariamente, de autorização prévia da CNPD, nos termos dos artigos 23.º n.º 1 alínea c) e 28.º n.º 1 alínea d) da Lei 67/98;
- XVII Os dados pessoais recolhidos não podem ser comunicados a terceiros.
- XVIII Os dados biométricos serão obrigatoriamente eliminados no momento da transferência do trabalhador para outro local de trabalho ou no caso de cessação do contrato de trabalho;
- XIX Os trabalhadores e os seus representantes são convidados a estar atentos ao funcionamento do sistema e canalizar os elementos úteis à avaliação da CNPD.

2 – REALIZAÇÃO DE TESTES DE DESPISTAGEM DE DROGA E DE ÁLCOOL
NO SANGUE DOS TRABALHADORES

a) *Autorização dos testes*

2.a.1. – Foi notificado o tratamento de dados pessoais realizado no âmbito da Gestão da Informação dos Serviços de Segurança, Higiene e Saúde no Trabalho, no qual se procede ao tratamento, entre outros, de dados de saúde, de informação relativa ao consumo de álcool.

2.a.2. – Este tratamento é feito nos termos do disposto no DL 26/94, de 1 de Fevereiro, na redacção que lhe foi dada pelo DL 109/2000, de 30 de Junho. Ou seja, há legitimidade, em termos gerais, para serem tratadas aquelas categorias de dados na medida em que a gestão de informação visa assegurar o cumprimento de uma obrigação legal (cf. artigo 7.º n.º 2 da Lei 67/98). Para que a CNPD possa autorizar este tratamento é necessário, ainda, que sejam asseguradas “garantias de não discriminação” e adoptadas “medidas de segurança” adequadas.

2.a.3. – Em geral, os dados tratados são necessários, pertinentes e não excessivos em relação à finalidade (artigo 5.º n.º 1 alínea c) da Lei 67/98).

Em que condições pode ser tratada toxicodependência e a alcoolémia?

No que respeita ao *consumo de drogas e alcoolémia* tem entendido a CNPD, como regra geral, que não deve ser autorizado o tratamento automatizado, de forma generalizada (para todo o universo de trabalhadores da empresa) e com um detalhe que permita estabelecer as quantidades consumidas, o tipo de produto consumido e as circunstâncias em que se realiza o consumo.

O registo detalhado do consumo de álcool, ao ponto de permitir a elaboração de “perfis de consumo” constitui uma devassa injustificada nos hábitos do trabalhador. Admite-se que seja feita uma “mera anotação” do historial de consumo (uma referência genérica consome/não consome), na sequência de informação do trabalhador. É o que parece existir no caso presente.

Porém, *o direito à privacidade pode ser limitado* quando estes factos tenham repercussões negativas na relação de trabalho, haja razões de interesse público relevante ou a necessidade de controlo estiver em conflito com outros direitos

constitucionalmente consagrados. Ora, para algumas categorias profissionais – v.g. motoristas ou gruistas – admite-se que sejam tomadas medidas de vigilância e de registo automatizado de meios auxiliares de diagnóstico ou de testes para prevenir perigos para a sua integridade física ou para a de terceiros.

Por isso, a CNPD não autorizou o tratamento detalhado de eventuais exames (vg. regulares) sobre consumo de drogas ou álcool para a generalidade dos trabalhadores por se revelar excessivo e discriminatório.

2.a.4. – Importava assegurar um tratamento leal e de acordo com os princípios da boa-fé (cf. artigo 5.º n.º 1 alínea a) da Lei 67/98), dando-se particular atenção ao direito de informação (cf. artigo 10.º n.º 1) e, quando aplicável, ao direito de oposição (cf. artigo 12.º alínea a) da Lei 67/98). Em relação à segurança – e porque estão em causa dados de saúde – importa considerar as medidas de segurança previstas no artigo 15.º da Lei 67/98. Devem ser adoptadas medidas de segurança que impeçam o acesso à informação a pessoas não autorizadas.

As observações clínicas relativas a exames médicos são anotadas em ficha própria, podendo a informação servir de base ao preenchimento da “ficha de aptidão”, a qual, sendo remetida ao responsável pela área dos recursos, não pode conter elementos que envolvam segredo profissional (art. 21.º n.º 3 do DL 26/94).

VIII – OUTRAS DELIBERAÇÕES SOBRE PROTECÇÃO DE DADOS PESSOAIS

1 – DADOS PESSOAIS TRATADOS PELOS CONDOMÍNIOS

1.1 – Foi solicitada a intervenção da CNPD por a administração de um condomínio de um prédio estar a divulgar “publicamente alguns dos seus dados pessoais”. Efectivamente, no *hall* de entrada do prédio era afixada “uma listagem onde consta o nome completo, a morada e o estado de pagamento das quotas do condomínio”.

1.2 – Foi alegado pelo titular que nunca foi autorizado que os seus dados fossem publicados em local público, tendo solicitado a cessação de tal procedimento de afixação, no referido local.

1.3 – Quer haja a divulgação do nome ou, tão só, da fracção, estamos perante dados pessoais na medida em que – à luz do artigo 3.º alínea a) da Lei 67/98 – integra-se no conceito de dados pessoais “qualquer informação..relativa a pessoa identificada ou identificável”. Será “identificável” a pessoa que possa ser identificada. Ora, através da identificação da fracção é facilmente identificável o respectivo proprietário, ainda que tenha que se recorrer à informação constante do registo predial (a qual é facilmente acessível).

1.4 – Encontrando-se a informação estruturada numa listagem (cf. artigo 3.º alínea c) da Lei 67/98) e por aplicação das disposições precedentes, estamos perante um tratamento ao qual é aplicável a Lei 67/98.

Não há dúvida que a informação tratada é necessária, adequada e não excessiva à finalidade da administração e gestão da actividade do condomínio (cf. artigo 5.º n.º 1 alínea c) da Lei 67/98, de 26 de Outubro). A grande dúvida que se coloca é a de saber se é legítimo o tratamento – na vertente de “divulgação” ou “difusão” – das quotas dos condóminos.

1.5 – Deve salientar-se, em primeiro lugar, que a afixação de dados no hall de entrada não consubstancia uma difusão em “local privado”, no sentido de ser acessível apenas aos condóminos.

Em matéria de legitimidade o artigo 6.º da Lei 67/98 admitirá a difusão de dados, nomeadamente, quando houver consentimento dos titulares (corpo do preceito), quando tal difusão resultar de disposição legal (alínea b) ou quando essa difusão decorrer de “interesses legítimos do responsável pelo tratamento ou de terceiros a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados” (alínea e).

1.6 – Verifica-se que, já depois da queixa, a assembleia de condóminos se pronunciou sobre a possibilidade de divulgação de dados dos devedores de quotas – com indicação da fracção – sem que tal assunto constasse da ordem de trabalhos. Efectivamente, tal assunto foi tratado na rubrica “assuntos de interesse”. Será, por isso, de duvidosa legalidade e força vinculativa tal decisão.

1.7 – Mas, independentemente da utilização do mecanismo de impugnação de deliberações, será que a CNPD pode intervir em matéria de divulgação destes dados?

Em termos de “legitimidade do tratamento” as respectivas condições (aí se incluindo a difusão de dados) só podem, no caso concreto, decorrer de consentimento ou de disposição legal, já que não parece à CNPD que o interesse na divulgação se possa sobrepor aos direitos dos titulares dos dados (os devedores de quotas do condomínio).

1.8 – A CNPD entende que é violadora do direito à privacidade e do bom nome a decisão dos condóminos que, em violação dos princípios de protecção de dados, consideraram que os dados pessoais dos devedores de quotas devem ser afixados no hall do prédio⁽²⁶⁾. A recolha de dados por parte da administração não foi feita com esta finalidade e qualquer desvio da finalidade carece da autorização da CNPD (cf. artigo 23.º alínea c) da Lei 67/98). Neste contexto, o direito de oposição dos titulares dos dados é legítimo (cf. artigo 12.º alínea a) da Lei 67/98).

1.9 – Entendeu a CNPD que o condomínio deve, depois de assegurar o direito de informação dos titulares dos dados (cf. artigo 10.º da Lei 67/98), omitir da listagem as fracções que exercerem o direito de oposição em relação a este procedimento.

⁽²⁶⁾ Veja se, em sentido similar, o acórdão da Relação de Lisboa de 11 de Janeiro de 1996 in Col. Jur. Ano XXI, 1996, Tomo I, pág. 79.

PARTE III
DECISÕES
DA CNPD

O elevado número de decisões emitidas pela CNPD, durante os anos de 2003 e 2004, levou-nos a optar por um meio diferente para as publicitar.

Por um lado, a sua publicação em suporte de papel tornava este relatório num instrumento de difícil manuseamento e consulta; por outro lado, os custos de produção ascendiam a valores praticamente incontroláveis.

Estando as decisões da Comissão (pelo menos, na sua maioria) disponíveis no nosso *site*, logo acessíveis ao público, cumprindo-se desta forma o dever que a lei impõe de publicidade dos tratamentos de dados, considerámos não se justificar a sua publicação em livro.

No entanto, tendo em conta que o *site* tem um motor de pesquisa autónomo para a busca de decisões, bastando para tal referenciar o ano, espécie e número respectivo, integrámos neste relatório de actividades uma listagem de todas as decisões da CNPD, que correspondem aos anos aqui abrangidos, de modo a permitir uma consulta mais rápida e eficaz.

Esta opção pela publicação das decisões em suporte digital tem ainda a vantagem de poder identificar-se mais facilmente a matéria sobre que versa cada decisão, bem como poder gravar os textos e arquivá-los, se for o caso, de acordo com os interesses de cada um.

As decisões da CNPD podem ser acedidas em: **<http://www.cnpd.pt/bin/decisoes/decisoes.asp>**

2 0 0 3

1 – Deliberações

- 1/03** – Contra-ordenação contra discoteca de Lisboa que na sua página de Internet fazia tratamento de dados sem consentimento dos titulares;
- 2/03** – Queixa relativa a uma correspondência registada numa estação dos CTT que não foi entregue nem ao destinatário nem ao remetente;
- 3/03** – Ratificação de um Despacho da CNPD sobre a inexistência de indicações sobre um requerente no SIS;
- 4/03** – Queixa relativa à listagem de inibição do uso de cheque;
- 5/03** – Contra-ordenação por falta de notificação de sistema de controlo de alunos em escola;
- 6/03** – Contra-ordenação por falta de notificação de videovigilância numa pastelaria;
- 7/03** – Queixa relativa à listagem de cliente de risco dum banco;
- 8/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 9/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 10/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 11/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 12/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 13/03** – Queixa relativa à confidencialidade das chamadas telefónicas;
- 14/03** – Acesso a dados de saúde de familiar falecido para processo de seguro de vida;

- 15/03** – Pedido para mudança de autorização com a finalidade de gestão de reservas;
- 16/03** – Contra-ordenação contra autarquia por falta de notificação de tratamento de dados pessoais;
- 17/03** – Contra-ordenação por falta de notificação de tratamento em entidade particular;
- 18/03** – Queixa contra empresa de telecomunicações por não eliminar dados pessoais;
- 19/03** – Arquivamento de queixa contra entidade bancária;
- 20/03** – Acesso de dados de saúde de familiar falecido em estabelecimento hospitalar para processo judicial;
- 21/03** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 22/03** – Pedido de informação sobre a Resolução do Conselho de Ministros 97/2002, de 18 de Maio;
- 23/03** – Queixa contra entidade de crédito por manter dados indevidamente;
- 24/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 25/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 26/03** – Pedido de informação de organismo público sobre comunicação de dados a terceiros;
- 27/03** – Contra-ordenação a hospital por falta de notificação de tratamentos de dados pessoais;
- 28/03** – Bloqueio temporário dos tratamentos e contra-ordenação a empresa informática por falta de notificação de tratamentos de dados pessoais;
- 29/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 30/03** – Acesso de dados de saúde de dois falecidos por entidade pública para processo de inquérito;
- 31/03** – Acesso de dados de saúde de familiar falecido em estabelecimento hospitalar;
- 32/03** – Bloqueio temporário de site de um estabelecimento escolar na sequência de uma queixa de tratamento de dados sem autorização e não notificado;

- 33/03** – Levantamento de bloqueio a sites de empresa informática;
- 34/03** – Parecer sobre voto por via electrónica numa entidade sindical;
- 35/03** – Acesso a dados de saúde para estudo epidemiológico;
- 36/03** – Confirmação de contra-ordenação contra pastelaria por não ter notificado uma videovigilância;
- 37/03** – Queixa contra estabelecimento de ensino por fornecimento de dados sem autorização;
- 38/03** – Acesso a dados de saúde em estabelecimento hospitalar por companhia de seguros;
- 39/03** – Queixa por divulgação indevida de dados pessoais por várias entidades públicas e privadas;
- 40/03** – Processo de averiguações relativo a documentos bancários encontrados num contentor de lixo;
- 41/03** – Queixa contra empresa ligada à Internet por recolha indevida de dados pessoais;
- 42/03** – Queixa contra entidades bancárias relativa à manutenção indevida em listagem de utilizadores de cheques sem provisão;
- 43/03** – Parecer sobre “Carta dos Direitos do Doente Internado”;
- 44/03** – Parecer sobre acesso a dados de saúde por estudante da Licenciatura em Radiologia;
- 45/03** – Parecer sobre programa de actualização de ficheiros clínicos de doentes portadores de VIH/sida;
- 46/03** – Contra-ordenação contra entidade de telecomunicações por comunicação de dados sem informar os titulares dos mesmos;
- 47/03** – Ratificação de decisão da CNPD de eliminação de dados pessoais na sequência de queixa contra estabelecimento escolar;
- 48/03** – Admoestação de estabelecimento escolar por não cumprir n.º1 do art.º 27 da Lei n.º 67/98, de 26 de Outubro;
- 49/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 50/03** – Queixa contra operador de transportes;

