

COLÓQUIO

OS DIREITOS DOS CIDADÃOS FACE AOS SISTEMAS DE INFORMAÇÃO POLICIAL

Centro Cultural de Belém
Lisboa
30 Junho 98

Programa

9.30 h – **Inscrição dos participantes**

10.00h – **Sessão de abertura**

Armando Vara – Secretário de Estado Adjunto do Ministro da
Administração Interna

Augusto Victor Coelho – Presidente da Comissão Nacional de
Protecção de Dados Pessoais
Informatizados

João Labescat – Presidente da Autoridade de Controlo Comum de
Schengen

10.45 h – Pausa para Café

11.00 h – **A experiência do Sistema de Informação Schengen e os
direitos dos cidadãos**

*O papel da Autoridade de Controlo Comum (ACC) de Schengen
na defesa dos direitos dos cidadãos” – **João Labescat** –
Presidente da Autoridade de Controlo Comum de Schengen*

*A integração de Schengen na União Europeia – **Nuno Piçarra** –
Coordenador Nacional para os Assuntos da Livre Circulação de
Pessoas no Espaço Europeu*

*O Sistema de Informação Schengen: a importância da cooperação
entre os Estados– **Frank Demot** – Presidente do Grupo Central de
Schengen*

*A protecção de dados na coordenação da informação nacional e na
comunicação entre os Estados – **Ester Guedes** – Coordenadora do
Gabinete SIRENE Português.*

12.00 h – Debate

12.30 h – Intervalo para almoço

14.30 h – **Os sistemas de informação policial: como conciliar segurança e liberdade?**

A integração dos sistemas de informação policial – **Fernando Negrão** – Director-Geral da Polícia Judiciária

A protecção de dados e a Europol – **Willy Bruggeman** – Coordenador Adjunto, Unidade de Estupefacientes da Europol

Sistemas de informação policial na União Europeia – **Charles Elsen** – Director-Geral da DG H – Justiça e Assuntos Internos, Conselho da União Europeia

15.30 h – Debate

16.30 h – Encerramento do Colóquio

INTRODUÇÃO

Ao promover o Colóquio “Os Direitos dos Cidadãos, Face aos Sistemas de Informação Policial”, com especial incidência na experiência de Schengen, a Autoridade de Controlo Comum, em cooperação com a Comissão Portuguesa de Protecção de Dados, pretendeu dar um contributo para um melhor conhecimento do modo como funciona o primeiro sistema de informação comum europeu de âmbito policial, dos direitos e dos princípios que o balizam, bem como aprofundar alguns aspectos práticos que, apesar de legalmente estatuídos, ainda se encontram por implementar.

Foi propositada a intenção de juntar na experiência comum, representantes de organismos executivos e da ACC, a troca de informações comuns e o futuro enquadramento da Europol, com a situação nacional na óptica dos direitos.

No fundo todos os sistemas comuns dependem, no seu grau de eficácia, da boa estruturação da informação a nível nacional.

A integração de Schengen na União Europeia e o avanço de mais sistemas comuns em diferentes áreas (Europol, Eurodac, aduaneiro) constitui uma verdadeira transformação do panorama existente em 1998.

Esperamos que os próximos anos signifiquem, ao mesmo tempo, maior segurança europeia, mas com plenos direitos e com respeito pela liberdade, questão essencial ao futuro da Europa e da humanidade, no novo século.

Lisboa, 30 de Junho de 1998

João Labescat

Presidente
da Autoridade de Controlo Comum de Schengen

ACTAS

Sessão de abertura

Armando Vara

Secretário de Estado Adjunto
do Ministro da Administração Interna

Exm^{os} Senhoras e Senhores,

É com imenso gosto que participo neste colóquio «Os direitos dos cidadãos face aos sistemas de informação policial» e que, convosco, reflicto sobre um tema de grande interesse para uma sociedade democrática consolidada como a nossa.

Um tema que envolve duas componentes essenciais das democracias modernas: a liberdade e a segurança. A liberdade, que permite o pleno exercício dos nossos direitos de cidadania. A segurança, que é condição de exercício da própria liberdade. Uma liberdade que viva sob a ameaça não se pode exprimir. Permanece um simples estado de espírito. Segurança sem liberdade é ditadura, logo, uma contradição. Porque em ditadura ninguém se sente seguro.

Liberdade e segurança ganham, pois, sentido em democracia. Da harmoniosa conjugação de ambos resulta uma democracia mais robusta, livre e plural.

Este o enquadramento que me parece adequado para um fórum que debate direitos de cidadania e sistemas de informação policial. Porque, se é verdade que vivemos num tempo em que os direitos se alargam, mercê do próprio aprofundamento da democracia, também é verdade que este alargamento aumenta as responsabilidades de quem deve garantir a estabilidade e a segurança do sistema onde se exercem esses direitos.

Se é verdade que as modernas tecnologias, designadamente no campo da telemática, abrem enormes espaços de liberdade, dando aos cidadãos novos e mais sofisticados meios de exercício dos seus direitos, também é verdade

que estes mesmos meios permitem desvios susceptíveis de interferir com o próprio exercício da liberdade e de ferir a legítima ordem legal instituída. Por isso se torna fundamental que esses amplos espaços de liberdade estejam devidamente enquadrados por normas de segurança capazes de impedir os desvios e de garantir estabilidade e legitimidade ao exercício dos direitos de cidadania.

Mas, ao mesmo tempo que se torna imprescindível que a segurança do sistema seja garantida, também se torna necessário impedir que ela ultrapasse a fronteira da liberdade, para que as garantias de segurança não se transformem em ameaças. Para que a segurança não se faça à custa da liberdade e da dignidade de cada um.

Minhas Senhores e meus Senhores,

É por isso que, ao abrir-se este colóquio organizado pela Autoridade de Controlo Comum (instituída pela Convenção de Aplicação do Acordo de Schengen e que tem a cargo a tarefa específica de verificação da boa execução das suas disposições no âmbito do Sistema de Informação Schengen), gostaria de sublinhar a grande importância do tema que aqui irá ser analisado, no contexto de uma sociedade democrática aberta e plural, que constantemente deve dar passos seguros para encontrar o justo equilíbrio entre a firme salvaguarda dos direitos, liberdades e garantias dos cidadãos e a importância de aceder a informações relevantes, em particular daquelas que possam interessar ao sistema de informação policial.

Sendo evidente que o crescente grau de organização e de internacionalização das actividades ilegais, no campo do tráfico de droga, de armas, de veículos, de pessoas, das redes de apoio à imigração ilegal, requer uma resposta pronta e eficaz por parte das diferentes forças policiais – o que obviamente implica o reconhecimento da possibilidade de recurso às mais modernas técnicas de recolha, tratamento e difusão de informações, no plano interno como no plano externo -, é também imperioso reconhecer, de igual forma, que grandes esforços têm vindo, paulatinamente, a ser realizados no sentido de consagrar legalmente todo um conjunto de mecanismos que, na prática, salvaguardem o direito à preservação da intimidade ou da vida privada dos cidadãos, enquanto potenciais titulares de dados que possam ser objecto de tratamento automatizado.

Este reconhecimento conhece já um vasto suporte institucional: 1) na nossa Constituição (artº 35º); 2) na Convenção europeia para a protecção das pessoais relativamente ao tratamento automatizado de dados de carácter pessoal (1981), que é tida como o instrumento jurídico internacional mais importante no campo do uso de dados pessoais; 3) na Recomendação R(87)15, do Comité dos Ministros do Conselho da Europa (1987), que veio clarificar a forma de aplicação correcta daquela Convenção, designadamente no que respeita à utilização dos dados pessoais na actividade policial; 4) na Lei de protecção de dados pessoais face à informática (Lei 10/91 de 29 de Abril); 5) nos diferentes regulamentos aplicáveis nesta matéria às Forças e Serviços de segurança; e, ainda, nouro plano, 6) nos artºs 114 e 115 da

Convenção de Aplicação do Acordo de Schengen; 7) nas Disposições Comuns relativas ao tratamento das informações, constantes da Convenção EUROPOL, já ratificada por Portugal; e 8) em vários outros instrumentos existentes no âmbito da União Europeia, designadamente Recomendações e Resoluções aprovadas pelo Conselho, bem como Convenções que têm vindo a ser desenvolvidas no âmbito da cooperação policial e judiciária, sendo de sublinhar, entre elas, o Sistema de Informação Aduaneiro e a EURODAC.

De todo este acervo de garantias configuradas institucionalmente resulta a clara consagração de alguns direitos fundamentais para o pleno e livre exercício da cidadania: **1) o Direito à Informação e ao Acesso** aos dados pessoais constantes de registos informáticos (artº 13 da Lei 10/91, de 29 de Abril), que dá ao cidadão a faculdade de ser informado quanto à existência de ficheiros relativos à sua pessoa, de ser esclarecido quanto à sua finalidade e de ter conhecimento da identidade e endereço da entidade responsável pela sua gestão; **2) O Direito de Contestação**, relativamente a todo o tipo de informações pessoais que considere incorrectas, incompletas ou omissas e que inclui o direito de peticionar a eliminação daquelas que, na sua perspectiva, forma recolhidas por recurso a meios ilícitos ou enganosos (CFR. Artº 30º da Lei 10/91, bem como a al.C do artº 8º da Convenção Europeia em uestão); e ainda **3) O Direito de Actualização**, consubstanciado no dever que o Responsável pela gestão de suportes informáticos tem de zelar pela exactidão e actualidade dos dados pessoais que foram objecto de tratamento informático (artº 14º da lei 10/91, e al. D do artº 5º da Convenção Europeia)

Para que estes direitos não constituam letra morta, mas, antes, ganhem efectiva consistência, torna-se necessário fixar um conjunto de princípios directores que enquadrem toda a actividade das instâncias responsáveis pela gestão do sistema e que garantam efectivamente: a) publicidade e transparência em relação à existência de ficheiros automatizados; b) a recolha lícita e não enganosa dos dados pessoais; c) a clara e prévia definição das finalidades que presidem à recolha de dados e constituição, e ainda d) a rigorosa limitação da sua utilização.

Para garantir uma observância efectiva dos direitos e princípios que atrás enunciei foram instituídas, nos planos nacional e internacional, algumas entidades independentes, isto é, com membros que não estão directa ou indirectamente relacionados com as entidades responsáveis pela gestão e tratamento de ficheiros.

Assim, no plano interno, à Comissão Nacional de Protecção de Dados Pessoais Informatizados – desiganda, no âmbito da Convenção de Aplicação do Acordo de Schengen, como a autoridade nacional de controlo sobre a parte nacional do Sistema de Informação Schengen -, compete controlar o processamento automatizado de dados pessoais, para assegurar o integral respeito dos direitos, liberdades e garantias consagradas na Constituição e na lei; no plano externo, e no quadro da Convenção de Aplicação do Acordo de Schengen, foi instituída uma Autoridade de Controlo Comum, a quem incumbe a execução da terefa a que já me referi, sendo certo que também no

âmbito da União Europeia, através da Comissão Europeia para a Protecção de dados, foram levadas a cabo diversas iniciativas no sentido da harmonização das regras substanciais e processuais que, em matéria de protecção de dados pessoais, se encontram já previstas em diferentes Convenções instituídas no quadro do terceiro pilar.

Estamos, pois, perante um sistema que prevê mecanismos capazes de conciliar, de um modo equilibrado, a salvaguarda dos direitos, liberdades e garantias fundamentais dos cidadãos e a necessidade crescente de comunicar e de aceder à informação, por parte dos serviços policiais.

Contudo, e não obstante o longo caminho já percorrido desde a década de 70, período a partir do qual se começaram a levantar as questões relacionadas com a protecção de dados pessoais, para o cidadão comum persistem ainda as questões que me parece estarem na origem deste colóquio, sobretudo no plano do conhecimento – deficiente – dos direitos que assistem ao cidadão, bem como dos mecanismos que já existem para os tornar efectivos.

Neste sentido, é importante informar e consciencializar os cidadãos dos direitos que os assistem em matéria de protecção de dados pessoais, sem perder de vista a necessidade de, igualmente, assegurar a capacidade operacional das polícias, na observância dos princípios da liberdade, da segurança e do Estado de Direito, pilares da sociedade portuguesa e de um espaço europeu que se quer cada vez mais alargado, mas, simultaneamente, seguro.

Estou certo que este colóquio virá também ele contribuir para uma definição mais precisa das linhas de orientação e de intervenção nesta matéria. Pela minha parte, e em nome do governo que aqui represento, quero assegurar-vos que tudo faremos para – sem descurar essa segurança que é condição da própria liberdade – garantir o pleno exercício dos direitos que assistem aos nossos concidadãos.

Muito obrigado. E votos de um bom trabalho.

João Labescat

Presidente da Autoridade de Controlo Comum de Schengen

Começo por agradecer a presença do Dr. Armando Vara, Secretário de Estado Adjunto do Senhor Ministro da Administração Interna. A sua presença constitui um incentivo para o desenvolvimento do nosso trabalho.

Queria também saudar em nome da Autoridade de Controlo Comum e agradecer aos nossos convidados que aceitaram intervir neste Colóquio, agradecimento e saudação extensível a todos os que quiseram partilhar connosco a reflexão que nos propomos fazer.

Ao promover o primeiro colóquio sobre *Sistemas de Informação Policial e os direitos dos cidadãos*, a Autoridade de Controlo Comum de Schengen continua a cumprir um dos objectivos que traçou para a sua actividade : maior **conhecimento e informação dos direitos** que estão associados aos sistemas de informação policiais, uma **maior transparência**, na forma como funcionam a instituição Schengen e o sistema de informação comum que lhe está associado.

Na era da globalização, a segurança dos cidadãos e a prevenção criminal estão cada vez mais dependentes de sistemas de informação e da capacidade organizacional, humana e técnica das polícias, no domínio das novas tecnologias.

O aprofundamento dos direitos dos cidadãos europeus, em torno da livre circulação e de estabelecimento, num fimdo, a verdadeira construção de um espaço comum de liberdade, determinaram a existência de um sistema comum de informação policial que contrabalançasse a inexistência de determinados controlos nas fronteiras internas.

A consagração de normas de protecção de dados pessoais, a definição de um catálogo de direitos fundamentais, o funcionamento de uma Autoridade de Controlo Comum, de natureza independente, com competência de fiscalização do sistema central, a existência de normas nacionais de protecção de dados e de autoridades nacionais competentes neste domínio são uma veia essencial que alimentam as garantias de legalidade e de democraticidade em todo este complexo sistema.

A Autoridade de Controlo Comum é, pela natureza das suas atribuições, e pela sua composição, **uma entidade independente** na estrutura de Schengen. Têm nela assento representantes das Comissões de Protecção de Dados dos quinze países, elas próprias entidades independentes. Esta é uma questão às vezes nem sempre bem compreendida. Não se trata aqui apenas de uma garantia formal prevista na Convenção. Esta garantia terá que ser correspondida na prática, com a dotação à ACC de meios que lhe

permitam exercer, com independência, as suas missões. Independência não é sinónimo de parente pobre.

A aplicação dos Acordos de Schengen e a circunstância da Convenção exigir, por um lado, um nível adequado de protecção de dados e, por outro, a existência de autoridades nacionais não deixou de contribuir igualmente para conclusão de processos legislativos em vários países, o que nos permite hoje afirmar, com satisfação, que todos os países da União Europeia e todos os que participam em Schengen têm em vigor leis específicas para a protecção de dados.

O Sistema de Informação Schengen funciona desde 26 Março de 1995, ou seja há três anos e três meses. Aos primeiros sete países que participaram nas trocas de informação (Alemanha, Bélgica, Espanha, França, Holanda, Luxemburgo e Portugal), juntaram-se, em 1997, a Áustria, a Grécia e a Itália. Prevê-se que o sistema inclua, no ano 2000, mais cinco países (a Dinamarca, Finlândia, Islândia, Noruega, Suécia).

Falamos actualmente de cerca de 7 milhões e duzentas mil indicações, das quais cerca de dois milhões correspondem a dados de natureza pessoal.

A nível operacional falamos de cerca de um centena de entidades que acedem, em diferentes níveis e graus, a determinadas categorias de dados e a dezenas de milhar de polícias que, no terreno, têm ou podem ter acesso a dados.

Constitui, por isso, um desafio enorme a aplicação e a garantia plena e diária do cumprimento das regras de protecção de dados e das normas especiais de segurança na informação, previstas no texto da Convenção.

Esta foi uma das prioridades da Autoridade de Controlo Comum que desde o início das suas missões, nos controlos que fez ao sistema central, nos pareceres que emitiu, no caso dos dados circularem para embaixadas ou consulados situados fora do espaço Schengen, na implementação de medidas que permitem a auditoria e o controlo de quem acedeu ao sistema, na decisão de proceder a uma verificação nos sistemas nacionais de troca de informações entre países participantes, conhecidos como Gabinetes Sirene, sempre procurou que fossem aplicadas as normas da Convenção.

De todo o esforço comum, que envolveu várias instâncias Schengen, poderemos dizer que o sistema central e a transmissão de informações para cada um dos países é segura. É um trabalho que tem que ser prosseguido e aprofundado.

O facto de o reconhecermos não nos leva a cruzar os braços. Pelo contrário, não só ao nível nacional há muitos aspectos a melhorar, como ao nível do sistema central e comum existem ainda aspectos que merecem alteração.

Schengen, como exemplo, deu e continua a dar uma resposta a alguns arautos da desgraça que entendiam e entendem que os sistemas de

informação policial são contra os cidadãos, que a livre circulação no espaço europeu significava a construção de muros inexpugnáveis, que a seguir a Schengen teríamos o martírio da divisão de famílias, a expulsão de estrangeiros, a quebra de solidariedades e de políticas de amizade entre os povos. A prática desmente e contraria tais visões negativistas. O caso português, e permitam-me que o invoque na presença do Senhor Secretário de Estado, é bem a confirmação da compatibilidade de Schengen com políticas activas de inserção das comunidades, de solidariedade, de legalização de imigrantes. Tivemos em vários países, incluindo Portugal, a legalização fundamentada, justa, equilibrada de imigrantes ilegais, estão a ser reforçados mecanismos de apoio à imigração legal e de combate às redes clandestinas, reconheceram-se novos direitos e reforçou-se o direito ao reagrupamento familiar, executaram-se políticas de solidariedade activa com o povo mártir de Timor-Leste e, recentemente, com o povo da Guiné-Bissau.

Estamos num momento de mudança, na informação policial e na estrutura de Schengen.

A integração de Schengen na União Europeia, a entrada em vigor e em funcionamento da Convenção Europol, a futura Convenção Eurodac, o reforço das medidas de cooperação policial, a troca de informações com carácter multilateral, os projectos comuns de combate às redes de imigração clandestina, a fluxos de imigração de determinadas zonas do globo levam-nos a questionar se não entrámos numa **nova era de acção comum e de informação comum**, no âmbito policial, naturalmente a mais efectiva forma para combater o crime mais organizado e com meios cada vez mais sofisticados.

Deixaria à reflexão cinco desafios.

O primeiro é o da **interoperabilidade, o da eficácia, o da complementaridade e o da integração harmoniosa** dos sistemas existentes e dos que vão ser criados na União Europeia. Os diferentes fins a que se destinam estes sistemas acabam, bastas vezes, por confluir num grupo restrito de utilizadores. Tal envolve também mais formação e informação do lado das polícias.

O segundo respeita aos **direitos e ao papel das Autoridades de Controlo**. O leque de direitos deve ser claro, comum, garantir um espaço de defesa individual, compatível com a liberdade pessoal e com os direitos do homem e devem ser aplicados de forma uniforme a nível de todos os países. Por outro lado, as Autoridades de Controlo de Schengen, da Europol, da Eurodac e outras devem coordenar esforços, não virar as costas, aproveitar os meios, coordenando-os com as Comissões Nacionais de Controlo. É também essencial que a União Europeia caminhe decididamente, como aliás muitos documentos já o denotam, para soluções que permitam que estes sistemas funcionem e mantenham um controlo efectivo e independente, sem agora discutir as formas como estes controlos devem passar a ser feitos.

O terceiro insere-se na **democraticidade e legalidade** dos sistemas de informação policial. Importa que esta integração de informação, a centralização de dados sensíveis seja acompanhada, não apenas por Autoridades independentes, mas também pelos Parlamentos nacionais e pelo Parlamento Europeu.

O quarto insere-se no **desafio da modernidade** e numa verdadeira alteração das práticas e dos meios tecnológicos disponíveis. Por um lado, os diferentes sistemas de informação nacionais devem ser compatíveis, servir a segurança e não interesses corporativos. Queremos sistemas de informação nacionais compatíveis e não sistemas parcelares, semnexo, muitas vezes de mais difícil controlo. Por outro lado, temos que adiantar o passo, numa corrida contra o tempo, quando já partimos com atraso. É preciso investir nos novos produtos de tratamento de informação, é preciso formar os nossos quadros.

O quinto tem haver com **a cidadania**. Não é possível conceber fortes sistemas de informação sem controlo, e esquecer que o controlo também pode e deve ser feito por cidadãos e cidadãs conscientes e informadas. Comemora-se este ano o cinquentenário da Declaração Universal dos Direitos Humanos, instrumento que traçou um vasto património de direitos e princípios, que tocam a dignidade do ser humano. Há que continuar a dar corpo a tais direitos. Voltaria, por isso, ao início para dizer que estes desafios podem e devem ser vencidos com maior transparência e mais informação. É para isso que estamos aqui.

1ª PARTE

A EXPERIÊNCIA DO SISTEMA DE INFORMAÇÃO SCHENGEN E OS DIREITOS DOS CIDADÃOS

O Papel da Autoridade de Controlo Comum (ACC) de Schengen
na defesa dos direitos dos cidadãos

João Labescat
Presidente da Autoridade de Controlo Comum
de Schengen

Autoridade de Controlo Comum: a actividade em prol dos direitos no quadro do Sistema de Informação Schengen

O Acordo e a Convenção de Aplicação de Schengen (CAAS) criaram um regime próprio de direitos, liberdades e garantias que, no essencial, se apresenta em dois planos, o da legislação comum, que todos os países signatários devem cumprir e o da previsão nacional de normas garantísticas, maxime a existência de tutelas jurisdicionais.

Nesse quadro de direitos (e obrigações) assumem particular relevo as normas materiais de protecção de dados pessoais. Não se satisfizeram os Estados pela mera previsão de normas gerais nesta matéria. O funcionamento do primeiro sistema de informação policial comum, com suporte informatizado central, impunha a existência de um controlo independente.

A competência para o exercício deste controlo foi atribuído a uma Autoridade de Controlo Comum (ACC), quanto à parte central do sistema e a autoridades nacionais, quanto às componentes nacionais. Quem somos, que competências temos, quais as normas que aplicamos, que articulação estabelecemos com os sistemas e as autoridades nacionais e no quadro da organização Schengen?

A Convenção de Aplicação institui uma Autoridade encarregue do controlo da função técnica do Sistema de Informação Schengen (nº 1 do artigo 115º da Convenção de Aplicação).

Esta entidade é composta por dois representantes de cada autoridade nacional de controlo das Partes contratantes. Existindo liberdade de designação por cada Estado das autoridades nacionais, todos eles optaram por atribuírem às Comissões ou Comissários de Protecção de Dados essa representação (é condição imposta pela Convenção que o controlo da parte nacional seja da responsabilidade de uma entidade independente) .

Actualmente compõem a Autoridade Comum representantes das Partes que têm dados no sistema (Alemanha, Áustria, Espanha, Bélgica, França, Grécia, Holanda, Luxemburgo, Itália, Portugal) e representantes dos países que ainda não têm dados no SIS, participando nos trabalhos da ACC com o estatuto de observadores (Dinamarca, Finlândia, Islândia, Noruega e Suécia).

Desta composição decorre uma primeira importante conclusão, que iremos ver confirmada quando analisarmos o leque de competências. É que, embora a palavra independente não esteja objectivada quanto à Autoridade de Controlo Comum esta é, na sua génese, uma entidade independente.

Nas competências da ACC podemos distinguir: as que respeitam ao exercício de autoridade própria, as consultivas e as de harmonização de procedimentos e normas.

Dois aspectos interessa referir, como ponto de partida e pressupostos essenciais da actividade da ACC. O primeiro é que não pode existir Sistema de informação Schengen sem que a ACC esteja constituída e exerça as suas competências (garantia de legalidade). O segundo, a função de transparência que a ACC exerce em todo o sistema, bem patente no facto desta poder elaborar Relatórios e enviá-los directamente, não apenas ao Comité Executivo (Comité de Ministros que tem a responsabilidade de aplicar a Convenção), mas às várias instâncias nacionais, designadamente aos respectivos Parlamentos (nº 4 do artigo 115º da CAAS).

A competência de controlo da função de apoio técnico – ou seja do Sistema Central – corresponde ao exercício de um verdadeiro poder de autoridade. À ACC cabe verificar a boa execução das disposições da Convenção em matéria de protecção de dados e de segurança da informação, de harmonia com a Convenção nº 108 do Conselho da Europa, para a protecção das pessoas relativamente ao tratamento automatizado de dados pessoais e com a Recomendação (87) 15, de 17 de Setembro de 1987, sobre utilização dos dados pessoais no sector da polícia, do Comité de Ministros do Conselho da Europa.