- 51/03** – Contra-ordenação contra empresa farmacêutica por incumprimento de autorização da CNPD;
- 52/03** – Acesso a dados de saúde de familiar de falecido para efeitos de seguro de vida;
- 53/03** – Acesso a dados de saúde de familiar de falecidos existentes em estabelecimento hospitalar para apuramento de eventual negligência;
- 54/03** – Contra-ordenação contra empresa por não notificar tratamento de dados pessoais;
- 55/03** – Contra-ordenação contra autarquia por não notificar tratamentos de dados pessoais;
- 56/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 57/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 58/03** – Queixa contra estabelecimento escolar por recolha de dados pessoais dos alunos sem autorização;
- 59/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 60/03** – Queixa relativa à listagem de cliente de risco dum banco;
- 61/03** – Queixa relativa à listagem de cliente de risco dum banco;
- 62/03** – Contra-ordenação contra empresa de construção civil por falta de notificação de tratamento de dados pessoais;
- 63/03** – Pedido de acesso ao Sistema de Informação Schengen;
- 64/03** – Contra-ordenação contra estabelecimento escolar por falta de notificação de tratamento de dados pessoais;
- 65/03** – Parecer sobre divulgação de dados pessoais de base de dados de uma entidade privada;
- 66/03** – Contra-ordenação contra estabelecimento hospitalar por falta de notificação de tratamento de dados pessoais;
- 67/03** – Pedido de parecer sobre acesso a dados de saúde por parte de estabelecimento hospitalar;
- 68/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;

- 69/03** – Acesso a dados de saúde em estabelecimento hospitalar por entidade pública;
- 70/03** – Acesso a dados de saúde em estabelecimento hospitalar por quadro daquele mesmo hospital;
- 71/03** – Queixa contra entidade de crédito por comunicação de dados sem autorização do titular;
- 72/03** – Pedido de informações sobre a existência de dados pessoais na Polícia Judiciária;
- 73/03** – Acesso a dados de saúde em estabelecimento hospitalar por entidade pública para apurar eventual negligência;
- 74/03** – Acesso a dados de saúde em estabelecimento hospitalar por familiar de falecido para acção judicial;
- 75/03** – Parecer sobre divulgação de dados de saúde de um estabelecimento hospitalar a uma seguradora;
- 76/03** – Acesso a dados de saúde em estabelecimento hospitalar por familiar de falecida para efeitos judiciais;
- 77/03** – Contra-ordenação contra empresa de restauração e bebidas por não ter notificado tratamento de videovigilância;
- 78/03** – Contra-ordenação contra estabelecimento escolar por falta de notificação de tratamento de dados pessoais;
- 79/03** – Contra-ordenação contra empresa turística por falta de notificação de tratamento de dados pessoais;
- 80/03** – Bloqueio temporário de tratamento de dados de entidade pública e contra-ordenação por falta de notificação desse mesmo tratamento e comunicação de dados sem autorização;
- 81/03** – Contra-ordenação contra seguradora na sequência de queixa de um segurado relativa a uma base de dados de não pagadores de prémios;
- 82/03** – Pedido de informação de entidade pública sobre eventual recurso a interconexão de dois tratamentos;
- 83/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;

- 84/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 85/03** – Pedido de autorização por parte de instituto público para comunicação de dados a entidade pública;
- 86/03** – Pedido de parecer sobre acesso a dados de saúde em instituto médico para efeitos de investigação;
- 87/03** – Acesso a dados de saúde em estabelecimentos hospitalares por familiar de falecido para acção judicial;
- 89/03** – Notificação de tratamento relativo a investigação médica por Faculdade de Medicina;
- 90/03** – Ratificação de parecer da CNPD, pedido por entidade pública, sobre permanência de cidadãos brasileiros em território nacional;
- 91/03** – Ratificação de despacho da CNPD sobre pedido de acesso ao Sistema de Informação Schengen;
- 92/03** – Ratificação de parecer da CNPD sobre decreto-lei que cria o Sistema de Identificação de Canídeos e Felinos;
- 93/03** – Ratificação de parecer da CNPD sobre proposta de lei relativa ao regime jurídico aplicável às comunicações electrónicas;
- 94/03** – Contra-ordenação contra centro comercial por falta de notificação de tratamento de videovigilância;
- 95/03** – Queixa contra instituição bancária por manter indevidamente dados na lista de “incidentes cheques”;
- 96/03** – Acesso a dados de saúde em estabelecimento hospitalar por entidade pública;
- 97/03** – Pedido de partido político para acesso à Base de Dados do Recenseamento Eleitoral;
- 98/03** – Revogação de contra-ordenação contra estabelecimento de bebidas por prescrição;
- 99/03** – Contra-ordenação contra firma por falta de notificação de tratamento de videovigilância;
- 100/03** – Queixa contra operadora de telecomunicações por troca de correspondência;

- 101/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 102/03** – Acesso a dados de saúde em estabelecimento hospitalar por entidade policial para instrução de processo de sanidade;
- 103/03** – Acesso a dados de saúde em estabelecimento hospitalar por familiar de falecido para processo de cobrança de seguro de vida;
- 104/03** – Queixa contra empresa de vendas por correspondência por enviar publicidade domiciliária sem autorização;
- 105/03** – Ratificação de parecer da CNPD sobre projecto de decreto-lei para criar uma linha de crédito para financiamento da aquisição, armazenamento e preservação da madeira de pinho e eucalipto;
- 106/03** – Notificação de tratamento de empresa farmacêutica para registar condições de utilização de medicamento;
- 107/03** – Queixa contra entidade pública por comunicação de dados sem autorização;
- 108/03** – Processo de averiguações sobre dados biométricos numa entidade pública;
- 109/03** – Parecer sobre processo judicial que envolve empresa de telecomunicações;
- 110/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 111/03** – Queixa contra instalação de videovigilância num prédio de habitação;
- 112/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 113/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 114/03** – Parecer sobre processo judicial que envolve empresa de telecomunicações;
- 115/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 116/03** – Contra-ordenação contra entidade pública por omissão de notificação de tratamento de dados pessoais;
- 117/03** – Acesso de dados clínicos em estabelecimento hospitalar por familiares de falecido para eventual processo judicial;
- 118/03** – Parecer sobre comunicação de dados por parte de uma entidade sindical;
- 119/03** – Parecer sobre a realização de um inquérito por parte de estabelecimento hospitalar;

- 120/03** – Parecer sobre comunicação de dados de uma entidade pública para entidade sindical;
- 121/03** – Acesso a dados de saúde em estabelecimento hospital por parte de familiar de falecida;
- 122/03** – Pedido de entidade ligada ao crédito de reapreciação de deliberações da CNPD no que respeita a prazos de conservação de dados;
- 123/03** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de doente;
- 124/03** – Contra-ordenação contra entidade de serviços médicos por tratamento de dados pessoais sem a devida notificação;
- 125/03** – Arquivamento de contra-ordenação contra entidade ligada ao crédito, relativa à não prestação do direito à informação, por prescrição;
- 126/03** – Pedido de acesso ao Sistema de Informação Schengen;
- 127/03** – Pedido de informação de instituto médico sobre possibilidade de comunicação de dados de saúde;
- 128/03** – Tratamento de dados pela NetSaúde;
- 129/03** – Acesso a dados clínicos em estabelecimento hospitalar por familiar de falecido para efeitos de seguro;
- 130/03** – Acesso a dados clínicos de falecida em estabelecimento hospitalar a pedido de seguradora;
- 131/03** – Queixa relativa a informação negativa de “cliente de risco” contra entidade bancária;
- 132/03** – Acesso a dados clínicos em estabelecimento hospitalar por familiar de falecida para efeitos de seguro;
- 133/03** – Parecer sobre projecto de protocolo entre uma associação e os seus associados;
- 134/03** – Acesso a dados clínicos em estabelecimento hospitalar por familiar de falecido para fins de acção judicial;
- 135/03** – Acesso a dados de saúde em estabelecimento hospitalar por familiar de falecida;

- 136/03** – Queixa contra empresa municipal por acesso a dados pessoais sem autorização;
- 137/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 138/03** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 139/03** – Perecer sobre tratamento de dados pessoais no quadro de operações de titularização de créditos;
- 140/03** – Acesso a dados de saúde em estabelecimento hospitalar por parte de seguradora;
- 141/03** – Pedido de autorização para tratamento de dados relativos a participações dos beneficiários por entidade para-militar;
- 142/03** – Queixa contra entidade bancária por utilização abusiva de dados pessoais;
- 143/03** – Acesso a dados clínicos em estabelecimento hospitalar por parte de seguradora;
- 144/03** – Parecer sobre acesso a gravações de um acidente por parte de corporação de bombeiros;
- 145/03** – Queixa contra empresa de actividades de lazer por omissão na notificação de tratamento de videovigilância;
- 146/03** – Tratamento de dados de saúde para rastreio de cancro da mama;
- 147/03** – Tratamento de dados de saúde para rastreio de cancro da mama;
- 148/03** – Queixa contra entidade pública por comunicação de dados pessoais sem autorização;
- 149/03** – Pedido de averiguação de uma cláusula contratual das condições gerais de utilização de cartões Vida e Eurocard/Mastercard e serviço MBNet de entidade bancária;
- 150/03** – Acesso a dados de saúde em estabelecimento hospitalar por parte de seguradora.

2 – Autorizações

- 1/03** – Tratamento de dados para registo de militantes para envio de correspondência, quotização, realizações de eleições e actividades internas
- 2/03** – Cedência de dados no âmbito de uma operação bancária de cessão de créditos;
- 3/03** – Cedência de dados a terceiros no âmbito de operação de titularização de créditos;
- 4/03** – Comunicação de dados por parte de instituição de crédito para fins promocionais entre empresas do grupo;
- 5/03** – Tratamento de dados com finalidade de gestão de clientes e serviços e acções de marketing;
- 6/03** – Pedido de acesso à base de dados do STAPE por instituto nacional de saúde;
- 7/03** – Tratamento de dados para cumprimento das suas atribuições legais por entidade pública;
- 8/03** – Tratamento de dados pessoais relativo a visitantes de reclusos em estabelecimento prisional;
- 9/03** – Fluxo de dados para a Alemanha e Canadá no âmbito de um tratamento de dados com a finalidade de recursos humanos;
- 10/03** – Tratamento de dados de saúde por um centro de fisioterapia;
- 11/03** – Tratamento de dados para avaliar resultados de campanha educacional para controlo da hipertensão arterial e o envio de materiais de campanha e, numa segunda fase, estudo científico da população hipertensa, por médica cardiologista de estabelecimento hospitalar;
- 12/03** – Cedência de dados entre entidades bancárias para permitir atendimento das solicitações de serviços por parte dos titulares dos dados;
- 13/03** – Comunicação de dados entre alguns laboratórios de Anatomia Patológica e a Coordenadora do Registo Oncológico Regional do Sul, no âmbito das suas atribuições;

- 14/03** – Tratamento de dados por parte de um estabelecimento escolar no âmbito de um sistema de cartão magnético para pagamentos no bar e cantina e controlo de acessos;
- 15/03** – Tratamento de dados de uma sociedade com a finalidade de registo de dados dos trabalhadores das empresas contratadas e relatórios anuais dos serviços de saúde no trabalho;
- 16/03** – Tratamento de dados relativo à gestão de cartões Visa Electron;
- 17 a 97/03** – Tratamento de dados de saúde pela NetSaúde;
- 98/03** – Cedência de dados entre entidades bancárias para permitir atendimento das solicitações de serviços por parte dos titulares dos dados;
- 99/03** – Tratamento de dados para análise estatística de moradores de habitação municipal; gestão de irregularidades na ocupação da via pública; registo, manutenção e pesquisa do cadastro de saúde dos trabalhadores de autarquia;
- 100/03** – Cedência de dados no âmbito de uma operação de titularização de créditos hipotecários;
- 101/03** – Transferência de dados pessoais para os Estados Unidos da América no âmbito de um tratamento de dados relativo à apreciação e gestão de propostas de crédito;
- 102/03** – Transferência de dados pessoais para os Estados Unidos da América no âmbito de um tratamento de dados relativo à apreciação e gestão de propostas de aluguer de longa duração;
- 103/03** – Tratamento de dados de saúde sobre doentes hospitalizados num serviço de medicina;
- 104/03** – Interconexão de dados oriundos da aplicação SINUS e conferência de facturas;
- 105/03** – Tratamento estatístico de dados relativos a utentes e actividade operativa de instituição pública;
- 106/03** – Comunicação de dados à Associação Nacional dos Engenheiros Técnicos por parte de autarquia;