Desta função de controlo decorre, em primeiro lugar, que só a ACC pode exercer esta função com acesso aos dados do sistema, de forma independente. Em segundo lugar, que a ACC tem o poder de aceder a todas as instalações onde se encontra o C-SIS, incluindo os locais de guarda de cópias do sistema, se estas se encontrarem, como é natural, fora do edifício do sistema central e exercer o respectivo controlo, na base de critérios por ela definidos. Não cabe ao controlado balizar a forma de exercício de controlo, mas cabe ao controlador definir as regras do controlo.

Com vista a evitar problemas no exercício desta função a ACC propôs a elaboração de um conjunto de princípios a ter em consideração durante o controlo. Estes estão em fase final de aprovação em análise com o Ministério do Interior francês, país responsável pela manutenção e gestão do C-SIS.

De facto, não se pode admitir, como já aconteceu, que técnicos a quem a ACC atribuiu a verificação de determinadas funções no C-SIS se tenham visto impedidos de as verificar plenamente.

Há ainda um terceiro aspecto quanto ao controlo do C-SIS que diz respeito à informação. O poder de controlar pressupõe o poder de ter acesso a todos os dados e elementos informativos sobre o sistema de forma a que o controlo se possa efectivar em condições de certeza e fiabilidade.

Em relação às funções consultivas, estas resultam especialmente do facto de existirem um conjunto de projectos e procedimentos que dizem respeito ao tratamento de dados pessoais e que a ACC, ou é consultada pelos

organismos executivos e técnicos, ou intervém por sua iniciativa. Por exemplo, na definição do tempo de conservação de dossiers pessoais depois da eliminação de uma indicação, nas condições e admissibilidade de determinadas entidades acederem a dados do sistema ou na de poder existir ou não transmissão de determinados dados a outras entidades policiais, como a Interpol.

Finalmente uma referência à competência de harmonização de práticas com vista a encontrar soluções comuns para problemas existentes, designadamente no exercício do direito de acesso. A ACC fixou regras de cooperação entre as autoridades nacionais com vista a garantir que um cidadão que solicite um acesso na Comissão de Protecção de Dados francesa (CNIL) de um dado que lhe respeite inserido por Portugal, exista uma perfeita articulação com vista a verificar a legalidade dessa inserção, o que pode implicar uma investigação por parte da Comissão portuguesa, junto da entidade policial nacional que o enviou para o sistema.

A segurança dos dados em Schengen, como em qualquer sistema de informação policial, é uma questão essencial. A Convenção consagra normas especiais relativas à segurança da informação, que devem ser cumpridas nos sistemas nacionais e no sistema comum. A ACC deve ser informada das medidas de segurança adoptadas quando existam dados transmitidos a serviços (consulados, embaixadas) situados fora dos territórios dos Países que participam no sistema.

Nesta matéria da segurança, foi pública a existência de uma fuga de informação de um dos Gabinetes SIRENE, gabinetes onde se procede à troca de informação suplementar sobre as indicações existentes no SIS. Esta fuga de informação que resultou não de falha informática, mas de um acto criminoso cometido por uma pessoa que trabalhava nesse gabinete e que copiava listagens impressas, foi considerada pela ACC como grave, e levou a tomar a decisão de, em todos os países, efectuar inspecções específicas à segurança dos SIRENE. Estas verificações, da competência de cada uma das comissões de protecção de dados, resultarão na elaboração de um relatório, tendo a ACC defendido que haja, para além dos critérios comuns definidos, regras harmonizadas em matéria de segurança.

É de salientar, finalmente, o contributo que a ACC tem vindo a dar paulatinamente para a transparência dos objectivos do Sistema de Informação Schengen.

Os Relatórios Anuais são publicados e distribuídos em todos os países, são enviados aos parlamentos e nalguns casos, são discutidos no âmbito de comissões especializadas parlamentares. A ACC promoveu, no ano passado (1997) em Lisboa, uma Conferência de Imprensa de divulgação do 1º Relatório de Actividades. As instituições europeias receberam o relatório.

Sempre que a ACC considerou dever tornar públicas as suas decisões, fê-lo sempre e de forma independente. No caso da acção de fiscalização dos

Sirene – decorrente da fuga de informação verificada no final de 1997 – a ACC emitiu um comunicado final com ampla repercussão em vários países.

Mas não estamos satisfeitos. Já há muitos anos que defendemos que onde não existe participação, onde não existe informação, o direito formalmente reconhecido, não passa disso mesmo: um direito formal. O exercício dos direitos está intimamente ligado com a informação e conhecimento pelos cidadãos e pelas entidades que os aplicam do seu conteúdo, das formas e dos meios para o seu exercício. E, nesta matéria, não há que esconder que existe um défice. Não tem havido, designadamente nas instâncias executivas, a preocupação na divulgação dos direitos dos cidadãos quanto ao SIS.

A realização deste Colóquio insere-se nesse esforço e no inverter de tendências ou teorias secretistas que fazem destes sistemas um assunto para especialistas, que poucos conhecem. As decisões de Schengen devem deixar a penumbra e passar a ser mais conhecidas do grande público, da comunicação social e dos Parlamentos, incluindo o nacional.

Com esse objectivo a ACC decidiu desenvolver e propor aos organismos executivos a realização de campanha “O Sistema de Schengen diz-lhe respeito”. A campanha, com uma imagem própria, é constituída por um cartaz e um folheto explicativo sobre os direitos dos cidadãos face o SIS. Procura-se explicar de forma simples os meios à disposição de qualquer pessoa para exercer um direito de acesso. Espera-se que estes folhetos – disponíveis em todas as línguas de trabalho Schengen – sejam distribuídos no decorrer de 1998 e em 1999.

Trata-se da primeira campanha comum sobre direitos dos cidadãos face aos sistemas de informação policiais, o que não deixa de ser significativo no posicionamento da ACC, como primeira autoridade nesta área.

O quadro de competências que se traçou, como se pode verificar, reforça o que já havia dito sobre a matriz independente da Autoridade de Controlo Comum.

O Sistema de Informação de Schengen obedece a um conjunto de regras de protecção de dados e a Convenção tipifica um catálogo bastante completo de direitos e princípios.

Tais regras e princípios não se aplicam apenas à componente central do SIS, mas devem ser entendidos como abrangendo todo o sistema Schengen, incluindo os sistemas nacionais e os gabinetes Sirene.

Tenho verificado a existência em Portugal, de alguma desinformação, fruto do desconhecimento dos objectivos da Convenção de Schengen. Esta Convenção não é contra os imigrantes, nem contra as especiais relações que cada país estabeleceu historicamente com outros povos e Estados. A Comunidade de Povos de Língua Portuguesa foi criada e desenvolve-se uma

ampla cooperação com os países que nela participam. Schengen não o impede.

Da mesma forma, a Convenção não admite a inserção no sistema de informação de dados pessoais que poderiam significar discriminação política, religiosa ou racial. O nº 2 do artigo 94º da CAAS determina que não são autorizadas referências a dados previstos no artigo 6º da Convenção nº 108 do Conselho da Europa, acima citada. Nesta norma estão incluídos dados pessoais que revelem a origem racial, as opiniões políticas, as convicções religiosas e outras, os dados de saúde e da vida sexual. Não há que ter dúvidas. A Convenção proíbe peremptoriamente o tratamento destes dados sensíveis.

Atendamos, mais em detalhe, as regras e princípios mais importantes:

- Princípio da finalidade, aplicada à utilização do sistema global e cada uma das categorias de dados. O SIS só tem por objectivo a preservação da ordem e segurança públicas, incluindo a segurança do Estado, bem como a aplicação da Convenção, sobre circulação de pessoas e os dados previstos só podem ser utilizados para finalidades que estão tipificadas (Artigo 93º e nºs 1, 4 do artigo 102º da CAAS).
- Princípio da legalidade e da responsabilidade nacional pela inserção e manutenção dos dados. Os dados são inseridos em conformidade com a legislação nacional de cada Estado autor de uma indicação, ficando este responsável pela sua alteração, difusão ou eliminação (nºs 1 e 2 do artigo 104 da CAAS), sem prejuízo da aplicação de normas mais rigorosas previstas na Convenção.
- Princípio da tipificação das categorias de dados e dos próprios dados que existem no sistema. Tal significa, que os dados inseridos estão organizados por finalidades (por exemplo, estrangeiros para não admissão, pessoas procuradas para detenção, protecção de testemunhas, vigilância discreta, veículos procurados, objectos procurados), conforme cada um dos artigos previstos na Convenção, que fundamentam a legalidade e a finalidade da inserção e utilização dos dados. Por seu lado, estão listados no artigo 94º, o tipo de dados que podem constar no sistema (citam-se a título de exemplo, o nome, os sinais físicos particulares, objectivos e inalteráveis, a nacionalidade, o sexo, a data e o local de nascimento, a conduta a adoptar). É pois uma lista de dados e de finalidades fechada, pelo que não podem existir razões de oportunidade política ou outras que possam admitir a inserção de outros dados, sem que a Convenção seja alterada.
- Princípio do *numerus clausus* das entidades que podem consultar o sistema, fixado pela Convenção, em função das competências que lhe estão atribuídas pela legislação nacional. Nos termos do artigo 101º, o acesso é reservado às entidades competentes para o controlo fronteiriço, para as verificações de polícia e aduaneiras, incluindo a sua coordenação, bem como as autoridades que controlam a emissão de vistos a sua análise ou que são responsáveis pela administração de estrangeiros. Acresce ainda, que o acesso é limitado em relação à competência de cada entidade. O acesso a cada categoria de informações deve

corresponder às competências legalmente estabelecidas a determinada entidade.

- Princípio do patamar comum de legislação nacional de protecção de dados pessoais, a que corresponde a obrigatoriedade de todos os países que têm dados no sistema, aplicarem um nível de protecção de dados pelo menos igual ao definido na Convenção nº 108 do Conselho da Europa e em conformidade com a Recomendação sobre utilização de dados no sector da polícia. Esta obrigação envolve três aspectos relevantes: a ratificação da Convenção pelos países Partes do sistema, a existência de legislação nacional de protecção de dados aplicável à informação policial e o funcionamento efectivo de uma autoridade independente de controlo de dados.
- Princípio da conservação limitada dos dados, que significa que no sistema não existem dados perpétuos, mas informações que têm uma duração limitada à finalidade da sua inserção e utilização. De acordo com este critério existem tempos diferentes para conservação de dados em função da respectiva finalidade.
- Princípio da segurança, segundo o qual, os Estados e os responsáveis pelo sistema central devem adoptar uma série de medidas que impeçam acessos indevidos, em todas as fases do processamento da informação e em todo o tipo de suportes (informatizados e não informatizados), incluindo a habilitação do pessoal que lida com informação policial.
- Princípio da exactidão, actualização e correcção dos dados que é base fundamental para a eficácia das informações contidas e das condutas policiais a adoptar, por um lado, e da salvaguarda dos direitos, por outro.
- Princípio da tutela jurisdicional e administrativa, segundo o qual, todas as partes garantem a qualquer pessoa a possibilidade de recorrer a um tribunal em defesa dos direitos ofendidos.

Por fim, e deixo propositadamente para a conclusão desta lista de princípios e regras, a indispensabilidade de existir um sistema de controlo de dados pessoais a funcionar, efectivo, com poderes e competências, tanto na dimensão nacional, como a nível do sistema central. Este último princípio envolve a existência de comissões nacionais de protecção de dados e de uma Autoridade de Controlo Comum.

Além dos princípios agora alinhados, a Convenção define uma panóplia de direitos das pessoas face ao SIS.

O direito de acesso e de comunicação de dados : qualquer pessoa pode aceder aos dados que lhe digam respeito. O pedido pode ser dirigido a qualquer autoridade nacional de protecção de dados, aplicando-se contudo, o princípio da propriedade de dados no qual o Estado, autor da indicação, tem sempre a última palavra.

A comunicação de dados pode ser recusada se for susceptível de prejudicar a execução da tarefa legal em causa ou se a recusa se revelar necessária para a protecção dos direitos e liberdades de outrem. A comunicação será sempre recusada se a pessoa estiver indicada para efeitos de vigilância discreta (artigo 109º da CAAS).

O **direito de rectificação** (artigo 110º da CAAS) segundo o qual, qualquer pessoa pode exigir a rectificação dos dados que lhe digam respeito, que se encontrem viciados por erro de facto ou exigir a eliminação dos dados viciados por erro de direito.

O **direito de instaurar uma acção para rectificação, eliminação, informação ou indemnização** : qualquer pessoa deve poder, no território de cada Parte Contratante, fazer valer os seus direitos perante órgão jurisdicional ou qualquer outra autoridade competente (artigo 111º da CAAS).

O **direito de exigir a verificação de dados** (nº2 do artigo 114º da CAAS), direito que abrange a possibilidade da pessoa poder solicitar a uma autoridade nacional de controlo que verifique se dados que lhe dizem respeito, bem como a sua utilização têm suporte legal. Caso os dados tenham sido inseridos por outro Estado, que não aquele onde foi apresentado o pedido, o controlo é exercido em estreita colaboração da autoridade de controlo do Estado autor da indicação.

Em resumo, poderemos concluir que o quadro dos direitos pessoais previstos na Convenção atribui a todos os cidadãos um importante instrumento de verificação da legalidade dos dados inseridos, do seu acesso e utilização. Contudo, apesar de não existir um balanço exaustivo do número de pedidos de acesso é possível, até pelo exemplo português (cerca três pedidos/ano), verificar que o exercício destes direitos está muito aquém do desejável. E, nesta matéria, a consciência de cidadania é necessária. É nosso entendimento que os Estados devem incentivar mecanismos de informação que propiciem o exercício dos direitos.

Em termos de organização e de estrutura Schengen onde se encontra a ACC?

Como órgão independente não reporta a qualquer outra entidade. As suas decisões são enviadas ao Comité Executivo ou ao Grupo Central. A estrutura de Schengen abrange uma série de domínios e de Grupos de trabalho, alguns directamente relacionados com o funcionamento do SIS, que são claramente técnicos e outros que lidam com a aplicação da Convenção nas áreas da cooperação judiciária, da política de vistos, das fronteiras. Existe ainda um secretariado-geral de apoio sediado em Bruxelas. Dois aspectos não podem deixar de merecer uma reflexão. O primeiro é se a estrutura de Schengen corresponde àquilo que são as responsabilidades que a Convenção lhes conferiu a outra são os mecanismos de interacção e colaboração entre todos os Grupos.

Convém deixar muito claro que a ACC não é mais um Grupo de trabalho, formado com base numa decisão do Comité Executivo. É uma Autoridade de Controlo cuja existência decorre da própria Convenção e cujo funcionamento é pressuposto para a efectivação prática do sistema de informação. Não pode haver um sistema de informação sem autoridade de controlo. Verificámos, neste três anos de funcionamento do sistema, por um lado, que

se prolongavam e prolongam as decisões e as tomadas de posição dos organismos técnicos em face dos Pareceres da ACC, o que é de lamentar. Por outro, por falta de coordenação e de informação mútua constata-se que a ACC não é informada de muitas iniciativas em curso, ou mesmo de documentos básicos, cujo conhecimento interessa para o exercício das suas competências.

A ACC tem vindo a pugnar pela alteração deste estado de coisas e pode dizer que houve pequenas inflexões e contributos positivos, designadamente durante a presidência portuguesa de Schengen. É um caminho que tem de ser aprofundado.

Não basta que existam Autoridades é também necessário dotá-las dos meios indispensáveis. À ACC foram recusados, inicialmente, os meios para que esta pudesse fazer as suas inspecções com independência. Após dois anos de negociações complexas e apesar da aprovação de uma linha autónoma no orçamento, continuamos ainda a não ter pessoal de apoio exclusivo para a ACC, o que implica objectivas restrições na forma de exercício do controlo. Não poderemos admitir que as normas da Convenção sejam vencidas e anuladas pela burocracia e por decisões que não visam a sua plena execução.

A ACC tem vindo a propor junto da presidência do Comité Executivo a agilização na forma de relacionamento das autoridades e tem insistido pela atribuição de mais meios.

Gostaria de deixar ainda algumas palavras quanto ao futuro de Schengen e, em particular da ACC. Como se sabe o Tratado de Amesterdão integra Schengen na União. É uma decisão muito importante para a democraticidade e controlo da legalidade das matérias alvo de Schengen.

Tenho defendido que aquilo que constitui património da actividade da ACC, as suas decisões e pareceres, bem como os aspectos relevantes da sua acção constituem aquis comunitário, como acontece com as decisões do Comité Executivo e dos Grupos a quem esse comité atribuiu poderes. Apesar do Protocolo de integração de Schengen, anexo ao Tratado, não ser específico, este é o entendimento que decorre da aplicação das regras da Convenção. Se uma decisão do Grupo Central é aquis, por que razão não seria uma decisão da ACC, órgão da Convenção? É o facto de ser independente? Pelo contrário, tudo justifica que as decisões independentes da ACC sejam tidas em consideração no futuro quadro institucional.

Importa que a integração do SIS no âmbito da estrutura comunitária seja acompanhada pelo controlo independente da ACC e que a sua actividade não seja afectada por essa integração. Faço sinceros votos para que esta integração não se faça à última hora e aos tropeços.

É preciso lembrar que os sistemas de informação na Europa sofrerão uma evolução sensível no próximo ano. Aproxima-se a aplicação da Europol, da Convenção Aduaneira e do sistema Eurodac, sendo muito importante

encontrar a boa fórmula que permita que todos os sistemas funcionem em harmonia, com controlo independente e efectivo.

A Autoridade de Controlo Comum tem um mandato que lhe foi conferido pelos Estados membros, ao ratificarem a Convenção. Goza de uma legitimidade directa. Nunca pretendemos, nem pretenderemos fazer o que não nos cabe. Mas nunca renunciaremos a exercer as nossas competências.

A minha última mensagem é de disponibilidade. A ACC está plenamente disponível para continuar a colaborar com todos, para que a protecção de dados pessoais continue com o alto nível que lhe reconhecemos actualmente no sistema de informação Schengen.

* Presidente da Autoridade de Controlo Comum de Schengen

A Integração de Schengen na União Europeia¹

Nuno Piçarra

Coordenador Nacional para os Assuntos da Livre Circulação de Pessoas
no Espaço Europeu

¹ Esta comunicação apenas exprime a opinião pessoal do autor. Para uma abordagem complementar do tema, ver, também do autor, «La mise en oeuvre du protocole intégrant l'acquis de Schengen dans le cadre de l'Union européenne: règles et procédures» in Monica den Boer (edit.) *Schengen's Final Days? The Incorporation of Schengen into the New TEU, External Borders and Information Systems*, Instituto Europeu de Administração Pública, Maastricht, 1998, pp. 25-58.

I. Indicação de sequência

1. Num dos primeiros comentários escritos ao Tratado de Amesterdão (a seguir, “TA”), publicado na *Common Market Law Review* de Agosto de 1997, observou-se, com muita razão, que o Protocolo que integra o acervo de Schengen no âmbito da União Europeia (“Protocolo”), anexado ao Tratado da União Europeia (“TUE”) e ao Tratado que institui a Comunidade Europeia (“TCE”) pelo TA, «é um exercício de redacção engenhoso – talvez demasiado engenhoso – sobre o qual serão provavelmente vertidos muitos litros de tinta académica. No entanto, a ideia básica é simples».

Na presente comunicação, após recordar brevemente a ideia básica do Protocolo e os seus antecedentes, tentar-se-á demonstrar – de um modo tão parco em tinta quanto possível – que, se em teoria ela é efectivamente simples, a sua aplicação prática comporta, no entanto, alguns aspectos bem complexos.

Cinco dos oito artigos do Protocolo contêm disposições que carecem da intervenção legiferante do Conselho para poderem ser efectivamente aplicadas. Isto significa que, através dessas disposições – as quais incluem simultaneamente “ordens de legislar” concretas –, o Protocolo devolve em larga escala ao Conselho a árdua tarefa de regulamentar uma série de aspectos essenciais para que, na data de entrada em vigor do TA, a cooperação Schengen possa transferir-se sem entraves para a União Europeia (“UE”). Ver-se-á, no entanto, que é porventura a este respeito que a solução consagrada no Protocolo se revela mais engenhosa: apesar de a maior parte das suas disposições remeter para uma intervenção legislativa do Conselho, o Protocolo salvaguarda um “núcleo duro” directamente aplicável, em termos, no essencial, “à prova de falha”.

Das medidas cuja adopção o Protocolo impõe ao Conselho, apenas será analisada aquela que, à primeira vista, parece a mais simples e que se prende com a definição do próprio acervo de Schengen para efeitos da sua integração na UE. Ver-se-á que o Anexo ao Protocolo, apesar de enunciar os critérios para o efeito de forma aparentemente inequívoca, carece de uma laboriosa operação interpretativa para poder ser correctamente aplicado.

Mas os problemas práticos mais complexos resultarão sem dúvida do regime de que beneficiam os Estados-Membros que não estão à partida vinculados pelo acervo de Schengen, como é o caso da Irlanda e o Reino Unido, ou que, estando-o, dispõem da faculdade de não ficar futuramente vinculados à totalidade das medidas adoptadas pelo Conselho em desenvolvimento desse acervo, como é o caso da Dinamarca. Analisar-se-ão os aspectos mais problemáticos deste regime, o qual, de resto, decorre não só do Protocolo Schengen, mas também do Protocolo relativo à aplicação de certos aspectos do artigo 14º do TCE ao Reino Unido e à Irlanda assim como do Protocolo relativo à posição do Reino Unido e da Irlanda face ao novo Título IV do TCE,

para o primeiro caso, e do Protocolo relativo à posição da Dinamarca face ao mesmo Título, para o segundo caso.

Terminar-se-á com uma breve apreciação global do Protocolo, com base nos diversos aspectos analisados.

II. Os fundamentos do Protocolo que integra o acervo de Schengen no âmbito da União Europeia

2. O artigo 1º do Protocolo autoriza os treze Estados-Membros que são Partes Contratantes no Acordo relativo à Supressão Gradual dos Controlos nas Fronteiras Comuns e na sua Convenção de Aplicação (“CAAS”) – Alemanha, Áustria, Bélgica, Dinamarca, Espanha, Finlândia, França, Grécia, Itália, Luxemburgo, Países Baixos, Portugal e Suécia – a prosseguir, a título de “cooperação reforçada”, a cooperação baseada naqueles dois instrumentos e disposições conexas, designados por acervo de Schengen, no quadro institucional e jurídico da UE, sem a participação da Irlanda e do Reino Unido.

Com a entrada em vigor do TA, a cooperação entre os Estados Schengen, até aqui prosseguida à margem da UE, transfere-se para o âmbito desta, passando, portanto, a fundar-se no TUE e no TCE. Tal só se tornou possível mediante a consagração pelo TA do instituto jurídico da “cooperação reforçada ou mais estreita”, que permite à UE avançar em determinados domínios sem a participação obrigatória de todos os Estados-Membros.

O Protocolo constitui um caso de cooperação reforçada na sua variante “predeterminada”: é ele próprio que autoriza directamente os treze Estados-Membros a prosseguir a cooperação Schengen no âmbito da UE, diversamente dos casos de cooperação reforçada mediante uma “cláusula de habilitação”, previstos pelos artigos 43º e 40º do TUE e pelo artigo 11º do TCE. Nestes casos, é ao Conselho que compete autorizar os Estados-Membros que se proponham instaurar entre si uma cooperação reforçada em determinado domínio a «recorrer às instituições, processos e mecanismos» previstos pelo TUE ou pelo TCE, nas condições aí estabelecidas.

3. A integração do acervo de Schengen na UE significa concretamente que, a partir da data da entrada em vigor do TA, a cooperação baseada naquele acervo passa a ficar abrangida pelo âmbito de competência do Conselho, da Comissão, do Parlamento Europeu e do Tribunal de Justiça, nos termos do TUE ou do TCE, consoante os casos. Assim, o artigo 2º, nº 1, primeiro parágrafo, última parte, do Protocolo prevê expressamente que o Conselho (em princípio, na sua formação “Justiça e Assuntos Internos”) se substitui ao Comité Executivo instituído pela CAAS. No que diz respeito ao Tribunal de Justiça, o artigo 2º, nº 1, terceiro parágrafo, explicita o princípio segundo o qual este órgão jurisdicional é competente para o controlo das «disposições ou decisões que constituem o acervo de Schengen», precisando, no entanto, que ele «não tem competência, em caso algum, para se pronunciar sobre medidas ou decisões relativas à manutenção da ordem pública e à garantia da segurança interna».

Por outro lado, nos termos do artigo 2º, nº 1, segundo parágrafo, última frase, «cada uma das disposições ou decisões que constituem o acervo de Schengen» deve ser reconduzida a uma base jurídica, ou no Título VI do TUE – relativo à cooperação policial e judiciária em matéria penal – ou no novo Título IV, aditado à Parte III, do TCE – que versa sobre «vistos, asilo, e outras políticas relativas à livre circulação de pessoas».

Além disso, por força do disposto no artigo 5º, nº 1, primeiro parágrafo, e nº 2, a partir da data de entrada em vigor do TA, as propostas e iniciativas baseadas no acervo de Schengen regem-se pelas disposições pertinentes do TUE ou do TCE. Isto significa que, a partir daquela data, todas as novas disposições, decisões e medidas destinadas a alterar ou a desenvolver o acervo de Schengen são adoptadas sob a forma e de acordo com os procedimentos previstos no artigo 34º do TUE ou no artigo 67º do TCE. Assim, elas revestirão:

- ou a forma de decisões-quadro, convenções, etc., adoptadas pelo Conselho deliberando por unanimidade, por iniciativa de qualquer Estado-Membro ou da Comissão e após consulta ao Parlamento Europeu, nos termos das disposições conjugadas dos artigos 34º, nº 2, e 39º do TUE;
- ou a forma de regulamentos, directivas, decisões, etc., adoptados pelo Conselho deliberando por unanimidade, sob proposta da Comissão ou por iniciativa de um Estado-Membro e após consulta ao Parlamento Europeu, durante um período transitório de cinco anos, no termos das disposições conjugadas dos artigos 67º, nº 1, e 249º do TCE.