- 107/03** – Tratamento de dados com finalidades de gestão de candidaturas à compra de bilhetes para o evento Euro 2004, marketing e manutenção da segurança pública;
- 108 a 270/03** – Tratamento de dados de saúde pela NetSaúde;
- 476/03** – Transferência de dados pessoais para os Estados Unidos da América no âmbito de tratamento relativo a recursos humanos;
- 477/03** – Transmissão de dados pessoais em Portugal e no estrangeiro no âmbito de um projecto de controlo e circulação de informação de clientes de instituição bancária;
- 478/03** – Tratamento de dados com finalidade de avaliar resultados de campanha educacional para controlo da hipertensão arterial, envio de material de campanha e estudo científico da população hipertensa;
- 479/03** – Tratamento de dados com finalidade de proporcionar o bem-estar psico-social dos trabalhadores de associação industrial, com rastreio de drogas e álcool;
- 480/03** – Tratamento de dados para registo, manutenção e pesquisa de cadastro de saúde dos trabalhadores de instituto de investigação médica;
- 481/03** – Tratamento de dados com finalidade de gestão de expediente e aplicações de contra-ordenações na sequência da realização de publicidade em violação da lei;
- 482/03** – Cedência de dados pessoais no âmbito de uma operação titularização de créditos;
- 483/03** – Transferência de dados para os Estados Unidos da América relativa a tratamentos de gestão de recursos humanos;
- 484/03** – Transferência de dados para os Estados Unidos da América relativa a tratamentos de gestão de recursos humanos;
- 485/03** – Transferência de dados para os Estados Unidos da América relativa a tratamentos de gestão de recursos humanos;
- 486/03** – Transferência de dados para a Índia para centralizar pagamentos interbancários;

- 487/03** – Cedência de dados a terceiros no âmbito de uma operação de titularização de créditos;
- 488/03** – Cedência de dados entre entidades bancárias para permitir atendimento das solicitações de serviços por parte dos titulares dos dados;
- 489/03** – Ratificação de autorização de tratamento de dados no âmbito do processamento de informação a associados dos serviços sociais de entidade bancária;
- 490/03** – Acesso a dados pessoais por entidade policial;
- 491/03** – Tratamento relativo a dados de doentes de consulta de Imuno-hemoterapia – dado raça/origem étnica;
- 492/03** – Fluxo de dados para os Estados Unidos da América no âmbito de um tratamento de gestão de recursos humanos;
- 493/03** – Tratamento de dados relativos à gestão de processos em instrução;
- 494/03** – Alteração na forma de recolha de dados de um tratamento relativo à análise comportamental de clientes e marketing directo;
- 495/03** – Tratamento relativo à gestão de dados de saúde e dados genéticos, com finalidades de diagnóstico e prestação de cuidados de saúde e investigação clínica e genética de certas doenças;
- 496/03** – Videovigilância num parque natural;
- 497/03** – Tratamentos de dados pessoais para diagnóstico e prestação de cuidados de saúde, para realização de estudos epidemiológicos ou científicos;
- 498/03** – Tratamento com a finalidade de identificação de características de grupos de utilizadores de um site e envio de promoções;
- 499/03** – Gestão de clientes de instituição bancária, com acompanhamento de aplicações financeiras e cedência de dados entre empresas do Grupo;
- 500/03** – Gestão de clientes de instituição bancária, com acompanhamento de aplicações financeiras e cedência de dados entre empresas do Grupo;
- 501/03** – Fluxo transfronteiriço de dados no âmbito de tratamento de gestão de clientes;

- 502/03** – Tratamento de gestão de reservas, emissão de bilhetes, controlo de partidas e controlo de bagagens com fluxo transfronteiriço de dados pessoais;
- 503/03** – Tratamento de dados de saúde de doentes hospitalizados no serviço de medicina;
- 504/03** – Tratamentos de dados pessoais e de saúde em estabelecimento hospitalar;
- 505/03** – Comunicação de dados a entidades em regime de subcontratação no âmbito de tratamento de gestão de clientes;
- 506/03** – Tratamento de dados pessoais relativo à selecção de concorrentes para programa televisivo;
- 507/03** – Tratamento de dados de saúde em centro de fisioterapia;
- 508/03** – Gestão de clientes de instituição bancária, com acompanhamento de aplicações financeiras e cedência de dados entre empresas do Grupo;
- 509/03** – Tratamento relativo a informações de crédito e solvabilidade;
- 510/03** – Registo de imigrantes para ajuda à integração social e profissional em Portugal;
- 511/03** – Tratamento de dados relativo à selecção de concorrentes para participação num programa de televisão;
- 512/03** – Gestão das acções de apoio social e de cuidados continuados dirigidos a pessoas em situação de dependência;
- 513/03** – Tratamento de dados com finalidade de acompanhar a execução do Programa de Iniciativa Comunitária EQUAL;
- 514/03** – Cedência de dados no âmbito de uma operação de titularização de créditos;
- 515/03** – Cedência de dados no âmbito de uma operação de titularização de créditos;
- 516/03** – Tratamento de dados relativo à selecção de concorrentes para participação em concurso de televisão;
- 517/03** – Tratamento de dados para análise, gestão e tratamento de contratos de cartões de crédito, com comunicação de dados para França;

- 518/03** – Tratamento de dados para análise, gestão e tratamento de contratos de cartões de crédito, com comunicação de dados para França;
- 519/03** – Tratamento de dados para análise, gestão e tratamento de contratos de cartões de crédito, com comunicação de dados para França;
- 520/03** – Tratamento com finalidade de gestão dos registos oncológicos na região centro;
- 521/03** – Acesso a dados clínicos relativos a tratamentos de estomatologia;
- 522/03** – Cedência de dados no âmbito de uma operação de titularização de créditos;
- 523/03** – Cedência de dados no âmbito de uma operação de titularização de créditos hipotecários;
- 524/03** – Cedência de dados no âmbito de uma operação de titularização de créditos;
- 525/03** – Cedência de dados no âmbito de uma operação de titularização de créditos;
- 526/03** – Tratamento de dados pessoais relativos a recursos humanos;
- 527/03** – Comunicação de dados para os Estados Unidos da América no âmbito de um tratamento de recursos humanos;
- 528/03** – Fluxo de dados para o Reino Unido e Índia relativo a um tratamento de conservação, gestão e processamento de dados pessoais de assinantes de serviços de telecomunicações;
- 529/03** – Gestão de consultas e exames de medicina ocupacional;
- 530/03** – Tratamento de dados relativo à selecção de concorrentes para participação em programa de televisão;
- 531/03** – Tratamento de gestão de consultas e exames de medicina ocupacional – Medicina do Trabalho;
- 532/03** – Tratamento de dados de saúde em unidade hospitalar – dados raça/etnia de forma não nominativa;
- 533/03** – Cedência de dados para fins de marketing, no âmbito do tratamento de dados para cartão de crédito;

- 534/03** – Cedência de dados para fins de marketing, no âmbito do tratamento de dados para cartão de crédito;
- 535/03** – Cedência de dados para fins de marketing, no âmbito do tratamento de dados para cartão de crédito;
- 536/03** – Tratamento de dados relativo a informações de crédito e solvabilidade;
- 537/03** – Tratamento de dados pessoais relativo à gestão de pessoas acreditadas para entrar nos recintos do Euro 2004;
- 538/03** – Base de dados da Segurança Social;
- 539/03** – Transmissão de dados a empresas do Grupo relativos a um tratamento de dados de gestão de clientes;
- 540/03** – Tratamento relativo à gestão da saúde ocupacional de funcionários de grupo bancário;
- 541/03** – Gestão de informação dos serviços de segurança, higiene e saúde no trabalho;
- 542/03** – Tratamento de dados relativo a uma dissertação de doutoramento em Psicologia Clínica;
- 716/03** – Registo de informação dos visitantes de um site para fins de marketing;
- 717/03** – Tratamento no âmbito dos serviços de Medicina do Trabalho;
- 718/03** – Tratamento com finalidade de concessão de empréstimos e créditos.

3 – Pareceres

- 1/03** – Projecto de Decreto/Lei que altera o estatuto da Câmara dos Solicitadores ao abrigo da Lei 23/2002 de 21 de Agosto;
- 2/03** – Projecto de Lei n.º 28/IX, relativo a informação genética pessoal e informação de saúde;
- 3/03** – Projecto de diploma que regulamenta a instituição do número de identificação fiscal, bem como as condições da sua atribuição, respectivos efeitos e a sua gestão;

- 4/03** – Protocolo de colaboração entre o Ministério das Finanças e o Instituto Nacional de Estatística;
- 5/03** – Projecto de Decreto/Lei que regulamenta as condições de acesso e análise, em tempo real, à informação pertinente à investigação dos crimes tributários, pela Polícia Judiciária e pela Administração Tributária;
- 6/03** – Proposta de Lei n.º 44/IX, que autoriza o Governo a legislar sobre certos aspectos legais dos Serviços da Sociedade de Informação, em especial do comércio electrónico, no comércio interno;
- 7/03** – Protocolo de acesso em linha à informação constante da Base de Dados de Emissão de Passaportes (BADEP) e ao Sistema de Informações Integrado do Serviço de Estrangeiros e Fronteiras (SII/SEF);
- 8/03** – Código de Trabalho;
- 9/03** – Projecto de diploma que regula o registo informático das execuções no Código de Processo Civil;
- 10/03** – Projecto de Lei n.º 217/IX que aprova o Regime Jurídico da Obtenção da Prova Digital Electrónica na Internet;
- 11/03** – Acesso, através do Sistema de Pesquisa On-line (SPO), à base de dados dos Serviços de Identificação Civil;
- 12/03** – Projecto de Lei n.º 208/IX/1.ª (PS) intitulado “Garante a protecção de dados pessoais e a privacidade das comunicações electrónicas na sociedade da informação, procedendo à transposição da Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002”;
- 13/03** – Projecto de decreto-lei que transpõe a Directiva sobre o comércio electrónico, Directiva 200/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000;
- 14/03** – Projecto de Decreto-Regulamentar relativo à gestão hospitalar;
- 15/03** – Projecto de diploma que regula o regime informático de execuções;
- 16/03** – Anteprojecto de alteração ao regulamento dos ficheiros informáticos da Direcção Geral da Administração da Justiça, em matéria de identificação criminal e de contumazes;

- 17/03** – Proposta de Lei 54/IX/1.^a (GOV) que visa a transposição para a ordem jurídica nacional da Directiva 2001/40/CE do Conselho, de 28 de Maio de 2001, relativa ao reconhecimento mútuo de decisões de afastamento de nacionais de países terceiros;
- 18/03** – Projecto de portaria com objectivo de aprovar modelo de identificação do utente do Serviço Regional de Saúde, bem como o modelo de formulário de identificação do utente e as respectivas instruções;
- 19/03** – Proposta de Lei n.º 59/IX/1.^a do Governo relativa a normas mínimas em matéria de concessão de protecção temporária no caso de afluxo maciço de pessoas deslocadas e as medidas tendentes a assegurar uma repartição equilibrada do esforço assumido pelos Estados-membros ao acolherem estas pessoas e suportarem as consequências decorrentes deste acolhimento;
- 20/03** – Projecto de Recomendação da Comissão Europeia relativo ao tratamento das informações de localização da pessoa que efectua a chamada nas redes de comunicações electrónicas tendo em vista os serviços de chamadas de urgência com capacidade de localização;
- 21/03** – Projecto de protocolo a celebrar entre a Polícia Judiciária e o Serviço de Estrangeiros e Fronteiras;
- 22/03** – Proposta de lei n.º 70/IX/1.^a que autoriza o Governo a alterar o regime jurídico do exercício da actividade de segurança privada;
- 23/03** – Projecto de decisão relativa à inclusão de dados pessoais dos assinantes nas listas telefónicas e serviço informativo no âmbito do Serviço Universal de Telecomunicações;
- 24/03** – Tratamento de dados pessoais que visa facilitar o trabalho administrativo de processamento e tratamento dos dados referentes aos cidadãos brasileiros que estejam em condições de beneficiar do acordo celebrado entre a República Portuguesa e a República Federativa do Brasil sobre Contração Recíproca de Nacionais;
- 25/03** – Proposta de lei de autorização legislativa que visa utilizá-la relativamente ao regime jurídico aplicável às comunicações electrónicas, ao regime de