No primeiro caso, as disposições e medidas adoptadas ficam sujeitas ao controlo do Tribunal de Justiça, em conformidade com o artigo 35º do TUE e, no segundo, em conformidade com o artigo 68º do TCE. Em ambos os casos poderão nomeadamente ser objecto de um recurso de anulação ou de um reenvio prejudicial.

III. Os antecedentes do Protocolo

4. Diversos antecedentes, de resto bem conhecidos, contribuem para explicar a solução jurídica finalmente fixada em 2 de Outubro de 1997 para a integração do acervo de Schengen na UE, cerca de dois anos e meio após a CAAS ter começado a ser aplicada por sete Estados-Membros – 26 de Março de 1995.

Recorde-se, em primeiro lugar, a falta de consenso entre os Estados-Membros quanto à competência da então Comunidade Económica Europeia para adoptar a totalidade das regras de direito comunitário consideradas necessárias para concretizar o objectivo de criação de um «espaço sem fronteiras internas no qual a livre circulação das mercadorias, das pessoas, dos serviços e dos capitais é assegurada», tal como ele era maioritariamente interpretado. Foi esse impasse que levou cinco Estados-Membros – Alemanha, Bélgica, França, Luxemburgo e Países Baixos – a instaurar entre si uma cooperação mais estreita e, por isso mesmo, então necessariamente

à margem do quadro institucional e jurídico da CEE, com vista à supressão dos controlos de pessoas nas fronteiras comuns, incluindo medidas compensatórias para o défice de segurança que tal supressão poderia implicar. Na impossibilidade de então recorrer às «instituições, processos e mecanismos» previstos no TCEE, aqueles Estados-Membros concluíram, portanto, para o efeito – como solução assumidamente transitória – o Acordo de Schengen e a CAAS, concebendo-os essencialmente como instrumentos de execução do então artigo 8º-A do TCEE, relativo ao estabelecimento progressivo do mercado interno.

Compreende-se, assim, que a própria CAAS tenha previsto, por um lado, que as suas disposições só são aplicáveis na medida em que sejam compatíveis com o direito comunitário (artigo 134º) – princípio agora expressamente confirmado pelo terceiro considerando do Protocolo, que se refere à necessária compatibilidade do acervo de Schengen «com o direito da União Europeia e da Comunidade». Por outro lado, o artigo 142º, nº 1, dispõe que, mediante o acordo das Partes Contratantes, as disposições da CAAS são substituídas ou alteradas em função das disposições correspondentes das convenções concluídas entre os Estados-Membros da UE tendo em vista a realização de um espaço sem fronteiras internas, desde que a CAAS não tenha previsto uma cooperação mais aprofundada do que a resultante das referidas convenções.

Recorde-se, por outro lado, que, de alguma forma impulsionado pela cooperação Schengen, o TUE incluiu no seu Título VI uma série de disposições relativas à cooperação no domínio da Justiça e dos Assuntos Internos, largamente inspiradas pelas mesmas premissas que a CAAS, passando inevitavelmente a verificar-se entre ambos os conjuntos normativos uma série de paralelismos e de sobreposições. Isto tornou-se, naturalmente, num argumento de peso a favor da integração do acervo de Schengen na UE.

Outro argumento neste sentido era o balanço largamente positivo que os Estados-Membros faziam da cooperação Schengen à luz do objectivo, também partilhado pela UE, da criação, sem défice de segurança, de um espaço europeu de livre circulação sem controlos de pessoas nas fronteiras internas. Nesta perspectiva, a integração do acervo de Schengen na UE deveria contribuir para realizar mais rapidamente aquele objectivo, compensando simultaneamente o fracasso relativo por que se saldava a cooperação prosseguida desde 1 de Novembro de 1993 no quadro do Título VI do TUE.

5. Na Conferência Intergovernamental (CIG) que culminou com o TA, a integração do acervo de Schengen na UE foi negociada conjuntamente com outros dois elementos de um mesmo pacote, estreitamente ligados ao primeiro: por um lado, a transferência de uma série de domínios relativos à livre circulação de pessoas — como o asilo, a passagem nas fronteiras externas dos Estados-Membros e a imigração — do âmbito de aplicação do Título VI do TUE para o do novo Título IV do TCE, domínios esses a que se juntou o dos vistos, já parcialmente “comunitarizado” (actual artigo 100º-C);

por outro lado, a reforma substancial do Título VI do TUE. Tudo isto tendo como pano de fundo a introdução formal no TUE e no TCE do instituto da cooperação reforçada, destinado a legitimar acções da UE que, pelas suas características, não sejam susceptíveis de envolver à partida todos os Estados-Membros.

Coube aos Países Baixos a iniciativa concreta de integração do acervo de Schengen na UE e a ulterior conclusão das negociações sobre o tema no decurso da sua presidência do Conselho, no primeiro semestre de 1997. Com efeito, foi este Estado-Membro que em 1996 submeteu à CIG um documento informal propondo que tal integração se efectuasse em três fases: a primeira consistiria em instaurar uma cooperação prática entre o Secretariado de Schengen e o Secretariado-Geral do Conselho; a segunda traduzir-se-ia na substituição das instâncias de Schengen pelas instâncias do Conselho, continuando embora a distinguir-se o acervo de Schengen do acervo da UE; a terceira implicaria a conversão do acervo de Schengen em acervo da UE, o qual se tornaria extensivo à Irlanda e ao Reino Unido.

O Protocolo acabou, no entanto, por consagrar uma solução bem diferente. O pouco tempo de que a CIG dispôs para a negociar determinou a própria natureza geral deste instrumento, que se limita a fixar os princípios essenciais, impondo ao Conselho a tarefa de os tornar plenamente aplicáveis mediante uma série de actos jurídicos a adoptar na data de entrada em vigor do TA.

IV. Os actos a adoptar pelo Conselho com vista à aplicação do Protocolo

6. O Protocolo dispõe no seu artigo 2º, nº 1, primeiro parágrafo, primeira parte, em conjugação com o nº 2, que, a partir da data de entrada em vigor do TA, o acervo de Schengen, tal como tiver evoluído até então, torna-se «imediatamente aplicável», no âmbito da UE, àqueles Estados-Membros, dentre os treze mencionados no artigo 1º, que antes de tal data já preenchiam as condições para o aplicar, constantes do próprio acervo.

Neste contexto, o artigo 2º, nº 1, segundo parágrafo, primeira frase, dispõe em termos gerais que o Conselho, deliberando por unanimidade daqueles treze Estados-Membros, toma todas as medidas necessárias para que o artigo 2º, nº 1, primeiro parágrafo, seja efectivamente aplicado a partir da data de entrada em vigor do TA. Trata-se de uma cláusula geral de habilitação que, em conjugação com o disposto no Anexo ao Protocolo, vincula desde logo o Conselho a definir, através de uma decisão, o próprio acervo de Schengen, para efeitos da sua integração na UE.

Para além disso, o Protocolo vincula especificamente o Conselho a adoptar os seguintes actos:

1º) uma decisão, nos termos do artigo 2º, nº 1, segundo parágrafo, segunda frase, determinando as disposições do TUE ou do TCE que constituirão a base jurídica de cada um dos actos incluídos na

definição de acervo de Schengen que venha a ser adoptada pelo Conselho; através de tal decisão, o acervo de Schengen torna-se direito especificamente subordinado, conforme os casos, ao TUE ou ao TCE, ou eventualmente a ambos;

2º) uma decisão, nos termos do artigo 2º, nº 2, fixando as datas a partir das quais o acervo de Schengen passará a aplicar-se – com a consequente supressão dos controlos nas fronteiras internas – àqueles dos treze Estados-Membros que só após a entrada em vigor do TA venham a reunir as condições necessárias para tal, que, como se sabe vão dos controlos efectivos nas fronteiras externas à ligação operacional ao SIS, etc.; os Estados-Membros a quem o artigo 2º, nº 2, diz individualmente respeito são a Dinamarca, a Finlândia e a Suécia, que apenas aderiram a Schengen no final de 1996, não tendo ainda podido preencher todas aquelas condições; mas a disposição em causa poderá ainda tornar-se extensiva à Grécia, na medida em que o Comité Executivo de Schengen se abstenha de constatar, até à entrada em vigor do TA, que estão reunidas as condições para a supressão dos controlos nas fronteiras internas com este Estado-Membro;

3º) uma decisão, nos termos do artigo 4º, por iniciativa do Reino Unido e/ou da Irlanda, determinando as partes do acervo de Schengen que se lhes aplicarão;

4º) um acordo de direito internacional com a Islândia e a Noruega, nos termos do artigo 6º, primeiro parágrafo, prevendo as modalidades de associação destes Estados à execução do acervo de Schengen e ao seu posterior desenvolvimento no âmbito da UE, com base no acordo assinado no Luxemburgo em 19 de Dezembro de 1996 entre os treze Estados Schengen e os dois primeiros;

5º) um segundo acordo separado de direito internacional com a Islândia e a Noruega, nos termos do artigo 6º, segundo parágrafo, condicionado à adopção da decisão supra-enunciada em 3º) e destinado a definir os direitos e obrigações entre estes dois Estados, por um lado, e a Irlanda e o Reino Unido, por outro, nos domínios do acervo de Schengen aceites por estes últimos;

6º) uma decisão, nos termos do artigo 7º, contendo as regras de integração do Secretariado de Schengen no Secretariado-Geral do Conselho.

De acordo com o Protocolo, a adopção do primeiro e do quinto actos jurídicos carece da unanimidade dos quinze Estados-Membros, a do segundo e do quarto exige a unanimidade dos treze Estados Schengen, a do terceiro carece da unanimidade dos treze Estados Schengen e de cada um dos dois Estados interessados, ao passo que a adopção do sexto acto apenas carece da maioria qualificada dos quinze Estados-Membros.

7. Como se disse, utilizando um conceito bem conhecido do direito constitucional, as disposições do Protocolo que acabam de ser enumeradas contêm “ordens de legislar” dirigidas ao Conselho, impondo-lhe a obrigação única de adoptar determinados actos jurídicos indispensáveis à plena aplicação do Protocolo. Algumas delas – como os artigos 2º, nº 1, segundo parágrafo, primeira frase, e 6º – remetem para critérios materiais específicos que o Conselho deve respeitar ao concretizá-las. Outras – como o artigo 7º – deixam ao Conselho-legislador uma margem de apreciação mais ampla. Sem a interposição legislativa do Conselho, nos termos das citadas disposições, o Protocolo não poderá, por conseguinte, ser plenamente aplicado na data de entrada em vigor formal do TA.

Neste contexto, compreende-se que a declaração nº 44 à Acta Final vincule o Conselho a adoptar todas as medidas necessárias à plena aplicação do Protocolo, estipulando que os respectivos trabalhos preparatórios deverão ser efectuados em devido tempo, de modo a estarem concluídos antes da data de entrada em vigor do TA. Assim com se compreende que a declaração nº 45, segunda parte, convide a Irlanda e o Reino Unido a fazer uso das disposições do artigo 4º do Protocolo a fim de que o Conselho possa deliberar logo na data de entrada em vigor do TA sobre a vinculação daqueles dois Estados-Membros ao acervo de Schengen, e que, por seu lado, a declaração nº 47 aponte para que os acordos a que se refere o artigo 6º do Protocolo entrem em vigor na mesma data que o TA.

No entanto, importa sublinhá-lo, há uma parte do Protocolo – e precisamente o seu “núcleo duro” – que não depende da prévia intervenção legislativa do Conselho para poder efectivamente aplicar-se. Tal núcleo duro é constituído pelo artigo 1º, que alicerça sem mais o direito de os treze Estados Schengen prosseguirem no âmbito da UE, a partir da data de entrada em vigor do TA, a cooperação que actualmente levam a cabo no quadro institucional e jurídico criado pela CAAS.

O carácter *self executing* desta disposição é confirmado não só pelo já citado artigo 2º, nº 1, primeiro parágrafo, relativo à «aplicabilidade imediata» do acervo de Schengen, mas também por duas outras disposições do Protocolo: o artigo 2º, nº 1, quarto parágrafo, e o artigo 5º, nº 2. Com efeito, de acordo com a primeira destas disposições, se à data de entrada em vigor do TA, o Conselho se tiver absterido de adoptar a decisão que determina as bases jurídicas para os diversos actos que constituem o acervo de Schengen, estes são considerados actos baseados no Título VI do TUE. Por outro lado, segundo o artigo 5º, nº 2, mesmo que tal venha a ser o caso, as propostas e iniciativas com vista ao desenvolvimento do acervo de Schengen não deixarão, ainda assim, de dever basear-se nas disposições pertinentes do TUE e do TCE.

Na data de entrada em vigor do TA, os treze Estados-Membros poderão e deverão em qualquer caso – com ou sem intervenção legislativa do Conselho – prosseguir no quadro institucional e jurídico da UE a mesma cooperação que actualmente levam a cabo no âmbito da CAAS. O acervo será formalmente recebido na ordem jurídica da UE – com ou sem decisão

definidora do Conselho, nos termos do artigo 2º, nº 1, segundo parágrafo, primeira frase –, passando a desenvolver-se sob a forma e segundo os processos decisórios previstos não somente no Título VI do TUE mas também no novo Título IV do TCE.

A este propósito, observe-se no entanto que, tendo em conta o facto de a cooperação actualmente levada a cabo no quadro institucional e jurídico da CAAS envolver também a Islândia e a Noruega, a não conclusão do acordo a que se refere o artigo 6º, primeiro parágrafo, do Protocolo na data de entrada em vigor do TA – condição *sine qua non* para a disposição em causa se tornar aplicável na parte em que prevê a associação da Islândia e da Noruega «à execução do acervo de Schengen e ao seu posterior desenvolvimento» através de «processos adequados» – poderia pôr em causa a identidade material, que se pretende em absoluto salvaguardar, da cooperação Schengen antes e depois da sua transferência para a UE. O aprofundamento desta questão seria, porém, pura especulação uma vez que o referido acordo já se encontra praticamente concluído.

Por outro lado, convém notar que, se por hipótese o Conselho não adoptasse, na data de entrada em vigor do TA, as regras de integração do Secretariado de Schengen no Secretariado-Geral do Conselho, nos termos do artigo 7º do Protocolo, a prossecução da cooperação Schengen no âmbito da UE ver-se-ia seriamente entravada por o Secretariado-Geral não dispor *a priori* dos meios necessários para fazer face às novas tarefas decorrentes de tal integração. No entanto, a adopção da decisão em causa – indispensável para tornar efectiva a integração do Secretariado de Schengen – há-de ser, de alguma maneira, facilitada pelo facto de apenas se exigir maioria qualificada no Conselho para o efeito. Nesta perspectiva, pode dizer-se que o requisito da mera maioria qualificada completa o sistema à prova de falha com que o Protocolo definitivamente salvaguarda a aplicabilidade directa dos seus artigos 1º e 2º, nº 1, primeiro parágrafo.

V. A definição do acervo de Schengen para efeitos da sua integração na União Europeia

8. O Anexo ao Protocolo qualifica como acervo de Schengen os seguintes elementos:

- o Acordo assinado em 14 de Junho de 1985, relativo à supressão gradual dos controlos nas fronteiras comuns;
- a CAAS, assinada em 19 de Junho de 1990, bem como a respectiva Acta Final e declarações comuns;
- os Protocolos e Acordos de Adesão da Itália, da Espanha, de Portugal, da Grécia, da Áustria, da Dinamarca, da Finlândia e da Suécia àqueles dois instrumentos bem como as respectivas Actas Finais e declarações;
- as decisões e as declarações adoptadas pelo Comité Executivo instituído pela CAAS;
- os actos adoptados em execução da CAAS pelas instâncias às quais o Comité Executivo tenha delegado competência decisória.

Do teor do Anexo, resulta que o acervo de Schengen constitui um conjunto híbrido de regras jurídicas, decisões políticas e medidas administrativas sem carácter normativo. Aplicando-lhe os princípios correntes da interpretação jurídica, para efeitos da adopção da decisão imposta ao Conselho pelo artigo 2º, nº 1, segundo parágrafo, primeira frase, resulta que tal decisão não deve obviamente integrar como acervo de Schengen todos aqueles actos mencionados no Anexo que, à data de entrada em vigor do TA, tenham esgotado os seus efeitos ou tenham sido revogados ou alterados. Para além deste “critério geral de não integração”, há que mencionar os “critérios especiais de não integração”, decorrentes dos mecanismos de substituição das disposições Schengen por disposições de direito comunitário, de direito da União Europeia ou de direito internacional convencional, previstos nos já citados artigos 134º e 142º da CAAS. Finalmente, a própria entrada em vigor do Protocolo fará caducar toda uma série de disposições mencionadas no Anexo.

O que precede basta para concluir que, de um ponto de vista estritamente formal, o conjunto do acervo de Schengen produzido até a data de entrada em vigor do TA e o acervo de Schengen definido pela decisão do Conselho a adoptar naquela data estarão longe de coincidir. Com efeito, e como se demonstrará a seguir, o acervo de Schengen, nesta última acepção, consistirá num conjunto de regras, decisões e medidas bem menos numerosas em comparação com o acervo na primeira acepção. Em contrapartida, de um ponto de vista material, e tendo em conta o objecto e o alcance do Protocolo, é indispensável que a coincidência seja absoluta. Em última análise, a diferença entre os dois conjuntos deverá ser de ordem quantitativa e não qualitativa.

9. Aplicando-se agora os critérios enunciados aos diferentes parágrafos do Anexo, resulta, em primeiro lugar, que o Acordo de 1985 – fundamentalmente concebido como um programa de trabalho de carácter geral – ficou sem objecto na sequência da entrada em vigor da CAAS. Relativamente a esta, o Acordo apenas se assumia como declaração de intenções, à imagem de um preâmbulo. Não é, por conseguinte, necessário incluir o Acordo de 1985, cujo valor é puramente histórico, na definição do acervo de Schengen para efeitos da sua integração na UE.

Em segundo lugar, no que respeita à CAAS, constata-se, à luz dos critérios gerais de não integração supramencionados, que ela nunca foi objecto de nenhuma revisão formal juridicamente eficaz. Com efeito, o único protocolo de revisão, assinado em Lisboa em 25 de Abril de 1997, ainda não entrou em vigor. Mesmo tal venha a ser o caso, o Protocolo de Lisboa ficará sem objecto na data de entrada em vigor do TA, tendo em conta que ele apenas visa subtrair a alteração de determinadas disposições da CAAS ao processo de revisão previsto no seu artigo 141º – o qual exige a ratificação, aprovação ou aceitação das alterações por todas as Partes Contratantes. Ora, em tal data, a CAAS converter-se-á em direito formalmente subordinado ao TUE e ao TCE e, por conseguinte, poderá ser alterada por simples acto do Conselho.

Por outro lado, tratando-se dos critérios especiais de não integração, é sabido que por força do artigo 142º da CAAS, os artigos 28º a 38º, relativos à determinação da Parte Contratante responsável pelo tratamento de um pedido de asilo introduzido no espaço Schengen, foram substituídos pela Convenção de Dublin relativa à determinação do Estado responsável pela análise de um pedido de asilo apresentado num Estado-Membro da UE, a qual entrou em vigor em 1 de Setembro de 1997. Uma vez excluídos os artigos 28º a 38º, torna-se igualmente supérfluo integrar na decisão do Conselho em causa a declaração nº 5 à Acta Final da CAAS, que se lhes refere.

Este é apenas um entre vários casos claros de substituição das disposições da CAAS por regras de direito comunitário ou de direito convencional. Mas há outros casos em que tal substituição não é tão clara. É designadamente o que sucede com os artigos 77º a 91º, relativos às armas de fogo e munições, perante a Directiva nº 91/477/CEE do Conselho de 18 de Junho de 1991, relativa ao controlo da aquisição e da detenção de armas. Se da comparação entre os dois conjuntos normativos resultar que as disposições dos artigos 77º a 91º da CAAS prevêm uma cooperação mais aprofundada do que a resultante da Directiva, tornar-se-á então necessário incluir na decisão do Conselho que define o acervo de Schengen as disposições da CAAS relativas a tal cooperação, a fim de que elas próprias substituam as disposições “ultrapassadas” da Directiva. Esta conclusão, que à primeira vista poderia parecer contrária às normas que regem as relações entre o direito comunitário e o direito Schengen, é todavia ditada pela declaração nº 15 à Acta Final do TA, segundo a qual as medidas adoptadas pelo Conselho que tenham por objectivo substituir as disposições da CAAS relativas à abolição dos controlos nas fronteiras comuns, incluindo obviamente as medidas compensatórias desta abolição, «devem garantir pelo menos o mesmo nível de protecção e de segurança» que as mencionadas disposições da CAAS.

Por sua vez, das disposições do Protocolo que constituem, elas próprias, fundamentos de não integração de determinadas disposições mencionadas no nº 2 do Anexo, pode citar-se o artigo 2º, nº 1, primeiro parágrafo, segunda parte, nos termos da qual, na data de entrada em vigor do TA, o Conselho substitui-se ao Comité Executivo instituído pela CAAS. Esta disposição torna evidentemente supérflua a integração das disposições da CAAS relativas ao Comité Executivo (artigos 131º a 133º).

No que toca, em terceiro lugar, aos instrumentos mencionados no nº 3 do Anexo, refira-se apenas não ser necessário integrar nenhuma das disposições dos Protocolos de Adesão ao Acordo de Schengen de 1985, tendo em conta não apenas que este Acordo não deve, como se viu, ser incluído na decisão do Conselho, mas também que o próprio artigo 1º do Protocolo autoriza expressamente estes Estados-Membros a prosseguir conjuntamente com os outros cinco a cooperação Schengen no âmbito da UE.

Por último, no que respeita às decisões e declarações do Comité Executivo, bem como aos actos adoptados por delegação deste, mencionados no nº 4 do Anexo, podem citar-se como exemplos de decisões que não devem ser integradas na decisão do Conselho, por terem esgotado os seus efeitos jurídicos, aquelas que se reportam aos orçamentos, quer do SIS quer do Secretariado de Schengen. Como exemplos de decisões substituídas por disposições de direito comunitário, pode citar-se a decisão do Comité Executivo que cria o modelo de vinheta de visto uniforme, substituída pelo Regulamento (CEE) nº 1683/95 do Conselho de 29 de Maio de 1995. Finalmente, como exemplo de actos cuja integração se torna supérflua com a entrada em vigor do Protocolo, podem citar-se as decisões do Comité Executivo estabelecendo o seu regimento interno e a forma das suas decisões, o processo escrito de urgência, o acordo administrativo e financeiro relativo ao Secretariado de Schengen, etc.

Resta ainda acrescentar que a interpretação do Anexo não determina apenas a exclusão, da definição do acervo de Schengen, de todas aquelas disposições, decisões ou medidas que, por uma razão ou por outra, se torna supérfluo integrar na decisão do Conselho baseada no artigo 2º, nº 1, segundo parágrafo, primeira frase. Com efeito, a correcta interpretação do Protocolo determina também a inclusão no acervo de Schengen de uma série de actos a que o Anexo se não refere expressamente. Entre tais actos, cabe mencionar principalmente os adoptados nos termos do artigo 115º, nº 3, da CAAS pela Autoridade de Controlo Comum (ACC) no exercício da sua competência em matéria de protecção dos dados pessoais inseridos no SIS. Estes actos constituem uma parte importante do acervo de Schengen em sentido material e devem, por isso mesmo, ser incluídos na decisão do Conselho em referência. Trata-se, no fundo, de proceder à interpretação extensiva do nº 4 do Anexo.

10. Tendo em conta o que precede, pode estimar-se que, das cerca de cento e setenta decisões e sessenta declarações adoptadas pelo Comité Executivo até ao final do primeiro semestre de 1998, apenas será necessário integrar no ordenamento da UE bem menos de metade de cada um destes conjuntos. Mas obviamente que tudo depende em última análise do consenso político que a este respeito se alcançar entre os treze Estados-Membros. Em todo o caso, e como já se referiu, a não adopção da decisão do Conselho em referência na data de entrada em vigor do TA também não obstará a que, por aplicação directa dos artigos 1º e 2º, nº 1, primeiro parágrafo, do Protocolo, a cooperação Schengen se transferisse efectivamente para o âmbito institucional e jurídico da UE. Apenas ficaria por fazer a triagem e a consolidação do acervo, que em última análise constitui o objecto da decisão do Conselho analisada.

É para «cada uma das disposições ou decisões» do acervo de Schengen identificadas em interpretação do Anexo que deverá ser encontrada uma base jurídica no TUE e/ou no TCE. Também esta operação se reveste de consideráveis dificuldades jurídicas e políticas, de que não cabe tratar no âmbito da presente comunicação. E não é de excluir que o facto de se saber de antemão que, se tal operação não chegar a bom termo antes da entrada

em vigor do TA, «as disposições ou decisões que constituem o acervo de Schengen são consideradas actos baseados no Título VI do TUE», venha a ser um não menosprezável estímulo para a não adopção da decisão imposta ao Conselho pelo artigo 2º, nº 1, segundo parágrafo, segunda frase, do Protocolo.

VI. As posições específicas do Reino Unido, da Irlanda e da Dinamarca face à integração do acervo de Schengen na União Europeia

11. A posição dos dois Estados-Membros da UE que não se encontram vinculados pelo acervo de Schengen – o Reino Unido e a Irlanda – é definida pelo artigo 4º do Protocolo, nos seguintes termos: ambos «podem, a todo o tempo, requerer a possibilidade de aplicar, no todo ou em parte, as disposições desse acervo», isto é, ambos podem prevalecer-se de uma faculdade de *opt-in*. Em toda a medida em que o não fizerem, manter-se-ão obviamente desvinculados do acervo. Por sua vez, a já citada declaração nº 45 incita o Reino Unido e a Irlanda a «fazerem uso» do artigo 4º por forma a que o Conselho possa deliberar sobre o respectivo pedido na data de entrada em vigor do TA, ou posteriormente, a todo o tempo, obtido o parecer da Comissão.

A flexibilidade de princípio introduzida pelo Protocolo relativamente à vinculação do Reino Unido e da Irlanda ao acervo de Schengen que será integrado na UE acentua-se ainda no que toca à participação futura destes dois Estados-Membros na adopção, pelo Conselho, de propostas ou iniciativas destinadas a desenvolver aquele acervo, com base no Título IV do TCE ou no Título VI do TUE. Com efeito, nos termos do artigo 5º, nº 1, segundo parágrafo, mesmo que nenhum dos dois Estados tenha, num prazo razoável, notificado por escrito o Conselho de que deseja participar nas áreas de cooperação em causa, a autorização para o fazerem considera-se tacitamente concedida.

O Protocolo é, todavia, omissivo no que respeita ao regime da vinculação do Reino Unido e da Irlanda às disposições de direito comunitário ou de direito da UE que venham a ser adoptadas sem a sua participação, já no âmbito da UE, em desenvolvimento do acervo de Schengen. Poder-se-ia pensar que, por analogia com o disposto no artigo 4º, os dois Estados-Membros apenas se podem associar à aplicação de tais medidas após decisão unânime do Conselho nesse sentido.

Esta não parece ser, no entanto, a solução mais defensável. Com efeito, em primeiro lugar, o regime do artigo 4º do Protocolo revela-se claramente excepcional em relação ao regime da associação de um Estado-Membro a uma cooperação reforçada já instituída, previsto genericamente no artigo 43º, alínea g), do TUE e especificamente no Título VI pelo artigo 40º, nº 3, bem como no TCE pelo artigo 11º, nº 3. O regime do artigo 4º do Protocolo contrasta ainda com o previsto no artigo 4º do Protocolo, também anexo ao TUE e ao TCE, relativo à posição do Reino Unido e da Irlanda no que respeita à sua associação a um outro caso de cooperação reforçada predeterminada que é precisamente o Título IV do TCE. Em todos estes

casos, para um Estado-Membro poder associar-se à cooperação reforçada em causa, basta uma autorização do Conselho, não por unanimidade mas por maioria qualificada. Além disso, uma coisa são as disposições e decisões do acervo de Schengen adoptadas ainda à margem da UE, outra são as medidas de desenvolvimento desse acervo que venham a ser adoptadas pelo Conselho, sob a forma e segundo os processos previstos nos TUE ou no TCE. Esta diferença substancial obsta definitivamente a que se estenda à segunda categoria a exigência de unanimidade prevista para a vinculação à primeira.

Por conseguinte, a determinação do regime aplicável à vinculação do Reino Unido e da Irlanda às medidas de desenvolvimento do acervo de Schengen adoptadas pelo Conselho sem a sua participação, deve, antes, fazer-se por analogia com o regime “mais próximo” do artigo 4º do Protocolo relativo à posição do Reino Unido e da Irlanda, onde se prevê que estes dois Estados-Membros podem, a todo o tempo, após a adopção pelo Conselho de uma medida em aplicação do Título IV do TCE, vincular-se a tal medida, para tanto bastando uma decisão por maioria qualificada do Conselho. Mal se compreenderia, com efeito, que o mesmo regime não vigorasse para as medidas de desenvolvimento do acervo de Schengen baseadas no Título IV do TCE e, por identidade de razão e em coerência com o artigo 40º, nº 3, do TUE, para as baseadas no Título VI deste. Tal entendimento é, de resto, o que melhor se coaduna com a declaração nº 46, pela qual os Estados-Membros se comprometem a envidar todos os esforços no sentido de tornar possível a acção de todos eles nos domínios do acervo de Schengen, em especial quando o Reino Unido ou a Irlanda tenham aceite, no todo ou em parte, as disposições desse acervo, nos termos do artigo 4º do Protocolo Schengen.

O recurso à analogia com o disposto no Protocolo sobre a posição do Reino Unido e da Irlanda relativamente ao novo Título IV do TCE, para colmatar lacunas do Protocolo Schengen não se confinará ao caso anterior. Na realidade, outro ponto importante relativamente ao qual este último protocolo se revela omissivo é o de saber como ultrapassar a situação em que não seja possível ao Conselho adoptar uma medida de desenvolvimento do acervo de Schengen com a participação do Reino e/ou da Irlanda, por bloqueio de um deles ou de ambos. Neste caso, a lacuna deve ser integrada por analogia com o disposto no artigo 3º, nº 2, do primeiro protocolo: se, decorrido um prazo razoável, não tiver sido possível adoptar uma tal medida com a participação do Reino Unido ou da Irlanda, o Conselho poderá-a adoptar sem estes, os quais obviamente não ficarão então vinculados por ela.

Todavia, a extensão em que o Reino Unido e a Irlanda pretenderão vincular-se ao acervo de Schengen a integrar na UE, participar no seu desenvolvimento ou vincular-se, em momento ulterior, às disposições entretanto adoptadas pelo Conselho, fica largamente condicionada pelo disposto no Protocolo, também anexo ao TUE e ao TCE, relativo à aplicação de certos aspectos do artigo 14º do TCE a estes dois Estados-Membros. Com efeito, os artigos 1º e 2º deste protocolo habilitam, sem qualquer reserva, o Reino Unido – e também a Irlanda, na medida em que se

mantiverem em vigor os convénios celebrados entre esta e o Reino Unido, relativos à circulação de pessoas entre os respectivos territórios (“Zona de Deslocação Comum”) – a instituir ou a exercer, nas suas fronteiras comuns com os outros Estados-Membros, os controlos sobre as pessoas que pretendam entrar nos respectivos territórios, quer com base no direito comunitário quer noutra base. No primeiro caso, os controlos serão fundamentalmente de identidade e documentação, ao passo que, no segundo, o protocolo em análise admite todos aqueles que forem considerados necessários. Além disso, habilitando o artigo 3º do mesmo protocolo os restantes Estados-Membros a procederem, em plena reciprocidade, a idênticos controlos sobre as pessoas que pretendam entrar nos seus territórios em proveniência do Reino Unido e da Irlanda, segue-se que tanto estes como os restantes Estados-Membros, nas suas relações com os primeiros, ficam irrestritamente dispensados de aplicar o “núcleo duro” do acervo de Schengen, ou seja, a supressão de quaisquer controlos de pessoas nas respectivas fronteiras comuns.

12. Para além do Reino Unido e da Irlanda, o Protocolo Schengen contempla ainda, no seu artigo 3º, o caso particular da Dinamarca. Fá-lo em conjugação com o Protocolo também anexo ao TCE e ao TUE, relativo à posição deste Estado-Membro e que lhe concede um *opt-out* relativamente ao Título IV do TCE, com excepção das disposições que, nos termos deste, determinem quer a lista dos países terceiros cujos nacionais devem ser detentores de visto para transporem as fronteiras externas dos Estados-Membros, quer o modelo-tipo de visto (artigos 1º, 2º e 4º). Apesar de se contar entre os treze Estados Schengen, a Dinamarca beneficia de um regime especial no que respeita quer à adopção das medidas de desenvolvimento do acervo de Schengen propostas e adoptadas pelo Conselho com base no Título IV do TCE, quer à vinculação às mesmas.

Assim, no que se refere ao primeiro aspecto, não está prevista a possibilidade de a Dinamarca participar na adopção de tais medidas — tal como não está prevista a possibilidade de participar na adopção de quaisquer outras medidas propostas em aplicação do Título IV do TCE. No que se refere ao segundo aspecto, o artigo 5º, nº 1, primeira parte, do Protocolo relativo à posição da Dinamarca concede a este Estado-Membro um *opt-in* absolutamente original, ao habilitá-lo a decidir no prazo de seis meses se transporá para o seu direito interno os actos de direito comunitário adoptados pelo Conselho com base em propostas ou iniciativas destinadas a desenvolver o acervo de Schengen ao abrigo do Título IV do TCE. Se decidir fazê-lo, a segunda parte da mesma disposição precisa que tal decisão «criará uma obrigação de direito internacional» entre a Dinamarca e os restantes Estados Schengen, «bem como entre a Irlanda ou o Reino Unido, se estes Estados-Membros participarem nos domínios de cooperação em causa». Se decidir não o fazer, os restantes Estados Schengen e, sendo caso disso, a Irlanda e/ou o Reino Unido «analisarão as medidas adequadas a tomar» nos termos do artigo 5º, nº 2, do protocolo em análise. De forma apriorística aponta-se aqui para uma situação claramente anómala, em que um acto adoptado com base no novo Título IV do TCE pode relevar no âmbito da UE simultaneamente do direito comunitário e do direito internacional.

Em contrapartida, no que respeita ao acervo de Schengen, enquanto conjunto de disposições, decisões e medidas adoptadas nos termos da CAAS, a integrar na UE na data de entrada em vigor do TA, a Dinamarca mantém-se integralmente vinculada por ele, independentemente de as respectivas bases jurídicas se encontrarem no Título IV do TCE ou no Título VI do TUE. É o que resulta do citado artigo 3º do Protocolo Schengen. Por outro lado, a Dinamarca participa obrigatoriamente na adopção das medidas de desenvolvimento do acervo de Schengen a adoptar pelo Conselho com base no Título VI do TUE e fica por elas, sem excepção, vinculada.

13. Para se perceber melhor o alcance das soluções especiais consagradas, por um lado, para o Reino Unido e a Irlanda e, por outro, para a Dinamarca, convém proceder a uma comparação entre ambas. E dela resulta claramente que as diferenças são substanciais.

Em primeiro lugar, avulta o facto de a Dinamarca, ao contrário do Reino Unido e da Irlanda, ficar vinculada à totalidade do acervo de Schengen que, na data de entrada em vigor do TA, for integrado no âmbito da UE, quer ele se considere baseado no novo Título IV do TCE quer no Título VI do TUE. Em segundo lugar, ao contrário do Reino Unido e da Irlanda, a Dinamarca não beneficia de qualquer *opt-out* em relação ao Título VI do TUE especificamente para as medidas de desenvolvimento do acervo de Schengen nele baseados. Em terceiro lugar, e com repercussão directa na cooperação Schengen, o *opt-out* da Dinamarca relativamente ao Título IV do TCE é mais restrito do que o do Reino Unido e da Irlanda.

Além disso, se o Reino Unido e a Irlanda fizerem uso do *opt-in* de que genericamente dispõem no âmbito do Título IV do TCE, relativamente às medidas de desenvolvimento do acervo de Schengen (e a quaisquer outras) nele baseadas, ficarão vinculados por actos de direito comunitário, adoptados sob a forma e com a força jurídica previstas no artigo 249º do TCE e segundo o processo do artigo 67º, nº 1, e sujeitos ao controlo do Tribunal de Justiça nos termos do artigo 68º. Assumirão, portanto, obrigações de direito comunitário. Diferentemente, se a Dinamarca fizer uso da sua faculdade de *opt-in*, limitada às medidas de desenvolvimento do acervo de Schengen adoptadas com base no Título IV do TCE, ficará vinculada a adoptar actos de direito interno com um conteúdo idêntico ao daquelas medidas de direito comunitário. Só através da sua transformação em direito interno é que tais medidas serão aplicáveis no ordenamento dinamarquês e não enquanto direito comunitário. Este “dualismo” é manifestamente contrário ao princípio geral da aplicabilidade directa do direito comunitário nos ordenamentos dos Estados-Membros.

Em última análise o que distingue o Protocolo relativo ao Reino Unido e à Irlanda do Protocolo relativo à Dinamarca é a natureza da reserva que motivou a respectiva negociação. O primeiro Protocolo exprime claramente uma reserva quanto ao conteúdo da cooperação Schengen, na parte em que ela impõe a supressão dos controlos de pessoas nas fronteiras internas. O segundo Protocolo, representando de algum modo um corolário da solução

especial consagrada para a Dinamarca pela Decisão dos Chefes de Estado e de Governo, reunidos no Conselho Europeu de Edimburgo, em 12 de Dezembro de 1992, e da posição aí explicitada por este Estado-Membro, traduz, em última análise, não tanto uma reserva quanto ao conteúdo da cooperação Schengen, mas antes uma reserva quanto ao prosseguimento de tal cooperação na UE através de outro método que não o estritamente intergovernamental. Todavia, a expressão jurídica que assumiu o compromisso político a este respeito alcançado é certamente das mais problemáticas.

VII. Observações finais

14. Tendo em conta as fragilidades institucionais que caracterizam a estrutura de concertação permanente criada pela CAAS e, nomeadamente, a sua falta de abertura e de transparência, bem como as suas fragilidades jurídicas e, em especial, o défice de publicidade e de controlo das disposições adoptadas no seu âmbito, é-se levado a considerar que a integração do acervo de Schengen na UE — com a publicidade, a participação parlamentar e o controlo jurisdicional, a nível central, que pressupõe, e o desenvolvimento futuro desse acervo num quadro institucional e jurídico mais sólido, democrático e transparente, apesar das suas insuficiências a este respeito — representa um progresso considerável. E isto, apesar de ser forçoso constatar que o Protocolo não colocou todas estas vantagens comparativas da UE ao serviço de tal integração.

Com efeito, o tipo de processo decisório para que invariavelmente remetem as diversas ordens de legislar contidas no Protocolo permite ao Conselho agir sem qualquer influência da Comissão e do Parlamento Europeu. Ora esta solução presta-se a sérias críticas. Em primeiro lugar, a uma crítica de ordem geral: tratando-se de matérias que relevam essencialmente dos novos Título VI do TUE e Título IV do TCE, seria lógico que o processo decisório escolhido se inspirasse, pelo menos, nas disposições que o TA aí introduz a fim de tornar mais democráticas e transparentes as decisões que o Conselho tomará ao seu abrigo. Entre tais disposições figuram os artigos 39º, nº 1, do TUE e 67º do TCE, que prevêem a competência consultiva obrigatória do Parlamento Europeu no âmbito de aplicação de ambos os Títulos. Esta crítica geral torna-se particularmente pertinente quanto ao artigo 2º, nº 1, segundo parágrafo, que impõe ao Conselho a definição do acervo de Schengen e a sua recondução a uma base jurídica nos tratados. Com efeito, é certamente contrário aos princípios pertinentes que, através do processo descrito, um conjunto de regras jurídicas e de decisões políticas como o que constitui o acervo de Schengen passe a integrar a ordem jurídica da Comunidade e da UE sem qualquer participação do Parlamento Europeu, a quem cabe o controlo democrático e a representação dos interesses dos cidadãos a nível central.

Independentemente deste aspecto bastante criticável, o preço a pagar pela integração de Schengen na UE é sem dúvida elevado, já que, através dela, se introduz uma dualidade de regimes num domínio nuclear da própria UE, que é precisamente a livre circulação de pessoas. É certo que o TA acentua

o carácter excepcional e desejavelmente transitório dos regimes aplicáveis quer ao Reino Unido e à Irlanda quer à Dinamarca, ao sublinhar que a cooperação Schengen se destina «a reforçar a integração europeia e, em especial, a possibilitar que a União Europeia se transforme mais rapidamente num espaço de liberdade, de segurança e de justiça» e que, por isso mesmo, está particularmente vocacionada para se tornar extensiva a todos os Estados-Membros. Note-se, de resto, que uma hipotética aceitação da totalidade do acervo de Schengen pelos Estados-Membros que negociaram um *opt-out* global ou parcial marcará logicamente o fim do estatuto de cooperação reforçada atribuído pelo Protocolo à cooperação baseada naquele acervo. Mas enquanto isto não se tornar realidade – e, como se viu, há sérios obstáculos a que se torne – ninguém duvidará que o verdadeiro *puzzle* que constitui a articulação dos diversos regimes excepcionais analisados será uma considerável fonte de dificuldades.

Nesta perspectiva, pode considerar-se positivo o facto de o artigo 8º do Protocolo dispor que não só o acervo de Schengen como as medidas adoptadas em seu desenvolvimento no âmbito da UE devem ser integralmente aceites por todos os Estados candidatos à adesão, excluindo, portanto, qualquer flexibilidade a seu respeito neste domínio. O Protocolo acentua, assim, mais firmemente do que em qualquer outra hipótese de cooperação reforçada, a vocação “universal” da cooperação Schengen.

Por estes motivos, a cooperação Schengen não pode deixar de ser encarada como um caso especial relativamente a todas as outras formas de cooperação reforçada introduzidas pelo TA. É, aliás, o que confirmam três disposições do mesmo teor, constantes do artigo 40º, nº 5, do TUE e do artigo 11º, nº 5, do TCE, relativos à cooperação reforçada, e do artigo 7º do Protocolo relativo à posição do Reino Unido e da Irlanda, nos termos dos quais o disposto nestes artigos, ou naqueles para os quais remetem, não prejudica o Protocolo Schengen.

15. Apesar de todos os aspectos negativos assinalados, não é exagero afirmar que o Protocolo Schengen traduz um dos mais importantes resultados alcançados em Amesterdão. E esses aspectos serão em boa medida compensados se o pragmatismo e a capacidade de inovação e de resposta às situações urgentes, até aqui demonstrados no âmbito da cooperação Schengen, não se perderem com a integração na UE, mas, ao contrário, firmemente a impregnarem. Se tal for o caso, a UE ganhará também em eficácia e dinamismo.

O tempo dirá se, tal como o equacionou uma conhecida académica, o Protocolo Schengen é um modelo atraente ou, afinal, um cálice envenenado. Em termos menos radicais, poder-se-lhe-á aplicar a sugestiva mas intraduzível expressão inglesa que, mais moderadamente, o comentário citado no início aplica genericamente ao TA, pretendendo significar que, se ele não é um sucesso, também não é um fracasso: «*neither a bang nor a whimper*». Tal como o TA, o Protocolo limita-se a reflectir o limitado compromisso que foi possível encontrar a quinze numa UE em transição.

O Sistema de Informação Schengen: a importância da cooperação entre os Estados

Frank Demot

Presidente do Grupo Central de Schengen

Introdução

O Sistema de Informação Schengen é indubitavelmente o melhor ficheiro europeu de informação. Contém actualmente mais de 6,5 milhões de indicações, sendo cerca de um milhão delas referentes a pessoas. No final de 1996 continha cerca de 4 milhões e no final de 1997 cerca de 5,5 milhões. Significa portanto um impressionante aumento.

Em 1996 mais de 32.000 indicações foram objecto de resposta positiva, e em 1997 mais de 36.000.

Mas Schengen é mais do que um mero sistema de informação. Schengen é também uma cada vez maior cooperação policial em muitos domínios específicos, tais como a entrada e permanência ilegais de estrangeiros, a luta contra a droga, o furto de veículos, etc. e a correspondente troca de informações, em especial nas zonas fronteiricas.

1. Causas

A primeira e de longe a principal causa da cada vez maior cooperação policial é indiscutivelmente o facto da criminalidade estar cada vez mais organizada, transpondo as fronteiras.

Acresce que por vezes é difícil fazer uma distinção entre actividades económicas e actividades criminosas, pois as associações criminosas cada vez mais entrelaçam ambas as actividades por forma a camuflar o crime. Assim, muitas vezes o produto das actividades criminosas é injectado no circuito económico, como capital inicial duma actividade económica legal.

Por vezes as organizações criminosas parecem-se com autênticas multinacionais. Pelo seu carácter internacional e pela sua consequente grande mobilidade, a luta por parte dum Estado, utilizando as mesmas armas contra esta forma de criminalidade é ainda mais difícil.

Também as formas mais correntes de criminalidade, tais como roubos "por esticção" e de carteiras, furto de obras de arte e roubos a lojas, adquirem cada vez mais uma dimensão internacional. Deste modo, há grupos de carteiristas e de ladrões "por esticção", que actuam num ou em vários continentes segundo o mesmo padrão, acompanhando manifestações desportivas.

Todavia, é também inegável que a luta contra a criminalidade organizada por vezes encobre outros objectivos, políticos ou militares. Isto não é uma coisa que fomente a confiança mútua entre os Estados.

A luta contra o crime organizado exige também cada vez mais conhecimentos especializados. Só poucos Estados dispõem de especialistas em todos os domínios. Daí também o interesse em intercâmbios internacionais.

Também na Europa a cooperação policial está a aumentar. No contexto de Schengen a supressão das fronteiras internas serve de corolário para um aumento da cooperação policial internacional.

Todavia, persistem fortemente as ideias de soberania. A tendência para reforçar o poder executivo na Europa não lhes é certamente alheia. A tenacidade de Schengen deve-se sobretudo ao seu carácter intergovernamental. O perigo de que Schengen depois da integração na União Europeia se venha a tornar num castelo de areia, não é de todo em todo impensável.

Quando é necessária uma cooperação policial internacional mais intensa, verifica-se ser a emergente sociedade de informação a plataforma onde esta cooperação pode assentar. Uma consequência disso, não negligenciável, será o rápido crescimento da cooperação entre as forças policiais e os serviços de vigilância e segurança do sector privado.

II. Sociedade da protecção

A cada vez maior mobilidade e o desenfreado desenvolvimento dos meios de comunicação e da técnica, tem como consequência um incremento crescente da sociedade da protecção. As autoridades pretendem manter estas novas tendências sob controlo.

Esta tendência para o controlo, é fortemente fomentada pela informática. Cada vez é mais ténue a fronteira entre vida privada e vida pública, e com a ajuda de todo o tipo de dados, como por exemplo informações do registo criminal, extractos de conta, registos, ficheiros de clientes, etc., podem-se organizar dossiers individuais pormenorizados.

A possibilidade ilimitada de guardar dados tem como consequência um crescimento explosivo da técnica da análise criminal. A chamada 'white coliar criminality', cada vez mais importante, tem aqui um papel preponderante. Não se pode analisar melhor o branqueamento de capitais do que com a ajuda da informática.

A pesquisa através de bancos de dados não está todavia isenta de riscos. Não é apenas imaginário o risco de que, da massa de dados, sejam pura e simplesmente extraídos artificialmente determinados perfis. A deslocação da

informação torna o controlo da fiabilidade da informação cada vez mais difícil. Além disso, a pesquisa através de bancos de dados gera dificuldades aos serviços de polícia para trocarem, com total independência, dados criminais com autoridades congêneres no estrangeiro.

III. Finalidade

Por vezes, a independência da competência da cooperação informática é legitimada juridicamente pela finalidade visada. Deste modo, procede-se a uma distinção entre finalidade essencialmente policial e finalidade essencialmente judiciária.

A informação essencialmente policial é a informação recolhida pelos serviços de polícia que não é directamente utilizada para efeitos de prova num processo judicial.

Em contrapartida, a informação essencialmente judiciária tem por vocação a prestação de prova num processo penal.

A informação policial "for police use only" tem o seu fundamento na morosidade das autoridades judiciárias, o que não a deve justificar.

A cooperação internacional aumenta fortemente as possibilidades de contornar as garantias constituídas por um controlo judiciário e administrativo.

Schengen tenta sanar parcialmente este mal, através do nº 2 do artigo 39º, o qual prevê que as informações policiais escritas que forem prestadas, só podem ser utilizadas para efeitos de prova dos factos incriminados, com o consentimento das autoridades do país requerido. Porém, este consentimento só é necessário quando esta informação for prestada por escrito e servir de meio de prova, e não como informação prestada para outros efeitos, como por exemplo, para análise criminal.

Deve-se portanto evitar absolutamente, que os serviços de polícia trabalhem em *stand-alone*.

IV. Não ao *stand-alone*

Nos dicionários de informática, "stand-alone" é definido como sendo a característica dum aparelho, por exemplo um PC, que funciona pelos seus próprios meios, isto é, sem condução externa, e que portanto não está ligado a (outros) computadores.

Os serviços de polícia não podem trabalhar em "stand-alone". Por isso, dever-se-á verificar atentamente se os serviços de polícia, não se aproveitam do contexto internacional para adquirirem mais autonomia e, por conseguinte, escaparem ao controlo das autoridades administrativas e judiciárias.

Todavia, a tendência que se desenvolve vai no sentido contrário. Em grande medida isso deve-se à protecção, por parte do cada vez mais forte poder executivo, dos seus serviços de polícia operacionais.

Este impulso para a independência tem também um fundamento na chamada investigação pro-activa. Na fase pro-activa da investigação, o Ministério Público só intervém, na maioria das vezes, quando são necessárias técnicas de investigação especiais. Nestas circunstâncias, são executados muitos trabalhos de investigação em casos concretos, sem que tal seja comunicado ao Ministério Público. Visto que os serviços de polícia recolhem e trocam eles próprios informação relativa a factos e circunstâncias que precederam os factos puníveis, cria-se deste modo muita informação "for police use only".