- controlo jurisdicional dos actos praticados pela ANACOM, de reforço do quadro sancionatório e de utilização do domínio público e respectivas taxas;
- 26/03** – Projecto de decreto-lei que cria o Sistema de Identificação de Canídeos e Felinos (SICAFE);
- 27/03** – Proposta de Decreto Legislativo Regional que cria a Bolsa de Emprego Público dos Açores;
- 28/03** – Proposta de lei n.º 53/IX, que tem por objecto autorizar o Governo a legislar em matéria de tratamento e interconexão dos dados constantes das informações a prestar pelas instituições de crédito mutuantes em relação a cada um dos contratos de empréstimo à habitação bonificados;
- 29/03** – Regime aplicável às contra-ordenações aeronáuticas civis;
- 30/03** – Proposta de lei relativa ao Estatuto do agente de cooperação;
- 31/03** – Projecto de Decreto-Lei relativo à assistência mútua em matéria de cobrança de créditos;
- 32/03** – Parecer sobre a possibilidade do tratamento informatizado (digitalização) de impressões digitais;
- 33/03** – Projecto de Decreto-Lei relativo ao regime de infracções no sector vitivinícola e respectiva autorização legislativa;
- 34/03** – Cedência de elementos da base de dados da Caixa Geral de Aposentações a entidade terceira;
- 35/03** – Projecto de Decreto-Lei que, na sequência dos incêndios de Verão, visa regular a criação de uma linha de crédito para financiamento, aquisição, armazenamento e preservação da madeira de pinho e eucalipto;
- 36/03** – Parecer sobre a possibilidade legal de cedência, aos parceiros europeus, da lista de nacionais de cada Estado Membro da UE inscritos nos respectivos postos consulares;
- 37/03** – Parecer sobre a instrução que visa regular a forma e termos de acesso às informações constantes do tratamento de utilizadores de cheque que oferecem risco, quando estas se destinam à avaliação de riscos;
- 38/03** – Projecto de Decreto-Lei definidor do regime jurídico do acesso e exercício da actividade de promoção e organização de campos de férias;

- 39/03** – Projecto de Decreto-Lei relativo à Rede de Cuidados Continuados da Saúde;
- 40/03** – Projecto de Decreto-Lei que tem por objecto estabelecer o regime jurídico do comércio electrónico;
- 41/03** – Projecto de Decreto-Lei relativo à segurança privada;
- 42/03** – Projecto de Decreto-Lei relativo à detecção de animais de companhia perigosos e potencialmente perigosos;
- 43/03** – Proposta de lei de autorização legislativa relativamente ao regime jurídico aplicável às comunicações electrónicas, ao regime do controlo jurisdicional dos actos praticados pela ANACOM, de reforço do quadro sancionatório e de utilização do domínio público e respectivas taxas;
- 44/03** – Novo Código de Conduta das Empresas de Marketing Directo;
- 45/03** – Proposta de lei n.º 96/IX/2.^a, do Governo, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas;
- 46/03** – Projectos de diplomas sobre o Regime Jurídico do Administrador da Insolvência e do Código de Insolvência e da Recuperação de Empresas;
- 47/03** – Parecer sobre a possibilidade de Portugal, no contexto do Euro 2004, inserir no Sistema de Informação Schengen os dados relativos aos adeptos de futebol que o Director da Joint Operational Authority, Sirene UK conhece como sendo violentos;
- 48/03** – Parecer sobre a instrução que visa regular a forma e termos de acesso às informações constantes do tratamento de utilizadores de cheque que oferecem risco, quando estas se destinam à avaliação de riscos de crédito por parte das instituições financeiras;
- 49/03** – Projecto de Decreto-Lei que cria o registo nacional de menores estrangeiros que se encontrem em situação irregular no território nacional;
- 50/03** – Projectos de decreto-lei relativos ao Estatuto do Notariado e ao Estatuto da Ordem dos Notários;
- 51/03** – Acordo a celebrar entre a República Portuguesa e a República da Moldova sobre readmissão de pessoas em situação irregular;
- 52/03** – Protocolo de Cartagena sobre Segurança Biológica.

2 0 0 4

1 – Deliberações

- 1/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 2/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 3/04** – Contra-ordenação a estabelecimento hospitalar por falta de notificação de tratamento de videovigilância;
- 4/04** – Pedido de acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecida para saber as causas da morte;
- 5/04** – Pedido de acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecida para saber as causas da morte;
- 6/04** – Pedido de acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecido para instaurar acção judicial;
- 7/04** – Pedido de acesso a dados de saúde em estabelecimento hospitalar para processo de beatificação;
- 8/04** – Tratamento de dados relativo a um programa de rastreio de cancro da mama de base populacional;
- 9/04** – Identificação por radiofrequência;
- 10/04** – Pedido de acesso a dados de saúde para efeitos de processo judicial;
- 11/04** – Contra-ordenação a entidade de formação profissional relativa à falta de notificação de tratamento de videovigilância;
- 12/04** – Pedido de acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecido para eventual procedimento judicial;

- 13/04** – Pedido de acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecido para apurar eventual negligência;
- 14/04** – Pedido de acesso a dados clínicos na posse de serviços de saúde por parte de seguradora;
- 15/04** – Contra-ordenação a empreendimento turístico por falta de notificação de tratamento de videovigilância
- 16/04** – Contra-ordenação a estabelecimento de hotelaria por falta de notificação de tratamento de videovigilância
- 17/04** – Pedido de acesso a dados de saúde em serviços de saúde por parte de entidade pública
- 18/04** – Pedido de acesso a dados de saúde em estabelecimento hospitalar por parte de seguradora
- 19/04** – Pedido de acesso a dados de saúde de falecido, na posse de serviços de saúde, por parte de uma seguradora
- 20/04** – Pedido de acesso de dados pessoais na posse de entidade pública por parte de entidade pública de segurança;
- 21/04** – Contra-ordenação contra empresa na sequência de queixa por parte de cidadão espanhol em relação à publicação dos seus dados pessoais no site daquela empresa e por esta estar em falta quanto à notificação daquele tratamento;
- 22/04** – Pedido de entidade pública de segurança para acesso a dados relativos a adeptos do futebol, no âmbito do Euro'2004;
- 23/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 24/04** – Ratificação de autorização dada pela CNPD a entidade bancária, respeitante a uma operação de titularização de créditos, em especial, no que diz respeito ao direito de informação;
- 25/04** – Contra-ordenação a estabelecimento de restauração por falta de notificação de tratamento de videovigilância;
- 26/04** – Pedido de parecer por parte de instituição de solidariedade social relativo ao fornecimento de dados pessoais a entidade pública de saúde, no âmbito do programa Saúde Escolar;

- 27/04** – Pedido de parecer por parte entidade pública de ensino relativo ao fornecimento de dados pessoais a entidade pública de saúde, no âmbito do programa Saúde Escolar;
- 28/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecida para fins de Seguro de Vida;
- 29/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de terceiro em relação ao nascimento de uma criança sobre a qual o requerente declara a paternidade;
- 30/04** – Acesso da dados de saúde em estabelecimento hospitalar por parte de familiar de falecido para efeitos de Seguro de Vida;
- 31/04** – Pedido de informação de entidade pública de saúde relativa à possibilidade de comunicação de dados pessoais a entidade privada de saúde;
- 32/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecida para eventual apuramento de negligência;
- 33/04** – Comunicação de dados relativos a facturação por parte de estabelecimento hospitalar a sub-sistema de saúde;
- 34/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de seguradora para efeitos de pagamento de seguro;
- 35/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecido, a pedido de seguradora;
- 36/04** – Denúncia por parte de trabalhador de um supermercado de existência de controlo sobre a caixa postal electrónica pessoal e páginas de Internet acedidas;
- 37/04** – Pedido de autorização de tratamento de dados sensíveis por parte de associação nacional ligada à saúde, que inclui comunicação de dados de um estabelecimento hospitalar;
- 38/04** – Acesso a dados de saúde na posse dos serviços de saúde públicos por parte de familiar de falecida para junção a processo judicial de inventário;
- 39/04** – Acesso a dados de saúde em estabelecimento hospitalar para processo de averiguações, no âmbito de um acidente ocorrido em serviço;

- 40/04** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 41/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecido para apuramento de eventual negligência;
- 42/04** – Parecer prévio sobre tratamento de dados com o objectivo de dotar a inspecção tributária de elementos actualizados sobre a fraude e evasão fiscais;
- 43/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de seguradora para efeitos de seguro de vida;
- 44/04** – Contra-ordenação a estabelecimento hospitalar por falta de notificação de tratamentos de dados pessoais;
- 45/04** – Tratamento de dados sem notificação num centro de saúde, descoberto na sequência de acção de fiscalização;
- 46/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 47/04** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 48/04** – Ratificação de decisão relativo a pedido de acesso à base de dados do STAPE;
- 49/04** – Divulgação pública de dados pessoais sem autorização dos titulares por parte de administração de um condomínio;
- 50/04** – Comunicação de dados por parte de entidade pública a pedido de estabelecimento escolar privado;
- 51/04** – Contra-ordenação a instituição de crédito relativa a uma queixa por manutenção indevida em listagem de utilizadores de cheques sem provisão;
- 52/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 53/04** – Queixa contra editora por incumprimento dos direitos de acesso e de oposição a dados pessoais;
- 54/04** – Contra-ordenação a estabelecimento hospitalar por falta de notificação de tratamentos de dados pessoais e de videovigilância;
- 55/04** – Contra-ordenação a estabelecimento comercial por falta de notificação de tratamento de videovigilância;
- 56/04** – Queixa contra empresa de vendas por catálogo por envio de marketing não requisitado;

- 57/04** – Averiguação sobre comunicação de dados de saúde sensíveis entre centros de saúde e estabelecimentos de ensino;
- 58/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de herdeiros de sinistrado para fins judiciais;
- 59/04** – Contra-ordenação a empresa distribuidora de gás por falta de notificação de tratamento de videovigilância;
- 60/04** – Ratificação de parecer da CNPD sobre a Proposta de Lei que aprovou o Código do Trabalho;
- 61/04** – Princípios sobre tratamento de videovigilância;
- 62/04** – Contra-ordenação a supermercado por falta de notificação de tratamento de videovigilância;
- 63/04** – Pedido de acesso a dados pessoais na posse de entidade pública;
- 64/04** – Contra-ordenação a empresa de comunicação social por falta de notificação de um tratamento de dados pessoais e de um sistema de videovigilância;
- 65/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecida para apurar causa da morte;
- 66/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecidos para instaurar processo judicial;
- 67/04** – Parecer sobre regime jurídico aplicável a dados recolhidos na sequência de acto eleitoral em entidade mutualista;
- 68/04** – Pedido de autorização para recolha de imagens no âmbito do Euro'2004 por parte de força de segurança;
- 69/04** – Ratificação de parecer da CNPD relativo ao regime temporário da organização da ordem pública e da justiça na final do Euro'2004;
- 70/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 71/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 72/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de seguradora para completar processo relativo a seguro de vida;

- 73/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecido a pedido de seguradora;
- 74/04** – Acesso a dados de saúde em estabelecimento hospitalar pedido por instrutor de processo de averiguações de acidente de serviço que resultou em falecimento;
- 75/04** – Contra-ordenação a estabelecimento de hotelaria por falta de notificação de tratamento de videovigilância;
- 76/04** – Parecer sobre realização de investigação sobre dificuldades de aprendizagem em crianças institucionalizadas;
- 77/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de seguradora;
- 78/04** – Acesso a dados de saúde em estabelecimento hospitalar para accionar seguro;
- 79/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecido a para apurar eventual negligência;
- 80/04** – Contra-ordenação a supermercado por falta de notificação de tratamento de videovigilância;
- 81/04** – Queixa contra empresa por envio de marketing sem consentimento prévio;
- 82/04** – Queixa contra editora por posse indevida de dados pessoais;
- 83/04** – Queixa contra entidade pública por utilização indevida de dados pessoais;
- 84/04** – Pedido de acesso a bases de dados públicas por parte dos tribunais arbitrais;
- 85/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecida para efeitos de seguro;
- 86/04** – Acesso a dados de saúde por parte de familiar de falecido para efeitos de seguro;
- 87/04** – Arquivo de projecto de deliberação relativo à prática de contra-ordenação;
- 88/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 89/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecido por alegada negligência;

- 90/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 91/04** – Contra-ordenação a associação empresarial por falta de notificação de tratamento de dados pessoais;
- 92/04** – Contra-ordenação a empresa de hotelaria e similares por falta de notificação de tratamento de videovigilância;
- 93/04** – Contra-ordenação a empresa de material informático por falta de notificação de tratamento de dados pessoais;
- 94/04** – Parecer sobre o regime de emissão de certidões comprovativas da qualidade de arquitecto;
- 95/04** – Queixa contra entidades públicas privadas por comunicação de dados pessoais sem autorização;
- 96/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 97/04** – Pedido de acesso à base de dados de entidades públicas por parte de tribunal arbitral;
- 98/04** – Parecer sobre acesso a dados de saúde em estabelecimento hospitalar por parte de uma escola;
- 99/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiares do falecido e de seguradora para efeitos de seguro de vida;
- 100/04** – Parecer sobre Regulamento do Arquivo Clínico de estabelecimento hospitalar;
- 101/04** – Contra-ordenação a entidade privada por falta de notificação de tratamentos de videovigilância e de dados pessoais;
- 102/04** – Contra-ordenação a estabelecimento nocturno relativa à violação do direito de oposição;
- 103/04** – Queixa contra ginásio por causa de tratamento de videovigilância não notificado;
- 104/04** – Contra-ordenação a junta de freguesia por falta de notificação de tratamento de dados pessoais;
- 105/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecido para efeitos de seguro;