O artigo 46º da Convenção de Schengen permite aos Estados membros comunicar por iniciativa própria, sem que tal lhes seja solicitado, a outro Estado membro, informações que se possam revelar importantes com vista à assistência em matéria de repressão de crimes futuros, à prevenção de crimes ou à prevenção de ameaças para a ordem e segurança públicas.

Este artigo é indubitavelmente um primeiro passo no sentido duma base legal para a investigação pro-activa. Dado que esta disposição está sujeita ao cumprimento da legislação nacional, não constitui, por agora, nenhum meio autónomo de entreatajuda judiciária.

No âmbito de Schengen é possível a cooperação tanto na área da informação administrativa como na da informação judiciária. Deste modo, é divulgado no SIS informação sobre *hooligans* que operam a nível internacional. Schengen visa tanto a prevenção como a repressão. A troca de informação administrativa deverá decorrer sob uma vigilância atenta pro-activamente ou sob um controlo estrito das autoridades administrativas.

No domínio jurídico, a cooperação em termos de informação policial pode ser independente, relativamente à troca de informação estratégica, de informação sobre factos conhecidos e retirados de bases de informação de acesso geral, e relativamente à informação relacionada com a investigação, caso haja uma base jurídica para o fazer. As autoridades judiciárias deverão também estar ao corrente de toda a informação comunicada. Contudo, pedidos de informação política estratégica poderão esconder determinadas outras estratégias.

V. **Canais Schengen de informação**

O Acordo de Schengen de 1985 estipula que as partes, no respeito pela sua legislação nacional, se esforçarão por melhorar o intercâmbio de informação e reforçar a troca de dados que possam ser úteis às outras partes.

Na Convenção de Schengen de 1990, a troca de dados não se limita à criação do Sistema de Informação Schengen. Numerosos artigos tornam igualmente possível a troca de dados no terreno.

Esta forma de cooperação não se limita ao intercâmbio de dados judiciais e policiais, abrangendo também a cooperação em termos de dados administrativos e de informação, como por exemplo no caso da aquisição de armas e no do transporte de drogas.

Os artigos 39º e 46º da Convenção de Aplicação de Schengen permitem uma estreita cooperação em termos de informação policial, tanto a nível judiciário como administrativo. O artigo 39º prevê que os serviços de polícia se podem assistir mutuamente tanto no domínio da investigação como no da prevenção de factos puníveis, quando receberem um pedido nesse sentido. O artigo 46º regula a transmissão de informação entre autoridades policiais sem que para o efeito tenha sido recebido um pedido. Este artigo limita-se exclusivamente à transmissão de informação policial administrativa.

Ambos estes artigos constituem disposições extremamente complexas, que deixam ainda margem para uma interpretação jurídica.

O artigo 39º da Convenção de Aplicação de Schengen estipula que quando as autoridades policiais requeridas não são competentes para tratar do pedido, o transmitem às autoridades efectivamente competentes.

Daqui transparece claramente que os Estados Schengen conferem às suas autoridades policiais poderes para trocarem entre si dados policiais judiciais ou administrativos. A resposta aos pedidos de informação é limitada tanto em termos operacionais como jurídicos. Todavia, a polícia continua a não ter competências para responder a pedidos, quando estes não se inscrevem no seu quadro legal.

O artigo 47º da Convenção de Aplicação de Schengen pretende promover e acelerar a cooperação entre os Estados membros, através do destacamento de oficiais de ligação. Estes não desempenham funções operacionais, mas sim de consulta e assistência.

O principal canal Schengen de informação é o Sistema de Informação Schengen. Trata-se duma rede de bancos de dados nacionais (N-SIS), consultáveis automaticamente, interligados através do sistema central (CSIS). A principal função do C-SIS é garantir a integridade dos dados.

A Convenção de Schengen não exclui *a priori*, como é o caso da Interpol, indicações relativas a determinados crimes, como por exemplo, os crimes políticos. O SIS é pois mais do que um banco de dados policiais para "crimes de direito comum". Tal transparece do próprio leque de serviços que podem consultar o banco de dados. Estes serviços são enumerados no artigo 101º da Convenção de Aplicação de Schengen, e são eles: as autoridades responsáveis pelos controlos fronteiriços, pelas outras verificações de polícia e aduaneiras efectuadas no interior do país, bem como a respectiva

coordenação, e as autoridades que concedem vistos e títulos de residência e que procedem ao controlo dos estrangeiros. Daí, a diferença clara entre Schengen e a Interpol.

O artigo 39º da Convenção de Aplicação de Schengen estipula que os pedidos de assistência bem como as respostas a esses pedidos podem ser trocados entre os órgãos centrais das diferentes Partes Contratantes encarregados da cooperação policial internacional, ou seja, os chamados Gabinetes SIRENE.

VI. Protecção de dados

Antes de analisarmos como é feita a protecção de dados no quadro da Convenção de Aplicação de Schengen, penso ser oportuno vermos como é assegurada a protecção de dados noutra instituição de cooperação policial em termos de informação, a saber, a Interpol.

Os estatutos da Interpol determinam, nas suas disposições introdutórias, que é função desta organização a actividade policial no espírito da Declaração Universal. Esta declaração de princípios tem em muitos países apenas o carácter duma declaração de intenções, não dispondo de qualquer força jurídica. Além disso, a Interpol não tem a possibilidade de punir as infracções aos seus estatutos nem de sancionar o seu desrespeito. Isto constitui uma importante carência em termos de democracia.

A Interpol nunca se submeteu a quaisquer disposições nacionais de protecção de dados. A regulamentação Interpol em matéria de dados só surgiu em 1983. Na sequência desta regulamentação, qualquer cidadão interessado tem o direito de solicitar uma verificação à Interpol.

Mas porque em lado nenhum se fala dum nível mínimo, a lista dos crimes ou factos que podem dar lugar a cooperação pode ser muito imprecisa. Basta apenas que um comportamento num determinado país seja considerado crime.

Os estatutos da Interpol permitem a cooperação entre "todas" as autoridades policiais dos diferentes países. Daí que muitos utilizadores não estejam sujeitos a um sistema de protecção de dados.

Também não há qualquer controlo da utilização que os gabinetes nacionais fazem da infra-estrutura de telecomunicações. Esta forma de divulgação de dados pessoais é muito mais difícil de controlar por parte do cidadão.

7

Os oficiais de ligação são considerados pela Interpol como agentes nacionais. Por isso podem fazer praticamente o que quiserem em termos de intercâmbios de dados pessoais.

Do ponto de vista democrático, a ratificação da Convenção de Aplicação de Schengen pelos diferentes parlamentos, constitui sem dúvida uma mais-valia e uma vantagem relativamente à Interpor. Por agora os acordos de Schengen ainda estão fora do direito comunitário e do controlo do Tribunal de Justiça das Comunidades Europeias. Depois da entrada em vigor do Tratado de Amsterdão, será posto termo a esta situação.

Embora a Convenção de Aplicação de Schengen no seu título mencione a supressão gradual dos controlos nas fronteiras comuns, podem todavia colocar-se algumas questões.

Logo desde o início da entrada em vigor que se recorre à aplicação do procedimento excepcional previsto no n.º 2 do artigo 2.1. Este parágrafo dispõe que «por razões de ordem pública ou de segurança nacional, uma Parte Contratante pode, após consulta das outras Partes Contratantes, decidir que, durante um período limitado, serão efectuados nas fronteiras internas controlos fronteiriços nacionais adaptados à situação. Se razões de ordem pública ou de segurança nacional exigirem uma acção imediata, a Parte Contratante em causa tomará as medidas necessárias e informará desse facto, o mais rapidamente possível, as outras Partes Contratantes.»

É claro que conceitos como "ordem pública" e "segurança nacional" se prestam a vastas interpretações.

1

A questão que se coloca é a de saber em que medida os controlos efectuados estão adaptados à situação. Não está correcto, e tem um efeito desproporcional, associar estes controlos fronteiriços às chamadas medidas compensatórias. Existe o perigo desses controlos recaírem sobretudo sobre estrangeiros. As chamadas brigadas móveis holandesas do "Mobiel Toezicht Vreemdelingen" (Controlo Móvel de Estrangeiros) são um exemplo ilustrativo disso.

O facto de com a aplicação da Convenção de Schengen pela primeira vez se trocar informação policial internacionalmente, dissociada da cooperação judiciária internacional, comporta um risco real. Tanto as autoridades judiciárias como as administrativas deverão fomentar o exercício de controlos sobre a recolha de informação policial internacional.

1

Dado que no quadro da Convenção de Aplicação de Schengen o direito de acesso está sujeito a rigorosas condições, o regime de protecção de dados não é certamente o ideal. Este regime contém também muitas excepções, sendo complexo e pouco claro.

8

A Convenção de Aplicação de Schengen não contém nenhuma referência à Convenção Europeia dos Direitos do Homem. Depreende-se pois que os direitos humanos não constituem uma prioridade Schengen, mas a eficácia da cooperação policial sim.

A consequência disso é que no contexto de Schengen, há um enfraquecimento do direito de defesa. Dado o suspeito não ter acesso directo aos dados disponíveis no estrangeiro, fica fortemente dependente do esforço que o seu juiz quiser consagrar à verificação da exactidão dos meios de prova reunidos no estrangeiro.

CONCLUSÃO

Desta nossa exposição, não se pode certamente concluir que nós entendemos que no domínio da cooperação internacional, os serviços de polícia devem ser abordados com uma certa dose de desconfiança.

Ao contrário, achamos que os serviços de polícia, organizados de forma profissional, são um garante do nosso regime democrático. Os serviços de polícia mal formados e insuficientemente equipados dependem demasiado das circunstâncias. Mais, nunca poderíamos contar com a confiança da população, o que é uma condição *sine qua non* para uma política policial democrática.

O que nós pretendemos sobretudo sublinhar é que uma cooperação policial internacional mais intensa deverá estar formosamente associada um controlo judiciário e administrativo também mais intenso. Os serviços de polícia funcionam integrados na sociedade e não em *stand-alone*.

Também se deverá dedicar muita atenção à integração do acervo de Schengen na União Europeia. É que a União Europeia não é nenhuma Utopia, onde reina a mais perfeita harmonia.

Existe, por um lado, o risco da primeira prioridade de Schengen, ou seja, a cooperação policial, adquirir, por falta de controlo eficaz, uma dimensão desmesurada, e por outro lado, o balanço inegavelmente positivo cair nas teias duma maior burocracia.

Por isso, há que velar por que esta integração não ocorre demasiado bruscamente. Com efeito, o controlo intergovernamental constitui também um ponto positivo para o qual não se encontra facilmente substituto.

Na sequência desta integração, a Autoridade de Controlo Comum é igualmente investido duma missão mais importante. A ACC deverá verificar que esta operação não implica um défice em termos de democracia. Depois, a ACC deverá ter que efectuar o seu controlo num contexto mais difícil e mais lato. Comprometemo-nos desde já a dar-lhe todo o nosso apoio nesse sentido.

Tinha-me sido pedido que com a minha exposição desse um contributo para o debate. Embora não sendo um especialista nesta matéria altamente delicada, que é a protecção de dados, espera que no entanto tenha podido ser útil com a minha intervenção.

A protecção de dados na coordenação da informação nacional
e na comunicação entre os Estados

Ester Guedes

Coordenadora do Gabinete Nacional SIRENE

Honrou-me a Autoridade de Controlo Comum de Schengen com este convite para aqui vir falar sobre a protecção de dados na coordenação da informação nacional e na comunicação entre os Estados.

A experiência dos gabinetes SIRENE e do SIRENE Portugal em particular, nesta matéria, é apta a sustentar a afirmação de que hoje, o tratamento e a difusão da informação de carácter policial (é desta que aqui se trata), a par dos critérios de rigor, fiabilidade e celeridade que se exigem, terão de cunhar-se no respeito pelos princípios e regras relativas à protecção da vida privada dos cidadãos.

Vivemos hoje uma realidade de planetização que não é virtual. A internacionalização dos interesses anda de mãos dadas com a internacionalização dos problemas e cada vez mais aos Estados se exigem soluções novas, adequadas e até comuns. Dizia Teilhard de Chardin em *L'Avenir de l'Homme* que «nos encontramos na era da unificação, tecnificação, racionalização crescente da Terra humana (...) Seria necessário fechar os olhos ante o espectáculo do mundo para imaginar que poderíamos escapar a qualquer das três correntes de fundo».

A esta internacionalização dos interesses e dos problemas e a esta unificação, não foi alheia a assinatura do Acordo de Schengen, que permitiu que alguns Estados membros da União Europeia, a despeito das dificuldades desta, e através de processos de cooperação intensa e prática, criassem um

espaço geográfico comum, onde a quarta liberdade prevista no Tratado de Roma foi efectivamente implantada - a liberdade de circulação de pessoas.

Com Schengen inicia-se o que sem sofisma se poderá chamar de uma nova era de cooperação policial europeia, cooperação essa que se verifica antes mesmo da entrada em vigor do Acordo e da respectiva Convenção de Aplicação e que, depois de 26 de Março de 1995, se tem vindo a traduzir numa cada vez maior multiplicação dos contactos internacionais e da troca de informação, a par de um patente aumento na qualidade das regras, das formas e dos meios de cooperação, em cuja concepção se enformam e se cumprem objectivos de segurança da informação e de garantia de protecção da vida privada dos cidadãos.

Com efeito, a Convenção de Aplicação do Acordo de Schengen não se quedou pela estatuição e adopção de determinadas regras e medidas de natureza legislativa, mas impôs mesmo aos Estados Parte a criação (nos casos em que, de direito ou de facto, ainda não existiam) de entidades nacionais de controlo independentes, de uma entidade de controlo comum e de meios técnicos arquitectados segundo regras precisas tendentes a evitar desvios àquele objectivo.

Naquelas regras e nestes meios centrarei agora esta minha exposição. Como medida compensatória do défice de segurança provocado pela abolição dos controles nas fronteiras internas, foi criado o Sistema de Informação Schengen, que passarei a designar simplesmente por SIS, e cuja operatividade e operacionalidade efectivas são, para cada Estado, condição *sine qua non* de vigência da Convenção de Aplicação de Schengen (o que implica igual e necessariamente a existência e normal funcionamentos do respectivo gabinete SIRENE).

O SIS, a que se dedica todo o Título IV da Convenção de Aplicação, poderá caracterizar-se muito rapidamente como uma base de dados policiais comum a todos os Estados Schengen, dados esses sobre pessoas, veículos, armas, documentos e notas de banco, que constituem indicações.

As pessoas, os veículos ou os objectos só podem ser indicados no SIS pelos motivos e para os fins enunciados nos artigos 95º a 100º da Convenção. A saber:

- as **pessoas**, independentemente da sua nacionalidade, poderão ser indicadas para efeitos de detenção provisória com vista à extradição; por motivo de desaparecimento; para detecção e colocação em segurança no seu próprio interesse (caso de menores e de pessoas sofrendo de perturbações mentais, desaparecidos); para determinação do paradeiro sempre que devam comparecer, no âmbito de um processo penal, perante as autoridades judiciais para responderem por factos que lhes são imputados, serem notificadas de uma sentença penal, cumprirem uma pena privativa de liberdade ou testemunharem em processo; podem ser indicadas para serem objecto de vigilância discreta ou de um controlo específico por motivos penais ou de segurança do Estado e, finalmente, no que exclusivamente concerne a cidadãos estrangeiros (isto é, não membros das comunidades europeias), para efeitos de não admissibilidade no território Schengen.
- Os **veículos** poderão ser inseridos para vigilância discreta e controlo específico pelos mesmos motivos que as pessoas e ainda para efeitos de apreensão, tal como os **documentos em branco, os documentos emitidos e as armas de fogo.**

Nos termos do nº 3 do artº 94º da Convenção, no que respeita às pessoas, só podem ser inseridos no SIS os seguintes elementos: o nome próprio, apelidos, alcunhas, os sinais físicos particulares objectivos e inalteráveis, a primeira letra do segundo nome próprio, a data e o local de nascimento, o sexo, a nacionalidade., a indicação de que a pessoa em causa está armada, que é violenta e ainda, naturalmente, a conduta a adoptar perante a pessoa indicada. Nenhuma outra referência é permitida e é possível. Digo possível porque, como atrás afirmei, em Schengen foi-se mais longe do que a simples estatuição de limites normativos: criaram-se limites de ordem técnica que impedem que outras referências, que não as permitidas pela Convenção, sejam introduzidas no Sistema. Com efeito, a inserção das indicações no

SIS é condicionada a campos e tabelas de referência, não havendo lugar para outro tipo de informação ou mesmo para a introdução de texto livre.

Também no que concerne aos motivos da procura e às condutas a adoptar, estão as mesmas definidas em códigos e tabelas de coerência que não permitem a inserção de dados por outros motivos ou para execução de outras condutas diferentes das previstas na Convenção, sendo igualmente impossível fazer corresponder a um motivo uma acção diferente daquela que a Convenção prevê.

Por outro lado, as indicações a inserir no SIS terão de obedecer aos critérios estabelecidos na Convenção e em decisões e recomendações do Comité Executivo e terão de ser exactas, actuais e lícitas.

Aqui a Convenção, no artº 105º, estatui igualmente um importante princípio – o da responsabilização do Estado autor das indicações, pela actualidade, correcção e licitude dos dados inseridos. Critério imediato de identificação da propriedade dos dados é também o número que é atribuído a cada indicação, e que se inicia exactamente pela letra correspondente ao país autor ou requerente. Esta particularidade enforma o importante princípio da propriedade dos dados, que tem como corolário que só o Estado proprietário possa proceder a qualquer alteração, correcção ou eliminação dos dados, o que também tecnicamente é garantido.

De igual modo, a nível interno, as indicações são referenciadas à entidade autora da sua criação (inserção). Esta referenciação tem, desde logo, três importantes funções: em primeiro lugar, determinar de imediato a entidade policial que poderá dispor de informação complementar necessária à execução da conduta ou à correcta determinação ou identificação da pessoa indicada (evitando-se assim que as perguntas se dirijam a várias entidades, circulando os dados pessoais por uma infinidade de mãos e durante muito mais tempo); em segundo lugar, assegurar o respeito pelo princípio da propriedade dos dados, o que impedirá, também a nível nacional, que uma entidade diferente da proprietária possa eliminar ou alterar tais dados e, em

terceiro lugar, determinar ou permitir a determinação da entidade responsável por uma eventual inserção incorrecta ou abusiva de dados. E aqui, sublinhe-se não só a consequência positiva da responsabilização interna e para efeitos indemnizatórios, mas também a possibilidade de muito mais rapidamente se poder proceder à correcção de dados viciados por erro de direito ou de facto, que venha a ser exigível.

Permitam-me que aqui faça um pequeno parêntesis para sublinhar como a transparência e o rigor das regras relativas à segurança dos dados e à protecção dos cidadãos face ao tratamento de dados pessoais, perfilhadas por Schengen, poderão ter ainda o mérito de contribuir para uma saudável e querida alteração de mentalidades e de culturas institucionais, que, obviamente, nem sempre ou nunca evoluem com a celeridade que a técnica impõe e o Direito exige. Refiro-me, concretamente, ao princípio da propriedade dos dados, que aqui é motivo de responsabilização e transparência e não, como poderia ser entendido, numa visão de Estado liberal das instituições, como garante de ascendência ou de poder de uma qualquer entidade proprietária.

Uma questão igualmente relevante é a da validade ou manutenção dos dados no SIS. A descoberta de uma indicação e a execução da conduta requerido por parte de um Estado Schengen, determina para o Estado autor da indicação a obrigação de proceder à sua imediata eliminação. O mesmo se diga quando, p estabelecidos pela Convenção para cada tipo de indicação (artºs 112º e 113º). Evita-se assim a poluição do ficheiro, mas este método constitui igualmente, tal como todos os outros acabados de referir, uma forma indirecta de protecção dos cidadãos contra eventuais abusos na manipulação e transmissão de dados pessoais.

Não menos importante nesta matéria é a definição de regras claras quanto à determinação das pessoas que podem aceder aos dados do SIS e que os podem consultar directamente. O art.º 101º da Convenção dispõe que tal acesso é exclusivo das entidades que efectuam controlos fronteiriços, as outras verificações de polícia e aduaneiras no interior do país e respectiva

coordenação. Aos dados relativos a estrangeiros inadmissíveis poderão aceder ainda as entidades competentes para a emissão de vistos, para a análise dos pedidos de visto, para a emissão de títulos de residência e para a administração dos estrangeiros. Contudo, ainda assim, os utilizadores de cada entidade habilitada a consultar o SIS só terão acesso aos dados que sejam necessários para o cumprimento das suas tarefas (acesso condicionado).

Garantia do cumprimento destes critérios é também o facto de cada um dos Estados ser obrigado a comunicar ao Comité Executivo a lista das suas autoridades nacionais competentes para consultar o SIS, bem como o tipo de dados que poderá consultar.

O acesso directo ao SIS faz-se através de uma *password* individual. Qualquer décima transmissão de dados pessoais é registada num ficheiro de auditoria, para efeitos de controlo de admissibilidade das consultas, ficando registado o utilizador que efectuou a consulta, a data e a hora, o local (terminal) e os dados que foram consultados.

Para se ter uma ideia do volume de informações de que falamos quando nos referimos ao SIS, até às zero horas de ontem, esta base de dados continha um total de 7.419.576 indicações, das quais 5.073.136 contêm dados pessoais.

Para que o SIS seja operacional, a troca de informação seja eficaz e a suficiente, haja actualidade e clareza nas condutas a adoptar, se analise e valide as indicações em conformidade com o direito nacional de cada Estado, nos termos precisos da Convenção, se girem os conflitos de interesses entre os Estados sobre indicações a criar sobre a mesma pessoa, ou veículo, se disponibilize de forma eficaz e imediata toda a informação complementar necessária à execução das condutas requeridas pelas indicações, se vele pela licitude, actualidade e correcção dos dados e se garanta aos Estados um ponto de contacto único e permanentemente disponível, foram criados os Gabinete SIRENE (abreviatura de Supplementary Information REquested at

the National Entries), e que, embora não estejam directamente previstos na Convenção de Aplicação, encontram indirectamente a sua base jurídica no art.º 108º da mesma e a sua definição e objectivos no Estudo de Viabilidade Técnica do SIS que foi aprovado pelo Comité Executivo.

Dos actuais dez SIRENE operacionais, só os SIRENE Portugal e França foram criados por lei interna. O SIRENE Portugal foi criado pelo DL nº 292/94, de 16 de Novembro, na dependência do Ministro da Administração Interna.

Os SIRENE funcionam segundo regras e procedimentos comuns, pormenorizadamente descritos em manual adoptado pelo Comité Executivo. São dotados de meios técnicos adequados a uma eficaz, rápida e segura transmissão de informação. Possuem um correio electrónico exclusivo e encriptado. Em poucos segundos, os SIRENE poderão fazer chegar a todos os seus congéneres as informações ou os pedidos de informação de que haja necessidade. Com igual celeridade se pode fazer chegar a todos os Estados Schengen um pedido de detenção provisória para efeitos de extradição através de uma indicação no SIS (cfr. artigos 64º e 95º da CAS) e a todos os SIRENE o correspondente "dossier" com os elementos a que se refere o art.º 16º da Convenção Europeia de Extradicação.

Para evitar erros graves na troca da informação complementar, designadamente pela deturpação dos dados pessoais, bem como para tornar o processo escrito mais célere e mais seguro, os SIRENE, através do seu correio electrónico, utilizam formulários pré-formatados, destinados a diferentes tipos de comunicação (existem neste momento 16 formulários em uso). Tais formulários encontram-se estruturados em rubricas numeradas, cujos títulos são acessíveis na língua de origem de cada SIRENE, seja no momento de elaboração de um formulário, seja na recepção de formulários de outros SIRENE. As rubricas relativas aos dados das indicações são transpostas automaticamente da indicação para o formulário, bastando que o operador digite o nº Schengen da indicação, o que evita erro na transmissão destes dados.

Ao correio electrónico SIRENE e aos arquivos SIRENE, físicos e electrónicos, só os funcionários SIRENE têm acesso e, também aqui, de acordo com as suas funções e competências.

Para além dos meios, regras e procedimentos comuns, os SIRENE estão obrigados a dispor de pessoal com o perfil adequado ao desempenho das tarefas SIRENE, designadamente um serviço de tradução, um serviço jurídico e um corpo de funcionários operativos que falem, para além da sua língua materna, pelo menos uma língua estrangeira, a dispor de equipamento de comunicações rápido e seguro para além, obviamente, do correio electrónico SIRENE e a funcionar 24 horas por dia, todos os dias do ano.

Alguns SIRENE, como o português, dispõem ainda da colaboração de um magistrado do Ministério Público.

Um facto que importa aqui relevar é o da capacidade de todos os SIRENE terem conseguido ultrapassar questões de ordem política, definindo e adoptando um regime linguístico para a comunicação multilateral. Nas comunicações bilaterais, os SIRENE utilizam a língua ou línguas que entre si acordarem, mas nas comunicações multilaterais é utilizada a língua inglesa. Esta medida, se é de primordial importância para a eficácia da cooperação, não será marginal também no que consigna a matéria de protecção de dados pessoais.

Uma de entre muitas tarefas dos SIRENE (não vou aqui descrevê-las todas para não tornar ainda mais longa esta intervenção), consiste na obrigação de se informarem mutuamente e *ex officio*, sempre que detectem que um Estado inseriu uma indicação que se encontra viciada por erro de direito ou de facto e de procederem à correcção de tal erro.