- 106/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 107/04** – Queixa por divulgação de dados pessoais na Internet;
- 108/04** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 110/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 111/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 112/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 113/04** – Ratificação de parecer da CNPD relativo a um pedido de acesso ao SIS;
- 114/04** – Ratificação de parecer da CNPD relativo a um protocolo entre a Direcção-Geral dos Registos do Notariado e o Instituto de Gestão Informática e Financeira da Saúde, respeitante à comunicação do dado “morte” dos utentes do SNS;
- 115/04** – Ratificação de parecer da CNPD relativo a um pedido de acesso ao SIS;
- 116/04** – Ratificação de parecer da CNPD relativo a um pedido de acesso ao SIS;
- 117/04** – Parecer da CNPD sobre notificação de tratamento de videovigilância numa creche e jardim de infância;
- 118/04** – Contra-ordenação a empresa de telecomunicações por falta de notificação de tratamento de videovigilância;
- 119/04** – Queixa contra empresa de defesa do consumidor por desrespeito do direito de oposição;
- 120/04** – Averiguação de sistema de videovigilância em empresa de construção civil;
- 121/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecida para apurar circunstâncias da morte;
- 122/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecida para efeitos de seguro de vida;
- 123/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 124/04** – Contra-ordenação a empresa que explora restaurante por falta de prestação do direito de informação relativo a um sistema de videovigilância;

- 125/04** – Queixa contra empresa de consultoria em recursos humanos e informática por remessa de publicidade não solicitada;
- 126/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecido para processo judicial relativo a seguro de vida;
- 127/04** – Contra-ordenação a autarquia na sequência de uma denúncia e fiscalização que constatou existência de sistema de tratamento de dados biométricos não notificado
- 128/04** – Contra-ordenação a empresa de comércio e importação de vestuário por falta de notificação de videovigilância;
- 129/04** – Queixa contra empresa por envio de publicidade sem consentimento;
- 130/04** – Queixa contra centro de saúde por alegado desaparecimento do processo clínico de familiar falecida;
- 131/04** – Pedido de acesso ao Sistema de Informações Schengen (SIS);
- 132/04** – Pedido de parecer sobre comunicação de dados a várias entidades suíças por parte de entidade pública;
- 133/04** – Contra-ordenação a empresa de marketing, na sequência de queixa, por falta de notificação de tratamento;
- 134/04** – Acesso a dados de saúde em serviços de saúde por parte de familiar de falecida para efeitos de seguro de vida;
- 135/04** – Acesso a dados de saúde em serviços de saúde por parte de familiar de doente;
- 136/04** – Acesso a dados de saúde por parte de estabelecimento hospitalar no âmbito de estudo epidemiológico;
- 137/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecido para apurar eventual negligência;
- 138/04** – Queixa contra estabelecimento de ensino por comunicação de dados a junta de freguesia;
- 139/04** – Queixa contra entidade pública por disponibilizar dados pessoais através da Internet;

- 140/04** – Queixa relativa à listagem de clientes com débitos em entidade que se dedica ao crédito;
- 141/04** – Acesso a dados de saúde em serviços de saúde por parte dos herdeiros de falecido para efeitos de seguro de vida;
- 142/04** – Acesso a dados de saúde em estabelecimento hospitalar em relação a falecido por parte de seguradora;
- 143/04** – Contra-ordenação a estabelecimento creche por falta de notificação de sistema de videovigilância;
- 145/04** – Queixa contra empresa de sector hoteleiro por comunicação de dados pessoais a tribunal;
- 146/04** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 147/04** – Parecer sobre a cedência de imagens por parte de hipermercado a entidade pública para fins de instrução de procedimento disciplinar;
- 148/04** – Acesso a dados de saúde em estabelecimento hospitalar pedido por entidade pública de segurança;
- 149/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecido para fins de processo judicial;
- 150/04** – Pedido de informações sobre situação laboral relacionada com dados pessoais em entidade pública;
- 151/04** – Pedido de acesso a dados sensíveis em entidade pública por parte de entidade judicial;
- 152/04** – Acesso a dados de saúde em estabelecimento hospitalar sobre falecido por parte de seguradora;
- 153/04** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 154/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de entidade pública em relação a funcionário daquela entidade;
- 155/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de familiar de falecido para apurar eventual hereditariedade da doença;
- 156/04** – Acesso a dados de saúde em estabelecimento hospitalar por parte de entidade pública;

- 157/04** – Acesso a dados de saúde por parte de familiar de falecido para apurar consequências legais da sua morte;
- 159/04** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral.

2 – Autorizações

- 1/04** – Comunicação de dados entre os vários serviços de entidade pública;
- 2/04** – Interconexão de dados dos utentes entre o Serviço Nacional de Saúde e outro sistema de saúde;
- 3/04** – Informatização de processo de filiação do agente, clubes e associações de federação desportiva;
- 4/04** – Transmissão de dados pessoais no âmbito do Euro'2004;
- 5/04** – Tratamento de dados clínicos resultantes da actividade de Medicina do Trabalho;
- 6/04** – Envio de questionários para casa de doentes para investigação na área da saúde;
- 7/04** – Recolha de dados e tratamento para emissão e gestão de cartões de crédito;
- 8/04** – Empréstimo e crédito, factoring, leasing, emissão e gestão de cartões de crédito, concessão de avais e garantias e subscrição de compromissos semelhantes;
- 9/04** – Gestão da segurança e de acesso a áreas restritas e reservadas de aeroporto;
- 10 a 17/04** – Tratamentos de dados clínicos resultantes da actividade de Medicina do Trabalho;
- 18/04** – Tratamento de dados relativos ao Rendimento Social de Inserção;
- 19 a 125/04** – Tratamento de dados de saúde pela NetSaúde;
- 126/04** – Tratamento de dados de saúde em estabelecimento hospitalar;

- 127/04** – Tratamento de dados de saúde pela NetSaúde;
- 128/04** – Pedido de acesso à base de dados da Direcção-Geral de Registos e Notariado e de divulgação de dados pessoais na Internet;
- 129/04** – Pedido de acesso à Base de Dados do Recenseamento Eleitoral;
- 130/04** – Tratamento de dados de saúde na posse de centro de saúde por entidade pública;
- 131/04** – Tratamento e envio de mailings em acções de marketing directo;
- 132/04** – Tratamento com comunicação, transmissão e consulta relativamente a dados informatizados de seguradoras;
- 133/04** – Tratamento de dados pessoais informatizados referentes ao sistema de informação do Cartão de Emergência para Diabéticos;
- 134/04** – Base de dados do Programa de Rastreio do Cancro da Mama;
- 135/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade e processamento de vencimentos em estabelecimento superior de ensino;
- 136/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade e processamento de vencimentos em entidade pública;
- 137/04** – Fluxo de dados para os Estados Unidos da América no âmbito de um tratamento de dados, demográficos e médicos, dos doentes em hemodiálise;
- 138/04** – Acesso a dados pessoais na posse de juntas de freguesia por autarquia local, no âmbito de uma campanha de sensibilização para detentores de cães;
- 139 a 142/04** – Sistemas de videovigilância em estádios para segurança das instalações e protecção de pessoas e bens; prevenção da violência e excessos dos espectadores;
- 143/04** – Estudo epidemiológico de avaliação da prevalência de depressão em consultas de psiquiatria;
- 144/04** – Sistema de videovigilância em estádio para segurança das instalações e protecção de pessoas e bens; prevenção da violência e excessos dos espectadores;

- 145/04** – Tratamento com finalidade de gestão dos solicitadores;
- 146/04** – Registo de atestados médicos para a carta de condução;
- 147/04** – Transferência de informações e transmissão de dados entre Segurança Social e Instituto do Emprego e Formação Profissional;
- 148/04** – Estudo estatístico da população para efeitos de tese de investigação;
- 149/04** – Cedência de dados no âmbito de uma operação de titularização de créditos;
- 150 a 223/04** – Tratamento de dados de saúde pela NetSaúde;
- 224/04** – Tratamento de dados de saúde em estabelecimento hospitalar;
- 225 a 454/04** – Tratamento de dados de saúde pela NetSaúde;
- 455/04** – Transmissão de dados no âmbito de um tratamento de gestão e comercialização de seguros de protecção de crédito;
- 456/04** – Tratamento de dados de saúde em instituto médico;
- 457/04** – Tratamento de dados de saúde em estabelecimento hospitalar;
- 458/04** – Tratamento de dados de saúde pela NetSaúde;
- 459/04** – Gestão de autos de contra-ordenação passados pela Polícia Municipal numa autarquia;
- 460/04** – Tratamento de dados de saúde para facilitar a análise e associação de dados em doentes de oncologia;
- 461/04** – Tratamento de dados com finalidade de cobrança de dívidas vencidas, certas e exigíveis;
- 462/04** – Rastreio pré-natal, com cálculo de risco de cromossomopatias e doença do tubo neural, e elaboração de relatórios de anatomia patológica e produção estatística do serviço;
- 463/04** – Rastreio pré-natal, com cálculo de risco de cromossomopatias e doença do tubo neural, e tratamento da informação para estudos científicos;
- 464/04** – Transmissão de dados pessoais entre empresas de um Grupo financeiro;
- 465/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade e processamento de vencimentos em estabelecimento de ensino;

- 466 a 470/04** – Tratamentos de dados biométricos (impressão digital) para controlo de assiduidade e processamento de vencimentos em autarquias;
- 471/04** – Tratamentos de dados biométricos (impressão digital) para controlo de assiduidade e processamento de vencimentos em entidade privada de solidariedade social;
- 472/04** – Tratamentos de dados biométricos (impressão digital) para controlo de assiduidade em estabelecimento hospitalar privado;
- 473/04** – Tratamento de dados biométricos (leitura da íris) para segurança no acesso às instalações de uma empresa;
- 474/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade e processamento de vencimentos numa empresa;
- 475/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa autarquia;
- 476/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade num sindicato;
- 477/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade e processamento de vencimentos numa associação de apoio social;
- 478/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade e processamento de vencimentos numa autarquia;
- 479/04** – Tratamento para prestação de serviços médicos do tipo assistência domiciliária;
- 480/04** – Tratamento de dados biométricos (impressão digital) para controlo de acesso à sala de informática de uma empresa;
- 481/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa autarquia;
- 482/04** – Tratamento de dados biométricos (impressão digital) para registo de entradas e saídas para contabilização da remuneração numa associação de bombeiros voluntários;
- 483/04** – Tratamento de dados de um instituto público para efectuar vigilância electrónica dos arguidos com obrigação de permanência na habitação;

- 484/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade num estabelecimento de ensino superior;
- 485/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade num conselho empresarial;
- 486/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa instituição de solidariedade social;
- 487/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa empresa;
- 488/04** – Tratamento para assistência a contratos de financiamento a crédito;
- 489/04** – Questionário sobre factores que favorecem os alunos com necessidades educativas especiais para efeitos de tese de doutoramento;
- 490/04** – Tratamento para informatizar o serviço de anatomia patológica, elaboração de relatórios de exames e produção estatística num estabelecimento hospitalar;
- 491/04** – Sistema de videovigilância instalado em Parque Natural para vigilância e detecção de fogos florestais, obras de construção ilegais, caça furtiva, depósito de entulhos, alterações de morfonologia do solo, actividades interditas e monitorização em áreas científicas;
- 492 e 493/04** – Tratamento de dados de saúde pela NetSaúde;
- 494/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade e processamento de vencimentos numa empresa municipal;
- 495 e 496/04** – Tratamento de dados para apoio à gestão financeira de empresas que integram Grupo empresarial;
- 497/04** – Transmissão de dados para os Estados Unidos da América no âmbito de um tratamento de gestão de recursos humanos de empresa informática;
- 498/04** – Tratamentos da dados pessoais no âmbito da gestão da informação dos serviços de segurança, higiene e saúde no trabalho;
- 499/04** – Gestão de processos de contra-ordenação em organismo público;
- 500 a 505/04** – Tratamento de dados para apoio à gestão financeira das várias empresas de um Grupo empresarial;

- 506/04** – Transferência de dados pessoais para países da União Europeia e para os Estados Unidos relativa a um tratamento de dados de recursos humanos numa empresa multinacional;
- 507/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa sociedade hoteleira;
- 508/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa autarquia;
- 509 a 511/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade em entidades públicas;
- 512/04** – Tratamento com finalidade de recolher e manter actualizada a informação relativa aos dadores de sangue;
- 513/04** – Tratamento de videovigilância instalado em linhas de abastecimento de combustível e lojas de conveniência;
- 514/04** – Tratamento para gestão comercial e administrativa de contratos de fornecimento de energia eléctrica e de gás, prestação de serviços afins, prospecção geral e marketing directo;
- 515 a 517/04** – Tratamentos de videovigilância instalados em linhas de abastecimento de combustível e lojas de conveniência;
- 518/04** – Comunicação de dados relativos a docentes que requereram prestações de desemprego entre duas entidades públicas;
- 519/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade em autarquia;
- 520/04** – Tratamento de dados biométricos (retina do olho) para identificação dos utilizadores de armazém de materiais e peças de desempanagem;
- 521/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa entidade pública;
- 522/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa autarquia;
- 523/04** – Tratamento de dados biométricos (íris) para controlo de assiduidade numa sociedade de construção civil;

- 524/04** – Tratamento de dados biométricos (geometria da mão) para controlo de assiduidade num estabelecimento de ensino superior;
- 525/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade num estabelecimento de ensino superior;
- 526/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade e acesso ao equipamento informático em estabelecimento de ensino superior;
- 527/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa autarquia;
- 528/04** – Comunicação de dados relativos às pensões ilíquidas auferidas pelos pensionistas/inquilinos de casas de renda económica entre entidades públicas;
- 529/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa autarquia;
- 530/04** – Tratamento de videovigilância instalado em autocarros de transporte colectivo de passageiros;
- 531/04** – Tratamento de videovigilância instalado nas bombas de abastecimento de combustível e respectiva loja;
- 532 a 536/04** – Tratamentos de videovigilância instalados em farmácias;
- 537/04** – Tratamento de videovigilância instalado nas bombas de abastecimento de combustível e respectiva loja;
- 538/04** – Tratamento de videovigilância instalado em farmácia;
- 539/04** – Tratamento de videovigilância instalado nas bombas de abastecimento de combustível e respectiva loja;
- 540/04** – Tratamento de videovigilância instalado nas linhas de abastecimento de combustível e lojas de conveniência;
- 541/04** – Tratamento de dados biométricos (geometria da mão) para controlo de assiduidade num instituto público;
- 542 a 546/04** – Tratamento de videovigilância instalado nas linhas de abastecimento de combustível e lojas;

- 547/04** – Tratamento de videovigilância instalado em farmácia;
- 548/04** – Tratamento de videovigilância instalado nas bombas de abastecimento de combustível e respectiva loja;
- 549/04** – Tratamento de videovigilância instalado nas linhas de abastecimento de combustível;
- 550/04** – Tratamento de dados biométricos (íris) para controlo de assiduidade no estaleiro de empresa;
- 551/04** – Tratamento de videovigilância num parque florestal;
- 552 a 560/04** – Base de dados de grupo empresarial para apoiar a gestão financeira de cada empresa do grupo;
- 561/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa junta de freguesia;
- 562/04** – Tratamento relativo à gestão das acções de fiscalização realizadas em unidades hoteleiras e de processos de contra-ordenação;
- 563/04** – Inquérito feito em instituições do ensino superior para dissertação de doutoramento;
- 564/04** – Ficheiro de ensaios clínicos relativos a tratamento de insuficiência cardíaca;
- 565 a 567/04** – Tratamentos de videovigilância em dependências bancárias;
- 568/04** – Tratamento de dados no âmbito de um doutoramento em Didáctica – Formação de Professores;
- 569/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade num governo civil;
- 570/04** – Pedido para alargamento da cedência de dados no âmbito de um tratamento de dados pessoais de um banco;
- 571/04** – Tratamentos de videovigilância numa empresa de restauração;
- 572 a 574/04** – Tratamentos de videovigilância em empresas hoteleiras;
- 575/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade em serviços municipalizados;

- 576/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade num instituto público;
- 577/04** – Tratamento de dados biométricos (íris) para controlo de assiduidade numa empresa de construção civil;
- 578/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade e processamento de vencimentos num estabelecimento hospitalar;
- 579/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade num estabelecimento de ensino superior;
- 580/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa entidade inter-municipal;
- 581/04** – Tratamento de televigilância em Parque Natural;
- 582/04** – Fluxo de dados para os Estados Unidos da América relativo a um tratamento que visa a gestão de um concurso audiovisual;
- 583/04** – Tratamento de televigilância em Parque Natural;
- 584/04** – Tratamento de dados no âmbito do Programa Porta-Bandeira do Euro’2004;
- 585/04** – Tratamento de dados relativo à avaliação do estado de saúde de subscritores de seguros, aceitação e gestão do contrato de seguro;
- 586 a 595/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 596/04** – Tratamento de videovigilância em estações de comboio;
- 597/04** – Tratamento de videovigilância em farmácia;
- 598/04** – Tratamento de videovigilância em estabelecimento comercial;
- 599/04** – Tratamentos de videovigilância em entidade bancária;
- 600 a 602/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 603 e 604/04** – Tratamentos de videovigilância em entidades bancárias;
- 605/04** – Tratamento de videovigilância em farmácia;
- 606/04** – Tratamento de videovigilância em estabelecimento comercial;
- 607/04** – Tratamento de videovigilância em farmácia;
- 608/04** – Tratamento de videovigilância em entidade bancária;

- 609/04** – Tratamento de videovigilância em farmácia;
- 610 e 611/04** – Tratamento de videovigilância em estabelecimentos comerciais;
- 612/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade em instituto público;
- 613/04** – Informatização de dados dos doentes de uma clínica;
- 614/04** – Recolha e tratamento de dados para análise, gestão, atribuição de crédito e realização de marketing;
- 615/04** – Tratamento de dados biométricos (íris) para controlo de acesso a instalações em empresa de telecomunicações;
- 616/04** – Comunicação de dados no âmbito de um tratamento de gestão de clientes;
- 617/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade e processamento de vencimentos em empresa de gestão de cobranças;
- 618/04** – Tratamentos de videovigilância em entidade pública;
- 619/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade e processamento de vencimentos em partido político;
- 620/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade em junta de freguesia;
- 621/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade em autarquia;
- 622/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade em autarquia;
- 623/04** – Tratamento de gestão de clientes e avaliação mínima sobre a origem e proveniência do património/recursos que permita responder aos requisitos legais e à Instrução 48/96 do Banco de Portugal;
- 624/04** – Tratamentos de videovigilância em unidades hoteleiras;
- 625/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa empresa industrial;
- 626 e 627/04** – Tratamentos de videovigilância em estabelecimentos de restauração;

- 628/04** – Tratamento informático dos dados do serviço de saúde e segurança no trabalho em instituto médico;
- 629/04** – Tratamento de videovigilância em estabelecimento comercial;
- 630/04** – Acesso a dados de saúde pela Netsaúde;
- 631/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade num estabelecimento de ensino politécnico;
- 632/04** – Comunicação de dados no âmbito de um tratamento de gestão de clientes de uma empresa financeira;
- 633 a 636/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 637 a 640/04** – Tratamentos de videovigilância em tribunais judiciais;
- 641/04** – Tratamentos de videovigilância em empresa de restauração e hotelaria;
- 642/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa empresa de realização de eventos culturais;
- 643/04** – Tratamento de gestão de pessoal numa autarquia;
- 644/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade em empresa ;
- 645/04** – Tratamentos de videovigilância em bombas de abastecimento de combustível;
- 646/04** – Gestão da informação de controlo de alimentação animal e processamento das respectivas contra-ordenações;
- 647 a 649/04** – Tratamentos de videovigilância em cadeia de hipermercados;
- 650/04** – Tratamento de dados biométricos (impressão digital) para controlo de acessos e assiduidade numa empresa;
- 651/04** – Tratamento de dados destinado a um estudo na área das doenças cardiovasculares;
- 652 a 655/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 656 e 657/04** – Tratamentos de videovigilância em discotecas;
- 658/04** – Tratamento de videovigilância em estabelecimento comercial;

- 659/04** – Tratamento de videovigilância em áreas florestais;
- 660/04** – Tratamento de dados com vista à inscrição em programa de televisão, através da Internet;
- 661/04** – Cedência de dados por parte de centro hospitalar relativos a processos clínicos dos registos operatórios das cirurgias realizadas por cesariana;
- 662/04** – Transmissão de dados para os Estados Unidos de América no âmbito de um tratamento de dados para gestão de e-learning dos trabalhadores de uma empresa;
- 663/04** – Fluxo de dados para os Estados Unidos da América relativos a um tratamento de dados com finalidade de gestão de clientes;
- 664/04** – Tratamento de videovigilância numa junta de freguesia;
- 665/04** – Tratamento de videovigilância nas instalações de uma empresa;
- 666/04** – Transmissão de dados para a Suíça no âmbito de um tratamento para organização de eventos de uma empresa farmacêutica;
- 667 a 670/04** – Tratamentos de videovigilância em instalações comerciais;
- 671/04** – Tratamento de videovigilância nas instalações de um laboratório;
- 672/04** – Tratamento de videovigilância nas instalações de uma empresa;
- 673/04** – Tratamento de videovigilância nas instalações de gare marítima;
- 674/04** – Tratamento de videovigilância em estabelecimento comercial;
- 675/04** – Tratamento de videovigilância em unidade fabril;
- 676/04** – Tratamento de videovigilância em instalações de universidade;
- 677 a 692/04** – Tratamentos de videovigilância em instalações de empresas;
- 693/04** – Tratamento de videovigilância em estações de transportes urbanos;
- 694/04** – Acesso a dados do STAPE por parte de estabelecimento universitário;
- 695 a 827/04** – Tratamentos de videovigilância em bombas de abastecimento de combustível e loja;
- 828/04** – Acesso a dados de saúde pela Netsaúde;
- 829/04** – Tratamento de dados pessoais relativos a cheques sem provisão;

- 830/04** – Tratamento de videovigilância instalado por uma autarquia;
- 831/04** – Prescrição de medicamentos de forma digital no âmbito do tratamento de dados da Netsaúde;
- 832/04** – Tratamento de dados para gestão de pessoal da Região Militar do Sul;
- 833/04** – Investigação para estudo de saídas profissionais de Pós-Graduados de estabelecimento universitário;
- 834/04** – Investigação sobre o impacto das ideias das mães de uma minoria étnica sobre adaptação e desenvolvimento escolar dos filhos;
- 835/04** – Tratamento de videovigilância em zonas florestais da zona do Tâmega;
- 836/04** – Tratamento de videovigilância em área de floresta do Ribatejo;
- 837/04** – Sistema de televigilância na área do Pinhal Interior Centro;
- 838/04** – Gestão de pessoal e gestão da informação dos serviços de segurança, higiene e saúde no trabalho;
- 839/04** – Estudo de dissertação para tese de Doutoramento;
- 840/04** – Tratamento relativo ao sistema de identificação de caninos e felinos;
- 841/04** – Comunicação de dados no âmbito de um tratamento de gestão de recursos humanos;
- 842/04** – Implementação de dois planos de acções destinados aos empregados de empresa de telecomunicações;
- 843/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade num estabelecimento hospitalar;
- 844/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa instituição universitária;
- 845/04** – Sistema de televigilância na área de Paisagem Protegida do Litoral de Esposende;
- 846/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa autarquia;
- 848 a 853/04** – Tratamentos de videovigilância instalados em sedes e armazéns de empresas;

- 854 a 860/04** – Tratamentos de videovigilâncias instalados em autarquias e equipamentos autárquicos;
- 861/04** – Tratamento de videovigilância instalado em entidade pública;
- 862/04** – Tratamento de videovigilância instalado num estádio de futebol de uma associação de municípios;
- 863/04** – Tratamento de videovigilância num estádio de futebol;
- 864 a 866/04** – Tratamentos de videovigilância instalados em farmácias;
- 867/04** – Tratamento de videovigilância nas bombas de abastecimento e respectiva loja;
- 868 a 892/04** – Tratamentos de videovigilância instalados em supermercados, hipermercados e outras instalações comerciais;
- 893 a 898/04** – Tratamentos de videovigilância instalados em departamentos de autarquias;
- 899 a 909/04** – Tratamentos de videovigilância em farmácias;
- 910/04** – Tratamento de videovigilância num laboratório nacional;
- 911/04** – Tratamento de videovigilância nas instalações de uma indústria química;
- 912/04** – Tratamento de videovigilância num museu municipal;
- 913 a 917/04** – Acesso a dados de saúde pela Netsaúde;
- 918/04** – Tratamento de videovigilância nas bombas de abastecimento de combustível, centro de formação, recepção e muro de acesso à EN109;
- 919 a 923/04** – Tratamentos de videovigilância em instalações industriais e comerciais;
- 924/04** – Tratamento de videovigilância em instituto público;
- 925 e 926/04** – Tratamento de videovigilância em estabelecimentos comerciais;
- 927/04** – Tratamento de videovigilância numa galeria de arte;
- 928 a 933/04** – Tratamentos de videovigilância em estabelecimentos e centros comerciais;
- 934/04** – Tratamento de videovigilância instalado numa discoteca;