Quanto à estrutura, compete a cada Estado determinar a estrutura do seu SIRENE, devendo respeitar as determinações comuns, podendo embora, se assim o entender, cometer ao seu SIRENE outras competências para além das que lhe são comuns.

Quanto ao Gabinete Nacional SIRENE (ou para usar a expressão mais comum no meio Schengen, ao SIRENE Portugal), constitui-se da seguinte forma:

Depende do Ministro da Administração Interna, que recentemente delegou as suas competências no Ex.mo Senhor Secretário de Estado Adjunto. Dispõe de um coordenador nomeado por despacho conjunto dos ministros da Administração Interna, da Justiça, dos Negócios Estrangeiros e das Finanças, coadjuvado por dois coordenadores adjuntos (ainda não nomeados). Dispõe de pessoal de todas as forças e serviços de segurança (GNR, PSP, PJ e SEF), que se estruturam em grupos operativos e que dependem do coordenador do Gabinete, apenas funcionalmente, mantendo a sua dependência hierárquica das estruturas de origem. O SIRENE Portugal dispõe de um serviço jurídico e de um serviço de tradução. Embora em regime de acumulação, a Procuradoria-Geral da República, nos termos da lei do SIRENE, nomeou para exercer funções junto deste um delegado do MP.

Para além das tarefas que são comuns aos SIRENE, algumas das quais se encontram enunciadas no artigo 3º do DL 292/94, de 16 de Novembro, ao SIRENE Portugal compete ainda *«velar pelo respeito das disposições da Convenção de Aplicação e do direito nacional, designadamente em matéria de protecção da vida privada»*, conforme se dispõe na alínea i) daquele artigo.

Importa assinalar que, neste particular, o SIRENE Portugal, enquanto constituindo a delegação portuguesa no grupo de Trabalho SIRENE na estrutura de concertação permanente de Schengen e em articulação com a Comissão Nacional de Protecção de Dados Pessoais Informatizados, tem defendido posições ou mesmo suscitado questões relativas a procedimentos e práticas de cooperação que, sem descuidar o aspecto operacional e de eficácia, procuram acautelar os direitos dos cidadãos. Algumas o dessas questões originaram mesmo pareceres da Autoridade de Controlo Comum.

O mesmo se diga quanto ao papel impulsionador do SIRENE para o estabelecimento ou regulamentação dos mecanismos internos de cada Estado Parte, tendentes à efectivação de direitos dos cidadãos, designadamente o direito a instaurar acção e de obter indemnização em qualquer Estado Schengen, por prejuízos causados pela exploração do SIS, nos termos do artigo 116º da Convenção.

No que respeita ao exercício do direito de acesso, rectificação e eliminação dos dados por parte dos cidadãos, também aqui importa referir a colaboração que é prestada pelo SIRENE Portugal à Comissão Nacional de Protecção de Dados Pessoais Informatizados.

É ainda aos SIRENE que compete efectuar as consultas aos Estados Parte, sempre que, no âmbito do processo relativo ao exercício daquele direito, a indicação SIS em causa seja da propriedade de um Estado diferente daquele onde tal direito é exercido.

Mas a troca de dados e de informação policial entre os SIRENE nem sempre se reduz a informação complementar relativa a indicações existentes no SIS.

Com efeito, alguns SIRENE dispõem de competências mais alargadas e foram designados como o órgão central competente para a troca de informação no âmbito da cooperação policial prevista nos artigos 39º, 40º, 41º e 46º da Convenção de Aplicação. No que consigna ao SIRENE Portugal, o D.L. 292/94 reconhece-lhe a competência para a troca de informação relativa aos artigos 39º e 46º (troca de informação policial que não caiba às autoridades judiciárias - para efeitos de prevenção e investigação de crimes e de prevenção de ameaças à ordem e segurança públicas). A cooperação relativa à vigilância e perseguição transfronteiriça (artigos 40º e 41º da Convenção), é da competência da Polícia Judiciária, conforme declaração do Estado Português no Acto de Adesão àquele Instrumento.

Muito embora algum trabalho haja ainda a realizar em matéria de articulação das várias entidades neste processo e na clarificação de alguns

procedimentos, parece evidente que todas as razões concorrem para concluir que também aqui, a protecção da vida privada dos cidadãos encontra condições de concretização. Com efeito:

- 1) se é obrigatório que a troca de informação a que respeitam os artigos 39º e 46º seja centralizada numa entidade através da qual são canalizados os pedidos de cooperação, tanto os que são dirigidos a Portugal, como os que as polícias nacionais dirigem aos restantes Estados Schengen;
- 2) se a cooperação policial neste domínio se dirige a todas as polícias nacionais por todas terem competências na matéria;
- 3) se existe uma entidade, o SIRENE, que congrega funcionários de todas as polícias e das quais continuam a depender hierarquicamente;
- 4) se esta entidade mantém uma independência hierárquica relativamente às entidades utilizadoras do SIS;
- 5) se dispõe de meios técnicos rápidos e de contactos privilegiados nos Estados Schengen e funciona 24 horas por dia;
- 6) e se, por fim, está sujeita ao controlo da Comissão Nacional de Protecção de Dados Pessoais, estão, em meu entender, reunidas todas as condições objectivas para evitar ou, pelo menos minimizar, os riscos de uma descoordenação e de uma maior dispersão e contradição na informação circulante, o que, conseqüentemente, não deixará de ter os seus efeitos positivos em matéria de protecção da vida privada.

Importa sublinhar, que a troca de informação no âmbito da cooperação policial a que se referem os artigos 39º e 46º da Convenção de Aplicação de Schengen está igualmente sujeita, *ex vi legis*, a regras precisas relativas a protecção de dados (confronte-se a este propósito o título VI da Convenção, especialmente os artigos 126º, 127º e 129º).

Depois de tudo o que acabo de dizer, parecerá que nenhuma lacuna, nenhum conflito de interesses e/ou de direitos, ensombra este quadro algo idílico.

Na verdade, alguns pontos merecem ainda uma maior atenção. Com efeito, muitas vezes a forma como se estruturam as relações e a troca de

informação internamente, poderá pôr em causa os princípios e regras estabelecidos em matéria de protecção de dados, de forma directa ou indirecta. A prática demonstra que nem sempre existe da parte das instituições a capacidade de reacção e resposta adequada aos desafios de inovação e de adaptação a novas necessidades e a novas regras no domínio funcional e inter-institucional, o que poderá, por vezes, funcionar como bloqueio à efectivação de mecanismos mais protectores e mais garantísticos dos direitos dos cidadãos. Por outro lado, o não respeito pela obrigatoriedade de inserção no SIS das indicações relativas aos motivos e acções taxados na Convenção e que já aqui mencionei, poderá apontar-se como uma forma indirecta de desrespeito pelas regras de protecção de dados pessoais, já que a informação poderá estar a ser tratada por métodos menos eficazes naquela protecção.

Por outro lado, o conflito entre o dever e o ser sempre subsistirá, já que ampla e diariamente a realidade se encarrega de nos mostrar que é bem mais rica na sua complexidade do que os sistemas e os Homens podem prever. E se é certo que regras mais rígidas relativas à protecção de dados pessoais e à defesa do cidadão face à manipulação e tratamento informatizado destes dados, é mais fácil quando se trata de ficheiros como o SIS, que apenas troca dados e informação factual e em que se pode determinar o Estado proprietário dos mesmos, a verdade é que, no que respeita à troca de informação complementar por parte dos SIRENE, se esbarra muitas vezes no conflito entre, por exemplo, transmitir determinado tipo de informação de carácter médico-clínico que poderá salvar uma vida ou cumprir as regras legais quanto à proibição de o fazer.

Outro aspecto reporta-se ao grande volume de dados pessoais acompanhados de fotografias e de impressões digitais que diariamente são trocados por via postal entre os SIRENE, relativas a pessoas cujos dados estão inseridos no SIS. A possibilidade técnica de o fazer através do próprio SIS, como desde sempre tem vindo a ser reclamado pelos SIRENE, deveria constituir uma efectiva preocupação dos Estados e da própria ACC.

Os poucos exemplos que aqui deixo, e que alvitram da possibilidade real de se ir um pouco mais longe em matéria de protecção dos cidadãos no actual Sistema de Informação Schengen, não anulam todos os aspectos positivos e inovadores que nesta matéria a Convenção de Aplicação do Acordo de Schengen e aquele Sistema concretizaram. Afirmar que até agora nenhum outro sistema de informação policial ofereceu aos cidadãos tantas garantias, nem esteve sujeito a tantas e rigorosas regras e entidades fiscalizadoras, não é leviano. Parece-me que Schengen tem sido capaz de provar que é possível cooperar internacionalmente e transmitir grandes volumes de informação e, simultaneamente, criar e manter mecanismos mais eficazes na protecção da vida privada dos cidadãos.

Não se espelhará aqui, com as devidas adaptações, o binómio realismo-idealismo de que falava o Prof. Adriano Moreira, a propósito da complexidade das relações internacionais, e que se traduzia na necessidade de «resolver a hesitação entre perder a República e salvar os princípios ou abandonar os princípios para salvar a República». Preciso é, a meu ver, optar por ambos, pelos princípios e pela República, ou melhor, transformar aqueles em verdadeira *res publica*, relacionando-se os direitos com os cidadãos e não com o Estado enquanto entidade abstracta e distanciada.

O que pretendo significar é que não haverá, de qualquer modo, suficiente protecção dos direitos dos cidadãos sem se investir seriamente na formação e sedimentação de uma consciência de cidadania de todos em geral, consciência esta que, para os agentes de polícia em particular, terá de ser o sustentáculo da sua própria formação profissional.

Temos de habituar-nos à ideia de que a tradição, também aqui, já não é o que era: na troca de informação policial transfronteiriça, no âmbito da UE, a celeridade divorciou-se da informalidade e casou-se com a eficiência. Nesta relação, é a protecção da vida privada dos cidadãos face à informatização dos dados pessoais que tem que ditar as regras de convivência.

Sabemos que a protecção e o respeito pelos direitos, liberdades e garantias dos cidadãos, designadamente o direito à privacidade, é e será sempre, face à evolução das sociedades e da tecnologia, uma tarefa inacabada, mas também por isso, se requer que tal facto constitua um permanente desafio e um estímulo a uma prática institucional cada vez mais conformada à ideia de comunidade, cooperante na construção do «elevado nível de protecção num espaço de liberdade, de segurança e de justiça», que o Tratado de Amsterdão preconiza como meta da União Europeia e para o qual, julgo, a prática e a experiência de Schengen dará também um forte contributo.

Espera-se que a futura integração do acervo de Schengen na União Europeia e o conseqüente alargamento, não só da área geográfica, mas também da intervenção do actual SIS e dos Gabinetes SIRENE, garanta aos Estados, pelo menos, os actuais níveis de cooperação e sem prejuízo dos mecanismos de protecção da vida privada dos cidadãos face à informatização dos dados pessoais.

2ª PARTE

OS SISTEMAS DE INFORMAÇÃO POLICIAL: COMO CONCILIAR SEGURANÇA E LIBERDADE?

A integração dos sistemas de informação policial

Fernando Negrão

Director-Geral da Polícia Judiciária

Falar de informação em Portugal é, ainda hoje, tocar num assunto que, mesmo sem querer, nos faz sentir receios e rodear-nos de algumas cautelas.

Falar hoje de informação em Portugal, para mais de sistemas de informação policial, é afinal falar do quase desconhecido, já que o legítimo desmantelamento de sistemas de informação que serviam de suporte a objectivos políticos definidos por um regime de natureza não democrática, não acarretou a necessária reflexão com vista à premente criação de um sistema de informação criminal integrante de uma sociedade livre, democrática, aberta e moderna.

Tal omissão de muitos anos levou à produção de um efeito perverso e que foi o da recolha e tratamento de informação se fazer de uma forma descoordenada, sem rosto, por vezes com a ausência de efectivo controlo e, pior ainda, levou à criação virtual de meia dúzia de entidades e pessoas, de quem muitos têm medo, por tudo indicar serem os detentores de toda e a mais importante informação.

A ausência de reflexão, a incapacidade para lidar com aqueles a quem deveria competir gerir tais sistemas e o afastamento preconceituoso de assuntos de tanta relevância, levaram à criação de um sistema de segurança acentadamente "coxo", bem como à criação da pior ameaça à liberdade e que é o "bluff" (no caso com a informação).

Posto isto, será interessante ver de forma breve como se passam hoje as coisas.

Do ponto de vista geral temos Lisboa e o resto do país, sendo que apenas na área da droga existe um sistema de informação de apoio à investigação criminal com ramificações a nível nacional. Nas áreas do crime económico e do furto existem dois sistemas que se limitam a Lisboa.

Realce-se que nenhum destes sistemas se entrecruza.

No mais a base é o sistema manual, havendo mesmo algumas descrições que pelo seu colorido merecem referência: " o subinspector peça no telex e manda circular de mão em mão para tomar conhecimento; o Chefe lê, como tem uma excelente memória, lembra-se e vão à pasta e procuram até encontrar.

Obviamente, como metodologia de investigação trata-se de uma solução a banir , já que assenta na memória dos investigadores. Existindo assim a perfeita consciência de que o agente recolhe informação na rua e que, na sua maioria, não é carregada no sistema.

A evolução do panorama criminal a nível nacional e as obrigações crescentes face às organizações internacionais de que Portugal é membro determinaram a Polícia Judiciária a encetar um processo de reorganização interno, actualmente em curso.

Tal necessidade foi ainda sentida dada a constatação de quadros de crime organizado que constituem hoje, por toda a Europa, uma realidade global variada e integrada, que coloca ao sistema policial e judicial a exigência de novas respostas no plano das metodologias da investigação criminal.

E estas, para poderem ser desenvolvidas com solidez e conteúdo, não-de forçosamente assentar em estruturas que lhes forneçam toda a informação criminal disponível, certo como é que a informação tem hoje um papel e uma importância decisiva no desenvolvimento global das sociedades modernas.

O Projecto Sistema Integrado de Informação Criminal (SIIC) é pois considerado como um projecto estruturante da Polícia Judiciária, tendo como objectivos os seguintes:

- 1.Promover a coordenação efectiva da investigação, eliminando a duplicação de investigações;
2. Melhorar a eficiência interna, diminuindo custos e aumentando a produtividade;
- 3.Incentivar o desenvolvimento da circulação de informação;
4. Passar de bolsas dispersas de informação a um sistema integrado contendo toda a informação do conhecimento da Polícia Judiciária e porque não mesmo das Polícias;

e por *fim*

5. Reforçar a qualidade de polícia de investigação aumentando a sua credibilidade. quer interna, quer externamente.

Quanto aos respectivos conceitos básicos, uma primeira classificação da informação baseia-se na sua natureza de investigação.

A informação pode ser confirmada, se é pós-investigatória, ou de elevado grau de confiança dada a sua origem ou processualmente confirmada.

Pode ser especulativa, que é toda a informação pré-investigatória ou pós-investigatória, mas sem confirmação.

E por fim protocolada que é proveniente de fontes externas de conhecida fiabilidade.

Estas definições estão intimamente associadas a conjuntos de informações que valem não só pelos dados individuais, a pessoa, o carro, o crime, mas sobretudo pelas relações entre elas. O carro foi utilizado por certa pessoa para praticar determinado crime.

Para conceber o SIIC, tirando partido das potencialidades dos novos sistemas de gestão de bases de dados foi necessário proceder a uma desagregação desses conceitos, procurando chegar aos elementos atómicos que vão construir o sistema propriamente dito. Temos, assim, a primeira noção fundamental deste projecto que é a distinção entre dados e informação.

Os dados, pela sua natureza, são objectivos e não veiculam nenhuma informação. Gera-se informação ao associar dados entre si, ao relacionar factos com os dados, ou ao processar os dados com vista a determinado fim ou objectivo. O facto de os dados serem objectivos não implica que sejam correctos, sendo, por isso, necessário manter uma classificação de fiabilidade desses dados.

O descer ao nível dos dados, separando-os por completo dos factos, relações e investigações a seu respeito, é o ponto de partida para a definição do SIIC, compatibilizando a partilha de dados entre sectores com a especialização entre sectores, a confidencialidade das investigações com a abertura necessária para potenciar um sistema integrado.

Desta forma, a nível do sistema integrado considera-se:

Dados atómicos são os dados básicos relativos a objectos atómicos sem qualquer relação entre si, de conteúdo objectivo e vazios de qualquer relação. São exemplos: um número de telefone, uma morada, uma chave, uma palavra-chave ou um nome.

Dados de base são dados relativos a objectos elementares, o fundamento de toda a informação gerada pelo sistema. São objectos elementares do sistema integrado, os locais, as viaturas, as embarcações, os telefones e, principalmente, os indivíduos. São estes os dados manipulados pelos utilizadores para construir a sua investigação.

Informação de investigação pode ser especulativa ou confirmada, constando basicamente de factos relativos ou objectos

elementares e relações entre estas.

E por fim,

Informação processual e de coordenação que é a informação confirmada destinada à coordenação interna, definição e gestão de processos, resposta a pedidos de outras entidades, etc.

Questão essencial num sistema desta natureza prende-se com os procedimentos de coordenação e que se iniciam da seguinte forma:

- a abertura da investigação termina com a instrução do documento original, que lhe deu origem, com a informação entretanto encontrada pelo analista, dados sobre os intervenientes, viaturas, telefones, etc. Informações sobre eventuais investigações em curso em que há sobreposição de intervenientes, ou do mesmo tipo de crime ou outros procedimentos. Para ser veiculada ao investigador-coordenador para coordenação, procedimento que pode envolver as seguintes acções:

- Determinação da natureza da abertura da investigação que pode ser: processo, averiguação sumária, carta rogatória ou ofícios precatórios, referência, registo da Europol, etc.
- Verificação da existência da sobreposição com outras investigações em curso para depois poder fazer a devida correcção.
- Decisão sobre a classificação da coordenação;
- Decisão sobre a classificação de segurança;

Terminada a análise, as decisões tomadas voltam a ser registadas no SIIC, sendo dada como assumida a coordenação, ou seja, o registo da coordenação, o tipo de investigação.

Quando se verifica haver duas investigações, incidindo sobre as mesmas pessoas, por exemplo Vulcano Martins, já está a ser investigado, ou analisando o mesmo facto, descarga de heroína, por exemplo ao largo de Leixões, são desencadeados os ditos mecanismos de coordenação de que podem resultar três situações típicas:

1. Investigação conjunta, isto é, existe apenas uma investigação levada a cabo por dois ou mais departamentos da Polícia Judiciária, que assim tem acesso simultâneo à abertura da investigação e a todos os dados a ela associados. Todos os eventos relevantes devem ser comunicados em simultâneo aos dois departamentos envolvidos.
2. Investigação única, quando uma das investigações em que

existe sobreposição é eliminada, ficando apenas um dos serviços com toda a responsabilidade. Todos os dados da abertura da investigação eliminada são passados à outra abertura da investigação, não se perdendo contudo a sua origem.

3. Investigações paralelas coordenadas, isto é, quando avançam as duas investigações em paralelo mantendo-se a troca de informação a nível de investigadores responsáveis.

ESTADO DA INVESTIGAÇÃO

Outra preocupação fundamental do projecto é a coordenação interna na Polícia. Não só com vista à optimização dos recursos, procurando evitar a duplicação de esforços, mas também com vista a uma maior eficiência de investigação, indispensável para fazer face às novas formas de crime organizado.

Para implementar na prática os conceitos de coordenação que propõe o projecto de sistema integrado, é necessário estar-se consciente de que a informação é o ponto de partida, introduzindo assim os conceitos de informação especulativa, seu estado e grande disponibilidade, e dentro destas informação temos:

a activa, que é a informação que está a ser sujeita a trabalho de investigação no âmbito de uma abertura de investigação em curso;

a passiva, que é a informação resultante de uma abertura de investigação, investigada, inconclusiva, estando o processo encerrado ou simplesmente parado, ou de investigação sem actividade de actualização por mais de dois meses, mas com matéria de interesse para futura investigação:

Informação finalizada, que é a informação que resulta de investigação que termina com proposta de acusação ou, se após investigada, foi provado que não houve delito.

Informação finalizada inconclusiva, que é a informação que resulta da investigação terminada sem contudo ter chegado a uma acusação ou condenação.

A estes estados de informação especulativa, junta-se a informação confirmada correspondente à informação especulativa em que houve confirmação dos factos.

À primeira vista pode parecer haver redundância entre a informação confirmada e a finalizada. Note-se que a informação finalizada é ainda

especulativa; no momento em que um processo é dado por terminado, estando a informação pronta a passar a confirmada, nem toda a informação constante da abertura da investigação deve passar a confirmada, mas apenas aquela que pode ser disponibilizada para o exterior como factos confirmados. Dado o restante manancial de informação existente ao abrigo da abertura da investigação deve continuar no foro estritamente especulativo.

Resumindo, o SIIC deve ser centralizado com vista à definição dos modelos, planeamento e definição dos objectivos e estratégias de investigação. Deve ser integrado para aumentar os níveis de disponibilidade, de utilidade e de recuperação de informação. Deve ser potenciador de efectiva coordenação por forma a permitir a consolidação do diálogo e da interactividade interdepartamental, o esforço da intervenção da cadeia hierárquica, e o recurso sistemático ao planeamento operacional ou metodologia de trabalho. Deve ser desconcentrado para possibilitar ao utilizador, no seu posto de trabalho, ter acesso directo a toda a informação relativa à sua investigação, recebendo alertas quando determinados eventos ocorrem. Deve ser, por fim, disponível, ou seja, toda a informação, contida em ambientes amigáveis, deve ser processada com maior rapidez e maior capacidade de recuperação.

CLASSIFICAÇÃO DE DADOS E INFORMAÇÕES

Ao distinguir dados e informação e ao separar os factos dos dados, o SIIC procura sistematizar toda a informação, aumentando o potencial informativo dos dados e contribuindo para um maior rigor em termos de controlo dos acessos no ambiente em que se procura partilhar o máximo de informação.

Ao enveredar por este caminho, começa necessariamente a haver uma maior distância entre o investigador que esteve na origem de determinado dado (por exemplo, uma dada pessoa) ou que investigou esses dados e os potenciais utilizadores da informação. Ou seja, quem trabalha com a informação não deve ser quem investiga os dados dessa informação. Este afastamento leva a que o conhecimento subjectivo que havia sobre os dados contidos numa dada investigação, fundamentais para apreciação dos factos, se tende a perder. Urge, portanto, associar aos dados e informações uma medida objectiva da sua qualidade. De acordo com a experiência anterior da Polícia Judiciária, existem duas formas de avaliar esses dados. Quanto à fonte, que determina de imediato a fiabilidade de determinada informação. E quanto ao dado propriamente dito, a fiabilidade da fonte determina em larga medida a confiança que pode ser depositada na informação. E esta pode ser considerada:

- de alta fiabilidade, normalmente para informações oriundas de organismos policiais, documentos sólidos ou outros;
- de média fiabilidade, quando é veiculada por informadores de confiança, mas requerendo trabalho de comprovação;
- de baixa fiabilidade, quando é oriunda de denúncias anónimas,

por exemplo.

A avaliação directa da informação só pode resultar do trabalho de investigação efectuado, que pode ser dividido em três categorias. A primeira que é a comprovada, se foi alvo de investigação e confirmada, a segunda se é boa, isto é, se ainda não confirmada mas considerada robusta. A terceira, desconhecida se não foi possível confirmá-la.

A classificação de segurança determina o nível de acesso aos dados e informações, tal como se referiu os objectos atómicos não são passíveis de classificação sendo utilizadas basicamente como dicionários internos do sistema. Os objectos elementares são passíveis de classificação para permitirem um controlo de casos de extrema sensibilidade. Contudo, em regra geral, todos os objectos elementares devem ser vistos como informação geral do sistema e assim de livre acesso, obviamente no SIIC.

A classificação segurança, por norma e aplicada às aberturas de investigação, é definida em cinco níveis.

Livre acesso, no âmbito do sistema integrado interdepartamentos, inter-regiões. Reservado, ou seja, acesso condicionado a um único departamento que, por exemplo, pode ser o da droga, mas dentro deste é sempre livre. Pode ser confidencial, ou seja, o acesso é condicionado unicamente ao investigador que abriu a investigação. Pode ser secreto com acesso sujeito a credenciação especial. Pode ser, por fim, muito secreto com acesso sujeito a credenciação especial.

Ao constituir um repositório único de todos os dados, elimina-se por completo a duplicação de dados com as imensas vantagens associadas. Cria-se no entanto uma maior exigência no controlo dos acessos, para garantir que os anteriores níveis de confidencialidade e segurança não sejam alterados. Isto passa pela credenciação funcional dos utilizadores do sistema, procedimento através do qual se determina:

- As áreas a que o utilizador tem acesso;
- O nível de acesso em função da classificação da segurança da informação;
- As tarefas que pode efectuar, ou seja, visualizar, alterar, apagar ou introduzir.

Embora sendo um processo intimamente ligado ao sistema integrado, a credenciação funcional é essencialmente um processo exterior ao sistema que determina qual o perfil de cada funcionário da Polícia Judiciária e inerentes responsabilidades.

CONCEITO DE IDENTIFICAÇÃO

O Sistema de Informação Criminal gira em torno de pessoas que são os criminosos responsáveis pelos crimes, os queixosos e os investigadores. Em última instância, a investigação visa identificar um criminoso e provar a sua culpabilidade. Durante todo o processo de análise subjacente ao presente trabalho tornou-se evidente a centralidade do processo de identificação do interveniente em todo o curso de investigação, sendo por isso fundamental clarificar os conceitos e apresentar definições claras.