- 935 a 938/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 939/04** – Tratamentos de videovigilância em instituto público;
- 940 a 944/04** – Tratamentos de videovigilância em estabelecimentos comerciais e armazéns;
- 945/04** – Tratamentos de videovigilância num instituto público;
- 946/04** – Tratamento de videovigilância instalado num estabelecimento comercial;
- 947/04** – Tratamento de videovigilância nas bombas de abastecimento de combustível;
- 948 a 958/04** – Tratamentos de videovigilância em estabelecimentos comerciais e empresas;
- 959/04** – Tratamentos de videovigilância num parque de campismo;
- 960/04** – Tratamento de videovigilância em estabelecimento comercial;
- 961/04** – Cumprimento do disposto nos artigos 13.º-A e 15.º-A da Lei n.º 43/90, designadamente no tocante à tramitação e publicitação das petições recebidas pela Assembleia da República;
- 962/04** – Comunicação de dados por parte de entidade bancária para fins de recuperação de créditos em dívida;
- 963 a 965/04** – Interconexão de dados entre empresas de um grupo financeiro no âmbito de um tratamento de gestão de clientes;
- 966/04** – Sistema de vídeo-conferência com recolha de imagens nas consultas de um estabelecimento hospitalar;
- 967/04** – Tratamentos de gestão de exames laboratoriais em laboratório de patologia clínica;
- 968/04** – Tratamento de dados com a finalidade de corte de lentes;
- 969/04** – Gestão de contra-ordenações cometidas no âmbito dos recursos florestais;
- 970/04** – Tratamentos de videovigilância em equipamentos de lazer;
- 971/04** – Tratamentos de videovigilância instalados num bar;
- 972/04** – Tratamento de videovigilância em dois parques comerciais;

- 973/04** – Tratamento de videovigilância em centro comercial e áreas envolventes;
- 974/04** – Tratamentos de videovigilância em estabelecimentos de restauração;
- 975/04** – Tratamento de videovigilância em instalações de empresa;
- 976/04** – Investigação científica sobre adolescentes e crianças inscrita num projecto de doutoramento em psicologia;
- 977/04** – Tratamento para licenciamento de transportadores de animais vivos;
- 978/04** – Tratamento relativo a gestão de clientes em empresa distribuidora de gás;
- 979/04** – Tratamento de dados pessoais relativo aos actos anestésicos para gestão do serviço num estabelecimento hospitalar;
- 981/04** – Tratamento de videovigilância num estabelecimento de ensino superior;
- 982/04** – Tratamento de videovigilância instalado num centro comercial;
- 983/04** – Tratamentos de videovigilância nas instalações de uma empresa;
- 984/04** – Tratamento de dados com finalidade de promoção de operações de marketing e vendas à distância, telemarketing e Internet;
- 985/04** – Cedência de dados na sequência de contrato de cessão de créditos;
- 986/04** – Gestão de recursos humanos e registo de sanções disciplinares;
- 987/04** – Tratamentos de videovigilância em empresa de exploração hoteleira;
- 988/04** – Gestão do serviço de Medicina do Trabalho, de acidentes em serviço e prestação de cuidados de saúde e serviços de enfermagem;
- 989/04** – Tratamento relativo a gestão de pessoal e registo de sanções disciplinares;
- 990/04** – Comunicação de dados a subsistemas de saúde por parte de estabelecimento hospitalar para efeitos de facturação;
- 991/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade e processamento de vencimentos numa autarquia;
- 992/04** – Tratamento referente à gestão de um estabelecimento de ensino;
- 993/04** – Tratamentos de videovigilância em instalações de entidade portuária;
- 994 a 999/04** – Tratamentos de videovigilância em instalações empresariais e comerciais;

- 1000/04** – Tratamento de videovigilância numa residência particular;
- 1001/04** – Tratamento de videovigilância numa empresa de animação cultural;
- 1002/04** – Tratamento de videovigilância instalado num estaleiro;
- 1003 e 1004/04** – Tratamento de videovigilância em instalações empresariais;
- 1005/04** – Tratamentos de videovigilância em empresa de restauração;
- 1006/04** – Tratamento de videovigilância em instalações empresariais;
- 1007/04** – Tratamentos de videovigilância em firma de actividades hoteleiras;
- 1008/04** – Tratamento de videovigilância instalado numa farmácia;
- 1009/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1010/04** – Tratamento de videovigilância em instalações empresariais;
- 1011 a 1014/04** – Tratamentos de videovigilância instalados em tribunais;
- 1015/04** – Tratamentos de videovigilância em empresa de actividades turísticas;
- 1016/04** – Tratamento de videovigilância em instalações empresariais;
- 1017/04** – Tratamento de videovigilância em instalações comerciais;
- 1018/04** – Tratamentos de videovigilância numa sociedade hoteleira;
- 1019 a 1022/04** – Tratamentos de videovigilância em instalações empresariais;
- 1023/04** – Tratamentos de videovigilância em centro comercial;
- 1024 a 1028/04** – Tratamento de videovigilância em instalações comerciais;
- 1029/04** – Tratamento de videovigilância em instituto público;
- 1030/04** – Tratamento de dados biométricos (impressão digital) para controlo de acessos em instituto público;
- 1031 e 1032/04** – Tratamentos de videovigilância em superfícies comerciais;
- 1033/04** – Tratamentos de videovigilância instalados em empresa de restauração;
- 1034 a 1037/04** – Tratamentos de videovigilância instalados em instituições judiciais;
- 1038/04** – Tratamento de videovigilância em instalações comerciais;
- 1039/04** – Tratamento de videovigilância numa farmácia;

- 1040/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade em estabelecimento de ensino superior;
- 1041/04** – Tratamento de videovigilância em bombas de combustível e respectiva loja;
- 1042 a 1045/04** – Tratamentos de videovigilância em instalações empresariais;
- 1046 a 1050/04** – Tratamentos de videovigilância em instalações comerciais;
- 1051/04** – Tratamento de videovigilância numa sociedade hoteleira;
- 1052 e 1053/04** – Tratamentos de videovigilância em superfícies comerciais;
- 1054/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1055 e 1056/04** – Tratamentos de videovigilância em bombas de abastecimento de combustível e respectivas lojas;
- 1057 e 1058/04** – Fluxo de dados para os Estados Unidos da América no âmbito de tratamentos de dados destinados a gerir recursos humanos;
- 1059/04** – Tratamento para recolha e gestão de dados de profissionais de saúde para participação em eventos científicos;
- 1060/04** – Comunicação de dados sobre rádios regionais, radioamadores e utilizadores da Banda do Cidadão, por parte de autarquia, com a finalidade de desenvolvimento de Plano Municipal de Emergência no âmbito da protecção civil;
- 1061/04** – Acesso a dados do STAPE por parte de autarquia;
- 1062/04** – Tratamento de videovigilância em superfície comercial;
- 1063 a 1066/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 1067/04** – Tratamento de videovigilância em bombas de abastecimento de combustível e respectiva loja;
- 1068/04** – Tratamento de videovigilância em superfície comercial;
- 1069/04** – Tratamento de videovigilância em instalações empresariais;
- 1070/04** – Tratamento de videovigilância em bombas de abastecimento de combustível e respectiva loja;

- 1071/04** – Tratamento de videovigilância em superfície comercial;
- 1072 e 1073/04** – Tratamento de videovigilância em estabelecimentos comerciais;
- 1074/04** – Tratamentos de videovigilância em estabelecimento hoteleiro;
- 1075/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade em associação industrial;
- 1076/04** – Tratamento de videovigilância em instalações empresariais;
- 1077/04** – Tratamento de videovigilância em entidade bancária;
- 1078/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1079/04** – Tratamento de videovigilância em instalações empresariais;
- 1080 a 1082/04** – Tratamentos de videovigilância instalados em instituições judiciais;
- 1083/04** – Tratamento de videovigilância em instalações empresariais;
- 1084/04** – Tratamento de videovigilância em entidade bancária;
- 1085/04** – Tratamentos de videovigilância em estabelecimento comercial;
- 1086/04** – Tratamentos de videovigilância em estabelecimento hoteleiro;
- 1087/04** – Tratamentos de videovigilância em estabelecimento comercial;
- 1088/04** – Tratamentos de videovigilância em estabelecimento hoteleiro;
- 1089/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1090 e 1091/04** – Tratamentos de videovigilância em instalações empresariais;
- 1092 a 1103/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 1104/04** – Tratamento de dados com a finalidade de avaliar a qualidade do serviço de atendimento numa empresa de telecomunicações;
- 1105/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1106/04** – Tratamento de videovigilância num consultório de medicina dentária;
- 1107 a 1109/04** – Tratamento de videovigilância em instalações comerciais;
- 1110/04** – Tratamento de videovigilância nas estações e carruagens de comboios suburbanos do Grande Porto e da Grande Lisboa;
- 1111 a 1113/04** – Tratamento de videovigilância em instalações comerciais;

- 1114/04** – Tratamentos de videovigilância num parque residencial;
- 1115/04** – Tratamentos de videovigilância em instalações empresariais;
- 1116/04** – Tratamento de videovigilância num centro de artes;
- 1117/04** – Tratamento de videovigilância numa residência particular;
- 1118/04** – Tratamento de videovigilância nas instalações de entidade associativa;
- 1119/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1120/04** – Tratamento de videovigilância em instalações empresariais;
- 1121 a 1123/04** – Tratamentos de videovigilância instalados em entidades públicas;
- 1124/04** – Tratamentos de videovigilância em instalações empresariais;
- 1125/04** – Tratamento de videovigilância em estabelecimento de ensino superior;
- 1126/04** – Tratamentos de videovigilância em instalações empresariais;
- 1127/04** – Tratamento de videovigilância num centro hospitalar;
- 1128/04** – Tratamento de videovigilância instalados em instituto público;
- 1129/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa autarquia;
- 1130/04** – Tratamento de videovigilância em instalações empresariais;
- 1131/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1132/04** – Tratamento de videovigilância numa autarquia;
- 1133/04** – Tratamento de videovigilância nas instalações de zona de lazer;
- 1134/04** – Tratamento de videovigilância em instalações empresariais;
- 1135/04** – Tratamento de videovigilância num estabelecimento escolar;
- 1136 a 1138/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 1139/04** – Tratamento de videovigilância em residência particular;
- 1140/04** – Tratamento de videovigilância nas instalações de um instituto de investigação científica;
- 1141 e 1142/04** – Tratamentos de videovigilância em instalações empresariais;
- 1143/04** – Tratamento de videovigilância num estabelecimento escolar;

- 1144/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1145 e 1146/04** – Tratamentos de videovigilância em instalações empresariais;
- 1147/04** – Tratamento de videovigilância nas instalações de um instituto de investigação científica de uma universidade;
- 1148 e 1149/04** – Tratamentos de videovigilância em instalações empresariais;
- 1150 a 1153/04** – Tratamentos de videovigilância em estabelecimentos escolares;
- 1154 a 1156/04** – Tratamentos de videovigilância em instalações empresariais;
- 1157/04** – Tratamento de dados biométricos (impressão digital) para controlo de acesso a piscinas municipais;
- 1158/04** – Transferência de dados para os Estados Unidos de América no âmbito de um tratamento de dados biométricos (impressão digital) para acesso ao sistema informático de uma empresa;
- 1159/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1160/04** – Tratamento de videovigilância em instituto público;
- 1161/04** – Tratamentos de videovigilância em instalações industriais;
- 1162/04** – Tratamento de videovigilância em entidade pública ligada à educação;
- 1163/04** – Tratamento de videovigilância em instalações empresariais;
- 1164/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 1165/04** – Tratamento de videovigilância em residência particular;
- 1166/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1167/04** – Tratamento de videovigilância em instalações empresariais;
- 1168 e 1169/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 1170/04** – Tratamento de videovigilância em sede de sindicato;
- 1171/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1172/04** – Tratamento de videovigilância em estabelecimento escolar;
- 1173 a 1177/04** – Tratamento de videovigilância em instalações empresariais;
- 1178/04** – Tratamentos de videovigilância instalados num casino;

- 1179/04** – Tratamento de videovigilância em funcionamento num museu;
- 1180/04** – Tratamento de videovigilância em instalações empresariais;
- 1181/04** – Tratamento de videovigilância num estabelecimento de ensino superior;
- 1182 a 1184/04** – Tratamentos de videovigilância em instalações empresariais;
- 1185/04** – Tratamento de videovigilância em agrupamento de escolas;
- 1186/04** – Tratamentos de videovigilância em entidades judiciais;
- 1187 e 1188/04** – Tratamentos de videovigilância em funcionamento em pedreiras;
- 1189/04** – Tratamentos de videovigilância em estabelecimento comercial;
- 1190 e 1191/04** – Tratamentos de videovigilância em instalações empresariais;
- 1192/04** – Tratamento de videovigilância instalado num sindicato;
- 1193/04** – Tratamentos de videovigilância instalados em estabelecimento de ensino superior;
- 1194/04** – Tratamento de videovigilância instalado numa entidade privada;
- 1195 a 1199/04** – Tratamentos de videovigilância em instalações empresariais;
- 1200/04** – Tratamento de videovigilância em residência particular;
- 1201 a 1203/04** – Tratamentos de videovigilância em instalações empresariais;
- 1204 a 1206/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 1207/04** – Tratamento de videovigilância em instalações empresariais;
- 1208 e 1209/04** – Tratamentos de videovigilância em estabelecimentos de restauração;
- 1210/04** – Tratamento de videovigilância em estabelecimento de ensino superior;
- 1211/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 1212/04** – Tratamento de videovigilância em bombas de abastecimento de combustível;
- 1213/04** – Tratamento de videovigilância num organismo público;
- 1214 a 1217/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 1218 e 1219/04** – Tratamentos de videovigilância em entidades judiciais;

- 1220/04** – Tratamentos de videovigilância num estabelecimento hoteleiro;
- 1221 a 1224/04** – Tratamentos de videovigilância em instalações bancárias;
- 1225/04** – Sistema de videovigilância instalado num condomínio;
- 1226/04** – Gestão de pessoal e cadastro dos funcionários de uma empresa de transportes urbanos;
- 1227/04** – Sistema de videovigilância instalado num condomínio;
- 1228/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1229/04** – Tratamento de videovigilância em instalações empresariais;
- 1230 a 1232/04** – Tratamentos de videovigilância em entidades judiciais;
- 1233/04** – Tratamento de videovigilância instalado numa entidade bancária;
- 1234/04** – Tratamento de videovigilância em hipermercado;
- 1235/04** – Tratamento de videovigilância instalado numa entidade bancária;
- 1236/04** – Tratamento de videovigilância em hipermercado;
- 1237 e 1238/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 1239/04** – Sistema de videovigilância instalado numa garagem;
- 1240/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa instituição de solidariedade social e de ensino;
- 1241 e 1242/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 1243/04** – Tratamento de videovigilância numa associação de bombeiros voluntários;
- 1244/04** – Tratamento de videovigilância numa casa de saúde;
- 1245 a 1247/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 1248/04** – Gestão de clientes e promoção de acções de marketing numa empresa de comércio e aluguer de bens e serviços;
- 1249/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa empresa;
- 1250/04** – Tratamento de videovigilância em instalações empresariais;
- 1251 a 1253/04** – Tratamentos de videovigilância em estabelecimentos comerciais;

- 1254/04** – Tratamento de videovigilância em instalações empresariais;
- 1255/04** – Tratamento de videovigilância instalado nas linhas de abastecimento de combustível e garagem;
- 1256/04** – Tratamento de videovigilância instalado num terminal de contentores;
- 1257/04** – Tratamento de videovigilância instalado em linhas de abastecimento de combustível e loja;
- 1258/04** – Tratamento de videovigilância em estabelecimento escolar;
- 1259 e 1260/04** – Tratamentos de videovigilância em superfícies comerciais;
- 1261/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1262/04** – Tratamento de videovigilância em superfície comercial;
- 1263/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa instituição bancária;
- 1264/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa autarquia;
- 1265/04** – Tratamento de videovigilância numa residência particular;
- 1266/04** – Tratamento de videovigilância em instalações empresariais;
- 1267/04** – Tratamento de videovigilância instalado numa farmácia;
- 1268/04** – Tratamento de videovigilância no estabelecimento de uma associação naval;
- 1269 a 1271/04** – Tratamentos de videovigilância em estabelecimentos comerciais;
- 1272/04** – Tratamento de videovigilância numa imobiliária;
- 1273/04** – Tratamento de videovigilância num estabelecimento de restauração;
- 1274/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1275/04** – Tratamento de videovigilância num estabelecimento de restauração;
- 1276/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1277 a 1286/04** – Tratamentos de videovigilância em bombas de abastecimento de combustível e respectivas lojas;
- 1287/04** – Tratamento de videovigilância em instalações fabris;

- 1288/04** – Interconexão entre os tratamentos de dados da Base de Dados do Recenseamento Eleitoral e da Caixa Geral de Aposentações;
- 1289/04** – Tratamento de videovigilância em instalações empresariais;
- 1290 e 1291/04** – Tratamentos para constituição de ficheiro de clientes de entidades bancárias;
- 1292/04** – Gestão de recursos humanos e registo de sanções disciplinares em entidade pública;
- 1293/04** – Gestão de recursos humanos e registo de sanções disciplinares num estabelecimento hospitalar;
- 1294/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa empresa;
- 1295/04** – Tratamento informatizado dos dados da celebração de contratos de crédito numa empresa de aluguer de viaturas;
- 1296/04** – Gestão do serviço de Medicina do Trabalho numa entidade portuária;
- 1297/04** – Comunicação de dados de uma entidade privada para uma pública ligada ao sector da saúde e tratamento dos mesmos pela segunda;
- 1298/04** – Cedência de dados pessoais no âmbito de uma operação de titularização de créditos;
- 1299/04** – Tratamentos realizados no âmbito da gestão de exames laboratoriais;
- 1300/04** – Tratamentos de videovigilância em instalações fabris;
- 1301/04** – Tratamento de videovigilância em estabelecimento comercial;
- 1302 a 1305/04** – Tratamentos de videovigilância em instalações empresariais;
- 1306/04** – Tratamento de videovigilância em estabelecimento de ensino;
- 1307/04** – Tratamento de videovigilância numa associação industrial;
- 1308/04** – Tratamentos de videovigilância numa firma de hotelaria e restauração;
- 1309/04** – Tratamento de videovigilância em escritórios de empresa;
- 1310 e 1311/04** – Tratamentos de videovigilância em instalações empresariais;
- 1312/04** – Tratamentos de videovigilância em estabelecimentos comerciais;

- 1313/04** – Tratamento de videovigilância em instalações empresariais;
- 1314/04** – Tratamento de videovigilância numa farmácia;
- 1315/04** – Tratamento de videovigilância em instalações empresariais;
- 1316/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa empresa;
- 1317/04** – Tratamento de videovigilância numa empresa de transportes rodoviários;
- 1318/04** – Tratamento de videovigilância em instalações empresariais;
- 1319/04** – Sistema de televigilância no Parque Natural da Serra de S. Mamede;
- 1320/04** – Sistema de televigilância na floresta da encosta poente da Serra de Sintra;
- 1321 a 1323/04** – Tratamentos de videovigilância em instalações empresariais;
- 1324/04** – Tratamento de videovigilância instalado numa farmácia;
- 1325/04** – Tratamento de videovigilância num estabelecimento hospitalar;
- 1326 a 1328/04** – Tratamentos de videovigilância em instalações empresariais;
- 1329/04** – Tratamento de videovigilância em bombas de abastecimento de combustível e respectiva loja;
- 1330/04** – Tratamentos de videovigilância em estabelecimento comercial;
- 1331/04** – Tratamento para avaliação de funcionários com vista à sua mobilidade na empresa e/ou Grupo;
- 1332/04** – Tratamento de dados biométricos (impressão digital) para controlo de assiduidade numa empresa;
- 1333/04** – Tratamentos de videovigilância em instalações empresariais;
- 1334/04** – Cedência de dados no âmbito de uma operação de titularização de créditos;
- 1335/04** – Registo e identificação de transgressores no exercício da caça para processamento de contra-ordenações;
- 1336/04** – Tratamento de dados para controlo, certificação e defesa da denominação de origem do vinho “Douro”, envio de informação e controlo das declarações de produção e de existência de mosto e vinho;

- 1337/04** – Tratamento para avaliação do desempenho dos trabalhadores de uma empresa;
- 1338/04** – Tratamento de videovigilância instalado numa residência particular;
- 1339/04** – Tratamento de videovigilância num estabelecimento de restauração;
- 1340/04** – Tratamento de videovigilância em instalações empresariais;
- 1341/04** – Tratamento de videovigilância num estabelecimento de restauração;
- 1342/04** – Acesso a dados pessoais por parte de um associado de associação de moradores.

3 – Pareceres

- 1/04** – Projecto de Decreto-Lei autorizado relativo à interconexão de dados entre a administração fiscal e a segurança social;
- 2/04** – Projecto de Decreto-Lei relativo às formalidades de declaração exigidas dos navios à chegada e/ou partida de portos dos Estados-Membros da Comunidade;
- 3/04** – Projecto de diploma que visa regulamentar a entrada, permanência, saída e afastamento de estrangeiros do território nacional;
- 4/04** – Projecto de Decreto-Lei que cria o PROHABITA – Programa de Financiamento para Acesso à Habitação;
- 5/04** – Diploma que modifica o regime jurídico aplicável às alterações dos termos das autorizações de introdução no mercado de medicamentos de uso humano;
- 6/04** – Projecto de Decreto-Lei autorizado relativo à interconexão de dados entre a administração fiscal e a segurança social;
- 7/04** – Projecto de Decreto-Lei sobre ensaios clínicos com medicamentos de uso humano;
- 8/04** – Alteração ao artigo 6.º do Decreto-Lei n.º 198/90, de 19 de Junho relativo ao regime de isenção de imposto sobre valor acrescentado nas vendas de

mercadorias efectuadas a exportadores nacionais que, não lhes sendo entregues, são exportadas no mesmo estado;

- 9/04** – Projecto de Decreto-Lei relativo ao enquadramento legal dos sistemas de vigilância epidemiológica referentes à saúde humana;
- 10/04** – Proposta de Lei n.º 117/IX/2.^a (GOV) que visa aprovar medidas preventivas e punitivas a adoptar em caso de manifestações de violência associadas ao desporto;
- 13/04** – Projecto de protocolo de cooperação e coordenação de procedimentos entre administração fiscal e as instituições de segurança social;
- 14/04** – Projecto de diploma que institui o número de identificação fiscal, bem como as condições da sua atribuição, respectivos efeitos e a sua gestão;
- 15/04** – Anteprojecto de Decreto-Lei tendente a regulamentar os ficheiros de dados de gestão processual automatizados dos Tribunais e serviços do Ministério Público;
- 16/04** – Projecto de Decreto-Lei que regula o acesso à profissão de podologista;
- 17/04** – Proposta de Lei n.º 122/IX/2.^a que autoriza o Governo a legislar sobre a possibilidade de utilização nas salas de jogos dos casinos de equipamento electrónico de vigilância e controlo, como medida de protecção de pessoas e bens;
- 18/04** – Nova versão do projecto de Decreto-Lei relativo ao regime de infracções no sector vitivinícola e respectiva autorização legislativa, na sequência do parecer n.º 33/03;
- 19/04** – Convenção n.º 185 da Conferência Geral da Organização Internacional do Trabalho relativa à revisão da Convenção sobre os Documentos de Identificação dos Marítimos – 1958;
- 20/04** – Possibilidade de cedência de dados, por parte do Instituto Nacional de Emergência Médica, às autoridades judiciais, bem como órgãos de polícia criminal, sem que para tal seja junto um despacho fundamentado daquelas autoridades;
- 21/04** – Pedido feito pela Câmara do Porto relativamente ao acesso à identificação fiscal dos contribuintes residentes naquele concelho;

- 22/04** – Projecto de Decreto-Lei que procede à regionalização do Sistema Fiscal na Região Autónoma da Madeira;
- 23/04** – Projecto de Decreto-Lei que disciplina as condições de acesso e análise, em tempo real, da informação pertinente para a investigação de crimes tributários, branqueamento de capitais e financiamento de terrorismo, pela Polícia Judiciária, a administração fiscal e as instituições da Segurança Social;
- 24/04** – Nova versão do projecto de diploma relativo ao regime de infracções no sector vitivinícola, na sequência dos pareceres n.º 33/03 e 18/04;
- 25/04** – Proposta de Lei n.º 116/IX sobre ensaios clínicos com medicamentos de uso humano;
- 26/04** – Projecto de diploma que, no uso da autorização legislativa concedida pela Lei n.º 8/2004, de 10 de Março, regula o exercício das actividades de mediação imobiliária e de angariação imobiliária;
- 27/04** – Projecto de Proposta de Lei que define o regime de prova digital electrónica;
- 28/04** – Projecto de Decreto-Lei que estabelece o regime jurídico da conservação, fomento e exploração dos recursos cinegéticos;
- 29/04** – Novo parecer sobre o projecto de Proposta de Lei que define o regime de prova digital electrónica;
- 30/04** – Projecto de Lei n.º 425/IX relativo à Lei de Organização e Funcionamento da Comissão Nacional de Protecção de Dados;
- 31/04** – Projecto de Lei n.º 464/IX/2.º (CDS/PP) que regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum;
- 32/04** – Pedidos de acesso à base de dados de identificação civil, através da linha de transmissão de dados, pelo Serviço de Estrangeiros e Fronteiras, pela Polícia de Segurança Pública e pela Guarda Nacional Republicana;
- 33/04** – Projecto de protocolo a celebrar entre a Direcção-Geral dos Registos e Notariado e o Instituto de Gestão Informática e Financeira da Saúde;

- 34/04** – Projecto que aprova a lei orgânica do Instituto Nacional do Consumidor
- 35/04** – Proposta búlgara de Acordo Bilateral entre o Governo da República da Bulgária e o Governo da República Portuguesa em matéria de cooperação policial;
- 36/04** – Anteprojecto de diploma relativo à criação da Base de Dados da Adopção
- 37/04** – Proposta de Lei n.º 140/IX que autoriza o Governo a alterar o regime jurídico do arrendamento urbano;
- 38/04** – Projecto de diploma que estabelece o regime jurídico do Sistema do Cartão de Utente do Serviço Nacional de Saúde;
- 39/04** – Projecto de Decreto-Lei que aprova o Sistema de Informações Operacionais da Polícia de Segurança Pública;
- 40/04** – Protocolo de 2003 à Convenção Internacional para a Constituição de um Fundo Internacional para a Compensação dos prejuízos devidos à Poluição dos Hidrocarbonetos;
- 41/04** – Alterações à proposta de Lei que autoriza o Governo a alterar o regime jurídico do arrendamento urbano;
- 42/04** – Projecto de acordo entre a República Portuguesa e a Confederação Suíça para a readmissão de pessoas em situação irregular.