No mundo criminal, a identificação assume contornos dificilmente compreensíveis na sociedade “normal” (que é a nossa de todos os dias), quer pela necessidade de identificar arguidos com base em informação incompleta, quer pela proliferação de identidades falsas. Assim, cada sujeito, entendido como uma pessoa em carne e osso pode assumir múltiplos nomes, usar inúmeros documentos falsos, referir vários pais e mães. De exemplos analisados, encontraram-se casos com 28 nomes, todos falsos, 12 documentos de identificação, 5 paternidades, sempre falsos, etc.

Para lidar com estes factos permite-se associar vários nomes, as várias paternidades, as várias nacionalidades a um mesmo indivíduo. E, afinal, permitir-se constituir uma dada identidade, ou seja, saber que paternidade ou documento de identificação foi usado com determinado nome.

Outro conceito fundamental assistente nas aplicações actuais é o da diferença entre os vários tipos de intervenientes, separando claramente os queixosos dos investigadores, dos arguidos, nos respectivos inquéritos. Actualmente, para os primeiros é feito apenas o registo de um nome, enquanto que os segundos são sujeitos a um processo completo de identificação.

No SIIC procura-se consolidar todos estes princípios, introduzindo um novo conceito que é o conceito de identidade. Passa assim a haver três níveis de caracterização dos intervenientes.

Registo de intervenientes, aquele em que apenas se toma nota do nome do interveniente devendo ser usado para caracterizar queixosos, investigadores e outras pessoas envolvidas não arguidos, ou um conjunto de nomes em que Carlos André Rodrigues é um nome distinto de Carlos Rodrigues, Carlos André ou André Rodrigues. Evitar na medida do possível a utilização da abertura da investigação nestas situações.

Outra situação é o registo da identidade, utilizado para caracterização dos arguidos ou suspeitos em processos de investigação, em que se procura caracterizar tão completamente quanto possível o indivíduo na perspectiva de o identificar univocamente, (implica o registo do nome completo, a data de nascimento, sexo, existência de um documento de identificação aceite e a respectiva morada).

Por fim, registo de sujeito, quando se procura o sujeito real por detrás da identidade ou das características dadas procurando os dados biográficos

existentes. Neste contexto, é possível um procedimento de pesquisa de identidade através do qual se procura, com base numa identidade mais ou menos completa, ou em características fisionómicas, identificar o sujeito por detrás da máscara da identidade dada, com vista a associar um dado biográfico, ou mesmo a própria identidade.

A definição destes três níveis de identificação é a base também para a distribuição das tarefas. O registo de intervenientes é uma tarefa corrente podendo ser feito or qualquer funcionário. O registo da identidade envolve um esforço de recolha de elementos com vista a identificar tão completamente quanto possível determinado indivíduo, normalmente suspeito.

O registo do sujeito é em si mesmo um processo de investigação. O processo mais complexo de todos é sem dúvida a pesquisa da identidade, sendo da responsabilidade dos funcionários de investigação. Ao introduzir um nome, o investigador é avisado da ocorrência prévia do nome, ou não. Caso o nome tenha ocorrido anteriormente, inicia-se um processo de pesquisa de identidades que utilizem aquele nome, agrupando-as por indivíduo. Esta pesquisa é feita da identidade como um todo aumentando assim de forma significativa a capacidade da investigação.

O resultado deste processo pode ser encontrar uma "visita" anterior do suspeito ou a conclusão de que se trata de um novo interveniente. Quando de trata de um novo interveniente, há que preencher um novo dado biográfico para o indivíduo e uma nova identidade. Pode ainda tratar-se de um visitante conhecido mas utilizando nova identidade, conclusão a que se chega por análise dos restantes elementos identificadores, devendo neste caso ser introduzida uma nova identificação devidamente associada ao respectivo dado biográfico.

O registo de dados biográficos é feito quando o processo é dado por terminado, regressando à Polícia Judiciária para encerramento, altura em que São registados os dados biográficos dos arguidos confirmados.

Para terminar, só dizer o seguinte:

No dia em que os objectos apreendidos numa busca feita no âmbito de uma investigação por tráfico de droga em Chaves possam ser de imediato identificados na área do furto de Portimão como procurados, é porque a informação, o seu cruzamento e, portanto, a sua integração está efectivamente conseguida.

A protecção de dados e a Europol
Aspectos da protecção de dados no intercâmbio interinstitucional de
informação: o caso da informação criminal e administrativa

Willy Bruggeman

Coordenador Adjunto

Unidade de Estupefacientes da Europol

1. Introdução

A criminalidade grave e organizada faz, actualmente, parte da vida quotidiana. Para combater o crime, a sociedade precisa de uma multiplicidade de informação, nomeadamente, sobre as pessoas. As modernas tecnologias facilitam este trabalho. A recolha, armazenamento e transmissão de dados pode realizar-se de uma forma rápida e eficaz. Ao mesmo tempo aumenta a ameaça à vida privada. O detentor e utilizador de dados pessoais mantém-se, frequentemente, desconhecido e impossível de identificar.

2. Garantias constitucionais

Antes de analisar as abordagens oficiais da protecção de dados, é necessário proceder a uma breve avaliação das disposições constitucionais em matéria de protecção de dados. Um estudo comparativo² sobre a maior parte das constituições europeias leva a concluir que na maioria dos sistemas legais, a privacidade, em termos de informação, é salvaguardada constitucionalmente como um dos direitos humanos básicos. Contudo, a abordagem jurídica nacional, relativa à protecção do cidadão face à recolha, armazenamento e ligação de dados pessoais revela-se heterogénea. Podemos operar a seguinte distinção:

- Constituições em que a protecção de dados é um direito humano expressamente garantido (por exemplo, nas constituições dos Países Baixos, de Portugal e da Áustria);
- Constituições em que a protecção de dados faz parte da vida privada. Não obstante, quase todos estes países (por exemplo, a Grécia e a Irlanda) dispõem de um sistema diferente de protecção da vida privada;
- Constituições em que a protecção de dados é parte de outros direitos humanos (por exemplo, na Dinamarca, na Finlândia e na França).

3. Protecção de dados no âmbito de actividades de aplicação da lei

² Vassilaki, I.E., *Crime investigations versus privacy protection - an analysis of colliding interests*, European Journal of Crime, Criminal Law and Criminal Justice, 1994, 1, 39-49.

3.1. Considerações gerais

No decurso de actividades de aplicação da lei, administrativas, proactivas e criminais, incluindo investigações, as autoridades procuram informação e meios de prova que as ajudem a resolver um crime e a condenar o seu autor. Durante este processo, é preciso ter em conta os problemas específicos que se colocam em termos de recolha, armazenamento e análise de dados pessoais. Quando se trata de criminalidade internacional é preciso ter em conta, não só as disposições nacionais de protecção de dados, mas também as normas internacionais neste domínio.

Assim, é importante analisar, em primeiro lugar, os instrumentos internacionais actualmente existentes, que incidem sobre questões relativas à protecção de dados. Embora a minha comunicação incida, em especial, sobre esses instrumentos internacionais recentes, não se deve tirar a conclusão apressada de que a protecção de dados pessoais nunca fora um foco de preocupação.

3.2. Resenha histórica

a. Desenvolvimentos nacionais

Durante a década de 70, a tecnologia da informação evoluiu a passo de gigante, produzindo uma quantidade de novas ferramentas para processamento automatizado de dados. Esta evolução causou preocupação entre alguns profissionais do direito e nos órgãos governamentais, acerca dos riscos que o processamento electrónico de dados representa para a vida privada do indivíduo.

Durante a mesma década, Hessen foi um dos primeiros Estados a introduzir regulamentação em matéria de protecção de dados pessoais, tendo outros Estados introduzido, em seguida, legislação idêntica: Suécia, Noruega, Dinamarca, Áustria, Alemanha (quer ao nível do Governo central, quer de outros Estados federais), França e Luxemburgo. Ao longo da década de 80 e durante os primeiros anos da década de 90, cada vez mais países introduziram alguma forma de protecção da vida privada no seu direito interno. Tal como já referido, alguns desses países chegaram mesmo a introduzir a protecção da vida privada como um direito constitucional.³

b. Desenvolvimento internacional: Conselho da Europa

Ao introduzirem tais regulamentações, os países em questão estavam a reagir às sucessivas recomendações e resoluções do Conselho da Europa. Na sua qualidade de instituição internacional, o Conselho tem ocupado um

³ Áustria, Bélgica, Espanha, Hungria, Países Baixos, Portugal, Eslovénia e Suécia. Nos termos do artigo 22º, alterado, da Constituição Belga "todo o indivíduo... tem direito ao respeito à sua vida privada e familiar, excepto quando determinado em contrário nos termos e sem prejuízo das condições previstas na lei." Nos termos do n.º 2 do artigo da Constituição, as regiões são obrigadas a salvaguardar esse direito na legislação ou em outras normas legais.

lugar pioneiro, nos esforços em prol da protecção dos direitos humanos. As recomendações e resoluções do Conselho, nesta matéria, baseiam-se no artigo 8º da Convenção Europeia relativa à Protecção dos Direitos Humanos e das Liberdades Fundamentais, que garante o direito ao respeito da vida privada.

Esta evolução foi precedida de um desenvolvimento que se revelou extremamente importante para o futuro desta nova área do direito. Em 1972, os Ministros Europeus da Justiça aprovaram uma resolução, durante a sua sétima Conferência. Essa resolução levou o Conselho da Europa a criar um grupo de peritos, em 1976. Este grupo tinha como missão elaborar o texto de um acordo relativo à protecção da vida privada, em questões que envolvessem o processamento de dados pessoais no estrangeiro e o processamento de dados num contexto transfronteiriço.⁴ O grupo de peritos tinha um mandato importante, que resultou na Convenção de 1981 relativa à protecção do indivíduo face ao processamento automatizado de dados pessoais. Esta Convenção geral foi depois completada por várias recomendações sobre protecção de dados em áreas específicas.

Desde 1981 que a Comissão Europeia tem vindo a apelar aos Estados-membros que ratifiquem a Convenção de 1981 do Conselho da Europa. A ratificação da Convenção só é possível, caso a legislação nacional preveja as medidas necessárias à implementação dos princípios básicos da Convenção.⁵

A existência deste novo instrumento jurídico internacional, juntamente com a crescente preocupação dos governos sobre a protecção de dados pessoais, explica por que é que muitos países têm sido, ao longo dos últimos 14 anos, tão céleres no desenvolvimento de regulamentações sobre esta questão.

c. Desenvolvimentos na União Europeia

Em 1990, a Comissão Europeia apresentou, por seu turno, uma série de propostas ao Conselho Europeu relativas a instrumentos jurídicos comunitários com vista à protecção de dados pessoais.

A mais importante dessas propostas resultou na adopção da Directiva sobre a protecção das pessoas físicas face ao processamento de dados pessoais e sobre a livre circulação da informação.⁶ Esta Directiva deverá garantir um equilíbrio entre: 1) os quatro tipos de livre circulação e as disposições destinadas a combater a concorrência desleal, tal como estabelecido pelo Tratado de Roma, com vista à criação do mercado interno; 2) a protecção de dados pessoais. A versão final desta Directiva, que, segundo o consenso geral, ultrapassa largamente todos os projectos anteriores, foi aprovada pelo Conselho em... de 1995. Não entraremos, contudo, nos pormenores da

⁴ Série de convenções europeias.

⁵ Artigo 4º da Convenção.

⁶ Não se trata do título original, utilizado em 1990. É o título dado pela Comissão à Directiva proposta, quando o texto foi revisto, na sequência da recomendação do Parlamento Europeu. Nós preferimos utilizar o último título, revisto, para evitar possíveis confusões entre os vários instrumentos jurídicos.

Directiva, pois a sua importância para o trabalho policial é limitada pelo facto de que apenas é aplicável ao processamento de dados relacionados com questões do âmbito do primeiro pilar do Tratado de Maastricht.

3.3 Convenção de 1981 relativa à protecção de dados e Recomendação R 87/15

Instrumentos de base

O instrumento internacional mais importante sobre a utilização de dados pessoais pela polícia, ao qual aderiram mais de 20 Estados europeus, é a *Convenção para a Protecção do Indivíduo face ao Tratamento Automático de Dados Pessoais*, de 28 de Janeiro de 1981, do Conselho da Europa ("Convenção de Protecção de Dados"). Os princípios fundamentais da protecção de dados, contidos nesta Convenção, deveriam ser entendidos como uma clarificação da aplicação dos artigos 8º e 10º da *Convenção Europeia de Protecção dos Direitos Humanos e Liberdades Fundamentais* ("Convenção dos Direitos Humanos") e (na ordem jurídica das Comunidades Europeias e, obviamente, da União Europeia como um todo) como "princípios gerais de direito comunitário".

Porém, os princípios básicos da Convenção de Protecção de Dados encontram-se elaborados em termos relativamente amplos e abertos. A Convenção contém, também, uma extensa cláusula derogatória. Tendo em vista clarificar a aplicação mais detalhada da Convenção de Protecção de Dados, o Comité dos Ministros do Conselho da Europa elaborou uma série de recomendações sobre a utilização de dados pessoais em alguns domínios.

Uma dessas recomendações é a *Recomendação n.º R (87) 15, que regula a utilização de dados pessoais no sector policial* ("a Recomendação"). A Recomendação é a declaração mais detalhada e de autoridade, actualmente existente, sobre o que é a prática adequada neste domínio. Embora a Recomendação não tenha a mesma força legal que a Convenção de Protecção de Dados ou a Convenção dos Direitos Humanos, dado que é apenas uma recomendação, trata-se de um instrumento que os Estados não podem ignorar a seu belo prazer, pelas seguintes razões:

Em primeiro lugar, e como já referi, a Recomendação pretende, expressamente, clarificar a aplicação da Convenção de Protecção de Dados, tanto no que respeita aos seus princípios gerais, como à sua cláusula derogatória. Formalmente adoptada (com um reduzido número de reservas) pelo Comité dos Ministros do Conselho da Europa, a Recomendação tem que ser entendida como um "instrumento que foi elaborado por uma ou mais partes [na Convenção de Protecção de Dados] em articulação com as conclusões [da Convenção de Protecção de Dados]" e "aceite pelas outras partes como um instrumento relativo à [Convenção de Protecção de Dados]", na acepção do artigo 31º da Convenção de Viena sobre a Força Legal dos Tratados, da mesma maneira que a própria Convenção de Protecção de Dados tem que ser entendida como um "instrumento elaborado em ligação

com a " Convenção dos Direitos Humanos". A Recomendação, enquanto questão de direito internacional, tem que ser tida em conta para efeitos de interpretação da Convenção de Protecção de Dados.

A Recomendação recebeu também um estatuto alargado na Convenção de Aplicação do Acordo de Schengen e na Convenção Europol, relativamente aos Estados que participam nestas iniciativas. Esses Estados acordaram expressamente em tomar em conta a Recomendação no momento de estabelecerem um nível nacional de protecção, tal como exigido por estas Convenções. A Recomendação ocupa por conseguinte, uma posição de relevo no direito internacional, nomeadamente no que respeita aos Estados que a adoptaram formalmente.

A Recomendação define claramente como e em que medida os princípios gerais da protecção de dados, contidos na Convenção de Protecção de Dados, deverão ser aplicados e até que ponto esses princípios poderão ser alterados ou limitados, à luz da cláusula de excepção contida no n.º 2 do artigo 9º da Convenção de Protecção de Dados. Neste procedimento, o Comité de Peritos, que elaborou a Recomendação, teve também em conta o seguinte:

"A jurisprudência relevante do Tribunal Europeu e da Comissão Europeia dos Direitos do Homem, no contexto do artigo 8º da Convenção Europeia dos Direitos Humanos, que incide sobre a recolha, utilização, armazenamento, etc. de dados pessoais pelas autoridades policiais." (n.º 7 do Memorandum Explicativo).

Dado que a Recomendação é uma clarificação da aplicação, num contexto específico, da cláusula derogatória geral contida na Convenção de Protecção de Dados, não existe qualquer cláusula de excepção na Recomendação propriamente dita. Por outras palavras, a Recomendação deverá ser aplicada integralmente a todas as actividades policiais que envolvam a recolha, armazenamento, divulgação e outra utilização de dados pessoais.

A Recomendação tem ainda um âmbito alargado:

"Os princípios contidos nesta Recomendação aplicam-se à recolha, armazenamento, utilização e comunicação de dados pessoais para fins policiais, que sejam sujeitos ao tratamento automatizado" e:

"A expressão "fins policiais" abrange todas as tarefas que as autoridades policiais desenvolvam para a prevenção e repressão do crime e para a manutenção da ordem pública."

A Recomendação não define "autoridades policiais". Mais uma vez, o termo deveria ser interpretado de forma abrangente:

"...independentemente da nomenclatura, os princípios deveriam aplicar-se a qualquer entidade com funções policiais, envolvido no processo de recolha, armazenamento, utilização e transferência de dados pessoais

para os fins estabelecidos no n.º 3 do [Capítulo "Âmbito e Definições"]."
(n.º 23 do Memorandum Explicativo).

Todas essas entidades deverão desenvolver todas as suas actividades ligadas aos "fins policiais" em conformidade com a Recomendação.

Por outro lado, a Recomendação não se aplica a questões de segurança do Estado. Tal não significa que os serviços que têm a cargo a segurança do Estado não tenham que respeitar a Recomendação: se o trabalho destes serviços envolver "a recolha, o armazenamento, a utilização ou a transferência" de dados pessoais para fins *policiais*, isto é, "para a prevenção e repressão do crime e manutenção da ordem pública" - têm, nessa medida, que ser encaradas como "autoridades *policiais*", submetidas aos princípios contidos na Recomendação. Este aspecto reveste-se de importância fundamental, tendo em conta o envolvimento crescente destes serviços em tais actividades.

Finalmente, é de referir que "os princípios contidos na Recomendação foram considerados pelos seus redactores como *garantias mínimas*" (n.º 30 do Memorandum Explicativo). Isto significa, não só que os "Estados-membros mantêm a liberdade de prever medidas mais fortes de protecção", mas também que a não observância dos níveis mínimos fixados pela Recomendação pode ser considerada como não "necessária numa sociedade democrática" para a protecção dos interesses enunciados no n.º 2 do artigo 9º da Convenção de Protecção de Dados ou no n.º 2 do artigo 8º da Convenção dos Direitos Humanos.

Exigências substantivas da Recomendação

Recolha de dados pessoais para fins policiais.

O princípio 2 define uma série de critérios importantes para a recolha de informação pela polícia. Em primeiro lugar, o princípio 2.1. determina que:

"A recolha de dados pessoais para fins policiais deverá limitar-se ao necessário para a prevenção de um perigo real, ou para repressão de um crime específico. Qualquer excepção a esta disposição deverá ser sujeita a legislação nacional específica."

As autoridades não podem, assim, recolher dados pessoais aleatoriamente; não podem "pescar" esses dados em "expedições de pesca". Tem que haver um perigo *real* e uma suspeita *razoável* do cometimento de um crime *grave*. Além disso, o "perigo" envolvido, além de "real" tem que ser específico.

A admissibilidade da recolha de dados para a "prevenção de um perigo real" não pode ser entendida, nomeadamente, como permitindo, de uma forma geral, a recolha de dados pessoais para a "*prevenção criminal*". Enquanto que a Convenção dos Direitos Humanos concede uma derrogação aos direitos que garante, para efeitos de *prevenção* criminal, a Convenção de Protecção de Dados de 1981 apenas concede tal derrogação para efeitos de *repressão* criminal. Esta diferença não é por acaso. Tem havido graves

problemas relativos à criação de ficheiros de dados para manter sob controlo algumas pessoas em determinados domínios.

Em segundo lugar, a menos que necessário para interesses policiais legítimos, não deveria haver recolha de informação secreta; caso tal segredo fosse necessário, numa determinada fase, o mesmo deveria terminar, logo que possível:

"No caso de terem sido recolhidos e armazenados dados sobre um indivíduo sem o seu conhecimento, e a menos que os dados sejam eliminados, esse indivíduo deverá ser informado, sempre que possível, de que existe informação a seu respeito, *assim que o objecto da actividade policial deixe de ficar comprometido*." (Princípio 2.2.)

Em terceiro lugar, a Recomendação exige que "a recolha de dados por meio de vigilância técnica, ou de outros meios automatizados, deverá ser objecto de disposições específicas".

As autoridades têm que respeitar, também, outros requisitos legais relativos à "detenção para interrogatório, busca e apreensão, métodos de interrogatório, recolha de amostras físicas, impressões digitais, fotografias, etc." - e o direito interno tem que respeitar as exigências da Convenção Europeia dos Direitos Humanos, nesta matéria. É preciso dizer que a recolha de dados em violação do direito interno ou das exigências da Convenção dos Direitos Humanos deverá ser igualmente entendida como tendo sido recolhidos contrariamente à Recomendação e às exigências gerais da Convenção de Protecção de Dados, segundo as quais os dados têm que ser obtidos "legalmente".

Em quarto lugar, a Recomendação contém uma limitação muito estrita relativa à recolha de "dados sensíveis":

"A recolha de dados sobre indivíduos meramente com base na origem étnica, nas convicções religiosas, na conduta sexual, na opinião política ou que pertençam a movimentos ou organizações específicas, não previstos na lei *deverá ser proibida*. A recolha de dados sobre estes aspectos só poderá ser realizada quando *absolutamente necessário* para efeitos de um *inquérito específico*." (Princípio 2.4.)

Por exemplo, pode haver motivos óbvios para o armazenamento de dados sobre a conduta sexual quando tenha sido cometido um crime sexual.

O princípio acabado de referir é de grande interesse, na medida em que revela claramente que as entidades policiais não podem fugir à proibição da recolha de dados sensíveis sobre actividades de grupos de pessoas, em vez de numa base de relacionamento de nomes.

Armazenamento de dados pessoais para fins policiais

O princípio 3.1. determina:

"Sempre que possível, o armazenamento de dados pessoais para fins policiais deverá limitar-se a dados precisos e apenas os que forem necessários para que as entidades policiais possam desempenhar tarefas legítimas, no âmbito do direito nacional e das suas obrigações decorrentes do direito internacional."

Este princípio tem que ser respeitado quando se procede ao intercâmbio ou ao armazenamento de dados com base em acordos de cooperação, como a Convenção de Aplicação do Acordo de Schengen ou a Convenção Europol. Nestes casos, os dados deverão, também, ser "necessários" para as missões em questão e deverão, por conseguinte, ser triados para tal fim, antes de serem armazenados.

A triagem de dados "em bruto", antes de serem registados em ficheiro deverá ser, também, utilizada para a avaliação, qualificação e classificação dos dados, tal como estabelece o princípio 3.2.:

"Sempre que possível, as várias categorias de dados armazenados deverão ser distinguidas de acordo com o grau de exactidão ou de fiabilidade e, nomeadamente os dados baseados em factos deverão ser distinguidos dos dados baseados em opiniões ou em avaliações pessoais".

Este requisito de triagem e classificação é um requisito essencial, num âmbito em que muita da informação é "bruta" ou "leve". Nomeadamente quando armazenada numa base de dados automatizada (com frequência sob a forma de uma síntese), essa informação tem uma enorme tendência a adquirir vida própria e a ser considerada muito mais fiável e "consistente" do que muitas vezes o é, efectivamente. Por exemplo, um carro pode ser descrito como um "carro armadilhado suspeito", por um agente policial, significando tão somente que o carro é "suspeito de conter uma bomba", sem que haja provas reais da existência de uma bomba - mas a frase, se proferida, pode ser entendida muito para além do seu sentido real, significando que existe uma suspeita razoável, ou mesmo provas "consistentes" de que o carro tem, efectivamente, uma bomba. Em alguns casos, estas confusões podem significar a diferença entre a vida e a morte dos responsáveis pelo carro. No que respeita ao trabalho da Europol, é interessante verificar que este princípio tem sido implementado, através de uma obrigação imposta aos Estados-membros, de indicarem a fiabilidade da informação e a fidedignidade da fonte, quando fornecem a informação à Europol para efeitos de análise.

Utilização de dados pessoais para fins policiais

O princípio 4 estabelece o princípio da "finalidade", que é um dos princípios gerais fundamentais da legislação de protecção de dados (*Vide* alínea b) do artigo 5º da Convenção de Protecção de Dados), nos seguintes termos:

"Nos termos do princípio 5, os dados pessoais recolhidos e armazenados pela polícia para fins policiais deverão ser utilizados exclusivamente para esses fins."

Comunicação de dados pessoais para fins policiais

Um dos aspectos mais importantes da utilização de dados pessoais pela polícia diz respeito à comunicação desses dados entre serviços policiais e entre os serviços policiais e outras entidades públicas ou privadas. Neste contexto, existe o perigo de que a utilização excessiva da cláusula de excepção, contida no n.º 2 do artigo 9º da Convenção de Protecção de Dados, conduza ao intercâmbio e à difusão indiscriminados, e sem controlo, de dados (frequentemente dados muito sensíveis e/ou "leves" ou não confirmados) - que tornariam a protecção de dados altamente imaginária, precisamente numa área em que as probabilidades de causar danos são enormes. Devemos, por isso, congratular-nos pelo facto de a Recomendação ser mais pormenorizada e abrangente, neste âmbito.

As questões são tratadas no princípio 5. Os princípios específicos operam uma distinção e estabelecem as condições prévias para a comunicação dentro do sector policial (princípio 5.1.), a comunicação com outras entidades públicas (princípio 5.2.), a comunicação com entidades privadas (princípio 5.3.) e a comunicação internacional (princípio 5.4.).

Estes princípios estabelecem alguns requisitos processuais e administrativos para a comunicação de dados policiais - relativamente aos pedidos de comunicação (princípio 5.5(i), condições para a comunicação (princípio 5.5(ii) e protecção da comunicação (princípio 5.5(iii)). Estes requisitos processuais e administrativos deverão ser aplicados, de uma maneira geral, a todos os tipos de comunicação.

Por fim, a Recomendação estabelece condições importantes relativas à interligação de ficheiros e ao acesso *on-line* aos ficheiros (princípio 5.6.).

Passemos à análise de cada um destes princípios.

Comunicação de dados pessoais dentro do sector da polícia

O princípio 5.1. determina:

"A comunicação de dados entre serviços de polícia, para serem utilizados para fins policiais, só deverá ser possível quando existir um interesse legítimo nessa comunicação, no âmbito das competências legais de tais serviços."

O Memorandum Explicativo refere mais pormenorizadamente que:

"A transferência de dados, dentro do sector da polícia, depende do facto de a autoridade policial receptora possuir um interesse legítimo na obtenção dos dados, por exemplo que o receptor necessite dos dados para a prevenção ou repressão criminal ou para a manutenção da

ordem pública. É legítimo que um serviço de polícia, que pede informação a outro serviço de polícia, possa comunicar determinados dados para que o pedido de informação possa ser satisfeito, desde que as partes envolvidas no processo de comunicação satisfaçam o requisito do interesse legítimo estabelecido no Princípio 5.1." (n.º 57).

De referir, contudo, que embora a condição prévia supra, esteja formulada em termos amplos ("o receptor necessita dos dados para a prevenção ou repressão criminal ou para a manutenção da ordem pública"), para pedidos de dados *ad hoc*, a autoridade autora do pedido tem que fornecer uma "justificação" mais específica para uma determinada comunicação, sob a forma de "motivo do pedido e seus objectivos". Transferências de carácter mais geral, sem esta "justificação" específica, só poderão ser autorizadas por leis ou tratados que abranjam ou regulem essas transferências (Princípio 5.3(ii), Memorandum Explicativo, n.º 71).

Comunicação de dados pessoais da polícia para outras entidades públicas

O Princípio 5.2. incide sobre a comunicação de dados policiais a outras entidades públicas, tais como serviços de segurança social ou autoridades internas de pensões que investiguem fraudes, autoridades de controlo da imigração, autoridades aduaneiras, etc. (os exemplos foram retirados do n.º 59 do Memorandum Explicativo). O Princípio 5.2(i) determina, em primeiro lugar, que:

"A comunicação de dados a outras entidades públicas só deverá ser possível quando, num caso específico, exista uma clara obrigação ou autorização legal, exista autorização da autoridade de controlo, ou quando esses dados sejam imprescindíveis para que o receptor possa desempenhar a sua tarefa legítima e desde que o objectivo da recolha ou tratamento, a ser realizado pelo receptor, não seja incompatível com o tratamento original e as obrigações legais da entidade emissora não se oponham."

Em segundo lugar, o princípio 5.2(ii) determina que:

"Acresce ainda que a comunicação a outras entidades públicas é excepcionalmente permitida quando, num caso específico, a comunicação seja, sem dúvida, do interesse do indivíduo objecto dos dados e, quer os dados tenham sido autorizados por aquele ou as circunstâncias permitam presumir claramente o seu consentimento, ou quando a comunicação seja necessária para prevenir um perigo grave e eminente."

Por outras palavras, todas as transferências de dados policiais para entidades públicas ou privadas, fora da polícia, deverão ser entendidas como excepcionais e sujeitas a uma comprovação rigorosa da necessidade dos mesmos. É preciso distinguir entre transferências gerais de dados, para outras entidades públicas, e transferências *ad hoc*, em casos específicos.

As transferências gerais de dados pela polícia para outras entidades só são possíveis se "existir uma clara obrigação ou autorização legal", ou "com autorização da autoridade de controlo". As "obrigações ou autorizações legais" poderiam constar de estatutos ou de instrumentos oficiais, como decretos ministeriais ou despachos judiciais (cf. n.º 60 do Memorandum Explicativo). Poderão ainda ter a forma de acordos internacionais entre Estados.

É preciso, contudo, referir que estas "obrigações" e "autorizações" (por lei ou nos termos de uma lei, de um acordo ou concedidas por um tribunal ou por uma autoridade de controlo) correspondem a derrogações "previstas na lei" na acepção do n.º 2 do artigo 9º da Convenção de Protecção de Dados. O termo "na lei", contido nessa disposição é, por sua vez, retirado do segundo parágrafo das disposições substantivas da Convenção dos Direitos Humanos, que prevê excepções e restrições (*Vide* relatório explicativo da Convenção de Protecção de Dados, n.º 55). Tal significa que as "obrigações" e "autorizações" em questão têm que ser conformes aos requisitos em termos de excepções e restrições "previstas na lei", na Convenção dos Direitos Humanos, ou seja, têm que ser convenientemente acessíveis (publicitadas) e suficientemente precisas. As disposições indevidamente abrangentes e vagas, mesmo que previstas por leis ou acordos formais, que permitam a difusão excessivamente alargada de dados policiais para outras entidades públicas, violaria o princípio 5.2 da Recomendação, da mesma maneira que as instruções ou ordens administrativas não publicadas (mesmo que claras e precisas, na substância).

Finalmente, do princípio 5.2 (i) resulta claramente que, mesmo que exista uma "obrigação" ou "autorização", que permita, de uma maneira geral, a divulgação de (determinado tipos de) dados policiais a outra entidade pública específica, é sempre necessário avaliar, em cada "caso específico", se o assunto em questão é efectivamente abrangido pela regra geral.

As transferências *ad hoc* de dados policiais para outras entidades públicas têm também que ser sempre entendidas como excepcionais, embora umas sejam mais excepcionais do que outras. Em primeiro lugar, tal como sublinhado pelo Memorandum Explicativo, há alguns tipos de entidades públicas (tais como serviços de segurança social, de impostos, de imigração ou serviços aduaneiros) que "participam em actividades que, de alguma maneira, são idênticas às actividades policiais", tais como investigações no âmbito da segurança social, impostos, fraude no IVA ou imigração ilegal (cf. n.º 61). Os fins destas actividades "não são incompatíveis" com os fins do trabalho policial, em sentido restrito, e a comunicação de dados policiais a esses serviços, no âmbito de tais investigações, não constitui, por conseguinte, uma violação do "princípio da especificação do fim (ou finalidade)" (alínea b) do artigo 5º da Convenção de Protecção de Dados, já referida). Mesmo assim, a Recomendação exige que, mesmo nestes casos, os dados pessoais só podem ser fornecidos, desde que sejam indispensáveis para uma tarefa legal a desenvolver pela entidade não policial e desde que não haja nenhuma obrigação legal que impeça a polícia de proceder à divulgação dos dados (disposições do Código Penal ou do Código de

Processo Penal que restrinjam a divulgação da informação ou disposições relativas a condenações "passadas").

Mais excepcional ainda é a comunicação de dados no âmbito do princípio 5.2(ii). Em primeiro lugar, esta disposição prevê, na alínea a), a divulgação de dados policiais a outras entidades públicas em casos excepcionais, quando tal seja inegavelmente do interesse do indivíduo objecto dos dados e desde que este tenha consentido na divulgação ou (mais excepcional ainda) as "circunstâncias sejam de modo a permitir a presunção clara desse consentimento". Esse consentimento pode não ser facilmente presumido, nem ser suficiente como tal: mesmo que uma entidade pública que solicita a informação produza um formulário no qual conste o consentimento do indivíduo objecto dos dados, a polícia tem a obrigação de se certificar de que a comunicação dos dados é efectivamente, e sem margem para quaisquer dúvidas, do interesse do indivíduo objecto dos dados. O termo "consentimento" pressupõe, para além disso, que o indivíduo objecto dos dados foi devidamente informado e que foi livre de exercer a sua vontade. As entidades públicas devem, por conseguinte, ser honestas e abertas quando pedem tal consentimento e, nomeadamente, não devem omitir a verdade aos indivíduos objecto dos dados, quanto ao carácter voluntário do pedido de consentimento. O "consentimento" dado na ignorância ou obtido com recurso a falsidades não é um "consentimento" e os dados assim obtidos são considerados como obtidos de forma "desonesta", em violação de um dos princípios fundamentais da protecção de dados.

Finalmente, o princípio 5.2(ii), alínea b) da Recomendação prevê um caso extremamente excepcional de comunicação de dados policiais a outras entidades públicas, quando forem necessários para prevenir um perigo grave e eminente. As comprovações deverão ser, sem dúvida, muito rigorosas. O Memorandum Explicativo acrescenta que, quando existe um perigo grave, mas não eminente, a "comunicação pode processar-se em conformidade com as disposições do princípio 5.2(ii), alínea a)", ou seja, é necessário, em primeiro lugar, a obtenção da autorização da autoridade de controlo (n.º 62).

O que acabo de referir constitui uma limitação clara e estrita da comunicação de dados policiais a outras entidades públicas. Em especial, na ausência de uma obrigação ou autorização legal, clara, precisa e publicamente anunciada, tais comunicações serão permitidas apenas num caso específico e, nesse preciso caso, terá que haver uma verificação específica sobre a justificação do pedido, à luz do Princípio 5.2(i). Quaisquer dados transferidos limitar-se-ão ao estritamente necessário para os fins a que os mesmos se destinam.

Comunicação de dados pessoais da polícia para entidades privadas

Tal como a comunicação de dados para entidades não policiais no sector público, a comunicação de dados pessoais para entidades privadas deverá ser também encarada, em todos os casos, como excepcional (cf. n.º 58 atrás citado e n.º 63 do Memorandum Explicativo). O Princípio 5.3, que regula tais comunicações de dados, é muito idêntico ao Princípio 5.2, acima discutido, em (b).

Assim, o Princípio 5.3(i) prevê tais comunicações de dados na mesma base que as comunicações às entidades públicas ao abrigo do Princípio 5.2(i), alínea a), ou seja, quando haja uma "clara obrigação ou autorização legal" para esse efeito, numa lei, decreto-lei, despacho judicial ou com base numa decisão da autoridade de controlo. Mais uma vez, as regras que determinam essas "obrigações" ou que concedem a competência para emitir tais "autorizações" terão que ser tornadas públicas e serem suficientemente claras e precisas.

O Princípio 5.3(ii), alínea a) prevê ainda tais comunicações, com carácter ainda mais excepcional, sob a mesma base da comunicação ao sector público, caso tal seja do "interesse inegável do indivíduo objecto dos dados" e com o seu consentimento (expresso ou, em determinados casos, presumido). O Princípio 5.3(ii), alínea b), permite tais comunicações em casos extremamente excepcionais, quando seja necessário prevenir um perigo grave e eminente. Aplicam-se, também aqui, as observações a estes requisitos, apresentadas acima, em b).

De referir que a Recomendação não prevê as comunicações de dados a entidades privadas numa base idêntica à definida como legítima no Princípio 5.2(i), alínea b), relativamente às entidades públicas, ou seja, quando seja "indispensável" para uma missão legal do receptor e "não incompatível" com o objectivo original do trabalho policial. Tal significa que, a menos que haja um perigo "grave e eminente", qualquer divulgação de dados pessoais que não seja manifestamente "do interesse do indivíduo objecto dos dados" como, por exemplo, a divulgação de dados sobre conhecidos (ou suspeitos) autores de fraudes em bancos, companhias de seguros ou lojas (cf. n.º 63 do Memorandum Explicativo), só poderá processar-se com base numa "obrigação" ou "autorização" legal.

Comunicação internacional de dados policiais

As disposições da Recomendação, relativas à comunicação internacional de dados policiais é, obviamente, de especial interesse para este estudo e, nessa medida, citaremos na íntegra a relevante disposição contida no Princípio 5.4 e os números relevantes do Memorandum Explicativo.

O Memorandum Explicativo refere várias vezes o intercâmbio de dados através dos canais da Interpol como se esse intercâmbio ocorresse nos termos ("de uma disposição legal clara") do direito internacional. De referir, contudo, que, surpreendentemente, a Interpol não assenta em nenhum tratado internacional, mas naquilo a que se chama tecnicamente um acordo "privado" entre forças policiais nacionais. De referir, também, que nessa altura a Europol ainda não "existia".

À parte este aspecto, as observações relevantes, contidas no Memorandum Explicativo, podem, por vezes, aplicar-se igualmente aos sistemas de cooperação policial devidamente assentes em tratados, tais como o Acordo

de Schengen, a Convenção de Aplicação do Acordo de Schengen e a Convenção Europol.

O Princípio 5.4 determina o seguinte:

"5.4 Comunicação internacional

A comunicação de dados a entidades estrangeiras deve limitar-se aos órgãos de polícia e só deverá ser permitida:

- a) quando exista uma disposição legal clara no direito nacional ou internacional;
- b) na ausência de tal disposição, quando a comunicação seja necessária para evitar um perigo grave e eminente ou seja necessária para a repressão de um crime grave, nos termos da lei geral, e desde que as disposições internas aplicáveis à protecção do cidadão não sejam afectadas."

O Memorandum Explicativo apresenta o seguinte comentário: "O Princípio 5.4 refere-se à transferência internacional de dados policiais, em sentido restrito, entre órgãos de polícia". A referência ao direito internacional refere-se, não só aos acordos internacionais relativos à assistência mútua em matéria penal, mas também, actualmente, à cooperação no âmbito da Interpol, da Convenção de Aplicação do Acordo de Schengen ou da Convenção Europol. Este Princípio tem também em conta a existência, ou a conclusão, de acordos entre Estados vizinhos, com vista a melhorar a comunicação transfronteiriça de dados entre serviços de polícia.

"Relativamente ao termo "serviços de polícia", é reconhecido que em alguns Estados-membros, determinados tipos de trabalho policial podem ser realizados por autoridades que não são "serviços de polícia" em sentido restrito. Por outro lado, pode acontecer que determinadas funções, supostamente da competência das autoridades policiais, em alguns Estados-membros, possam ser delegadas por serviços não policiais em outros Estados-membros.

"Para efeitos do Princípio 5.4, o termo "serviços de polícia" deverá ser entendido em sentido lato". A questão que se coloca é a de saber se o serviço desenvolve uma função relacionada com a prevenção ou repressão criminal ou com a manutenção da ordem pública. Finalmente, o Princípio 5.4 não deverá ser interpretado como excluindo a possibilidade de os dados serem transferidos para autoridades judiciais estrangeiras quando essas autoridades exerçam funções relacionadas com a prevenção e repressão criminal. Convém que se diga que os requisitos contidos no Princípio 5.4 são para respeitar.

"A comunicação internacional de dados pessoais entre serviços policiais só poderá processar-se de acordo com as condições estabelecidas nas alíneas a) e b)". O Princípio 5.4, alínea b) aplicar-se-á quando o Estado receptor não for membro da Europol, parte na Convenção de Aplicação do Acordo de Schengen ou quando não exista qualquer convénio (por

exemplo, a Convenção EUROPOL) que autorize a comunicação de dados ao Estado receptor.

"O texto do Princípio 5.4 reflecte, de alguma maneira, as disposições do artigo 12º da Convenção de Protecção de Dados, que define a questão da circulação transfronteiriça de dados. De referir que a cláusula "e desde que o direito interno de protecção do cidadão não seja afectado" corresponde ao conceito de "protecção equivalente" no Estado receptor, contido na alínea a) do n.º 3 do artigo 12º da Convenção de Protecção de Dados. Da mesma maneira, a autoridade emissora dos dados deverá observar o nível de protecção de dados policiais do Estado receptor. Caso a autoridade emissora imponha condições para a utilização dos dados no Estado receptor (por exemplo, no que respeita ao período de conservação dos mesmos), é preciso interiorizar que essas condições são para respeitar. As alíneas a) e b) do Princípio 5.4 são reguladas por esta disposição."

(n.ºs 65 a 69 do Memorandum Explicativo)

A clarificação do termo "serviços de polícia" no contexto acabado de referir, não se afasta, efectivamente, da clarificação do termo "autoridades policiais", como atrás referido; apenas se esclarece que, por vezes, determinados serviços deverão ser entendidos como "serviços de polícia" relativamente a algumas actividades, mas não relativamente a outras. Este aspecto poderia aplicar-se, por exemplo, aos serviços aduaneiros e de impostos indirectos ou aos serviços de informação. Tal parece implicar que os dados recolhidos, armazenados e utilizados por tais serviços, para "fins policiais", deverão ser mantidos em separado dos ficheiros utilizados pelos mesmos serviços, para outros fins.

A autorização do intercâmbio de dados, com base em "disposições legais claras" (Princípio 5.4, alínea a)), deverá, mais uma vez, ser entendida como exigindo que tais disposições sejam tornadas *públicas*, sejam *claras* e *precisas* (*Vide supra*, alínea b)). Tais requisitos aplicam-se, igualmente, à legislação nacional, que autoriza a transferência internacional de dados, e aos acordos internacionais pertinentes. Obviamente que a Convenção Europol satisfaz estes requisitos.

De referir que o Princípio 5.4 não contém qualquer disposição (ao contrário dos Princípios 5.2 e 5.3) que autorize a transferência internacional de dados apenas mediante "autorização da autoridade de controlo", embora tal não exclua, presumivelmente, a possibilidade de a autoridade de controlo ser autorizada a autorizar essas transferências, através de uma "disposição legal clara". Contudo, neste último caso, resultaria que a "disposição legal" de decisão de conceder ou não essa autorização, bem como a própria autorização deveriam, em princípio, ser igualmente tornadas públicas.

Fora dos referidos acordos (tratados) formais, os dados policiais só podem ser transferidos além fronteiras, com base no Princípio 5.4, alínea b), ou seja, quando a transferência for *necessária* para a prevenção de um perigo *grave* e *eminente*, ou quando for *necessária* para a repressão de um crime *grave* nos

termos da lei geral. A primeira possibilidade é a mesma que a possibilidade excepcional de comunicação de dados policiais a entidades não policiais, entidades públicas e privadas, nos termos, respectivamente, dos Princípios 5.2(i), alínea b) e 5.3(ii), alínea b) (*Vide supra* em b) e c)): mais uma vez é preciso entender que tais transferências só são admissíveis em casos extremamente excepcionais.

A possibilidade de transferência de dados, quando *necessária* para repressão de um "*crime grave nos termos da lei geral*" é interessante, mas infelizmente nem o termo "crime grave", nem o termo "lei geral" são expressamente definidos na Recomendação ou no Memorandum Explicativo. Contudo, a maior parte dos códigos penais nacionais estabelecem uma distinção entre os vários tipos de crime, desde os "pequenos delitos" até aos "crimes". Existe um amplo consenso entre os Estados-membros relativamente a esta distinção, mas não há nada como a uniformidade das categorias em que deverão ser integradas as várias infracções. Os acordos internacionais relativos aos intercâmbios de dados policiais, como a Convenção Europol, têm definido claramente em que "crimes graves" poderá haver transmissão de dados.

A expressão "(crime nos termos) da lei geral" deverá ser entendida como excluindo crimes previstos em legislação especial, de emergência ou anti-terrorista. Os acordos internacionais que autorizam o intercâmbio regular de dados sobre terrorismo (como a Europol, no Tratado da União, n.º 9 do artigo K.1) tiveram que fornecer uma base legal clara, sob a forma de texto, que definisse os crimes, sobre os quais poderá haver intercâmbio de dados, e definir linhas directrizes específicas e pormenorizadas sobre protecção de dados, a par da Recomendação. Desta forma, os intercâmbios de dados, em questão, são autorizados nos termos do Princípio 5.4, alínea a), ou aplica-se o Princípio 5.4, alínea b).

Finalmente, é preciso que a transferência internacional de dados, para fins policiais, não afecte as "disposições internas de protecção do cidadão". Tal como esclarece o Memorandum Explicativo. Isto significa, em primeiro lugar, que não poderão ser enviados dados policiais de um país com determinado nível de protecção de dados (no domínio dos dados policiais), para outro país que não tenha um nível "equivalente de protecção" (naquele domínio), a menos que se encontrem estabelecidas determinadas garantias sobre a forma de "condições de utilização dos dados no Estado receptor". Tais condições terão que ser respeitadas pelo Estado receptor. Porém, os termos "disposições internas de protecção do cidadão" não se limitam necessariamente, como tal, à protecção de dados. Não seria desadequado interpretar esta frase como estendendo-se a outras garantias legais, em especial, no domínio da legislação penal como, por exemplo, regras para obtenção de provas pela polícia ou a admissibilidade dessas provas em processo penal.

Todos os requisitos acabados de referir, relativos à comunicação internacional de dados policiais, tiveram e continuam a ter, implicações claras

sobre os acordos internacionais em matéria de intercâmbio de dados policiais e criação de redes informáticas internacionais, nomeadamente a Europol.

Pedidos de comunicação de dados policiais

Tal como referido na alínea a), o Princípio 5.1 autoriza, em termos gerais, a comunicação de dados dentro do sector da polícia "para fins policiais", ou seja, quando o receptor necessitar dos dados em questão para a prevenção ou repressão de crimes ou para a manutenção da ordem pública. O Princípio 5.5(i) estabelece mais algumas *condições* importantes a este respeito:

"Sujeitos às disposições específicas contidas na legislação nacional ou em acordos internacionais, os pedidos de comunicação de dados deverão fornecer *indicações* relativas à *entidade ou à pessoa que os solicita*, bem como aos motivos do pedido e *objectivos*."

Relativamente aos pedidos *ad hoc* de dados, apresentados na ausência de tais providências nacionais ou internacionais, a autoridade requerente tem, por conseguinte, que apresentar uma "*justificação*" específica para uma determinada comunicação, sob a forma de "motivo do pedido e seus objectivos". Estes motivos e objectivos têm, ainda, que ser *registados* juntamente com os pormenores da autoridade requerente.

Acresce, ainda, que, quando as leis ou tratados internacionais autorizam as transferências gerais de dados sem "justificação" específica, como disposições ou providências legais, constitui uma derrogação "por lei" aos requisitos gerais contidos na Recomendação e na Convenção de Protecção de Dados. Estas transferências têm a sua base legal no n.º 2 do artigo 9º da Convenção de Protecção de Dados e no n.º 2 do artigo 8º da Convenção dos Direitos Humanos e têm, por conseguinte, que satisfazer as exigências destas cláusulas de excepção. Isto significa, mais uma vez, que as transferências em questão deverão ser circunscritas e reguladas pelas disposições legais pertinentes, que deverão ser *claras, detalhadas, específicas e tornadas públicas*.

Estas transferências com carácter excepcional têm que ser claramente necessárias para as tarefas envolvidas; têm que "corresponder a uma necessidade social premente" e têm que ser "proporcionais" a essas necessidades. Mais adiante argumentaremos que, mesmo que autorizada "por lei" sem mais "justificação", todas as transferências terão que ser *registadas* no ficheiro ou base de dados pertinentes.

Requisitos da comunicação de dados pessoais

O Princípio 5.5(ii) da Recomendação determina:

"Sempre que possível, a qualidade dos dados deverá ser verificada no momento da sua comunicação. Sempre que possível, em todas as comunicações de dados deverão ser indicadas as decisões judiciais, bem como as decisões de arquivamento e os dados baseados em

opiniões ou considerações pessoais deverão ser verificados na fonte antes de serem transmitidos, indicando também o respectivo grau de exactidão ou de fiabilidade.

Caso se constate que os dados deixaram de ser exactos, ou não estão actualizados, não deverão os mesmos ser comunicados. Caso os dados, que deixaram de ser exactos ou que não estão actualizados, tiverem sido comunicados, a entidade que os comunicou deverá informar, tanto quanto possível, todos os receptores dos mesmos, da sua não conformidade".

O Memorandum Explicativo acrescenta:

Tal como referido anteriormente, é do interesse, quer da polícia, quer do próprio indivíduo, que os dados sejam exactos. O Princípio 5.5(ii) é flexível, na medida em que prevê a existência de diferentes períodos de controlo nos vários países. É por esta razão que a verificação da qualidade dos dados é possível até ao momento da sua comunicação.

O Princípio em questão é de grande importância. Este confirma, em primeiro lugar, que, pelo menos em princípio, os dados têm que ser (novamente) triados, avaliados e classificados, *até ao momento da sua transmissão*. No que respeita aos sistemas recém-criados (como a Europol) não há qualquer desculpa para a não inclusão das características e verificações necessárias.

É também interessante referir que, caso os dados que deixaram de ser exactos e não estão actualizados, tenham sido comunicados, todos os receptores deverão ser informados. Este aspecto sublinha que um serviço policial que comunique dados a outro serviço (policial ou não) tem alguma responsabilidade quanto aos dados. Caso o serviço emissor saiba, ou presuma, que o serviço receptor guardou os dados, deverá informá-lo de desenvolvimentos subsequentes (como decisões de arquivamento, de absolvição ou de condenação) relativos aos dados. Tal como já referido, é também uma consequência natural dos requisitos previstos neste Princípio, que os serviços policiais que comuniquem dados a terceiros guardem um registo dessas transferências.

Garantias quanto à comunicação de dados policiais

O Princípio 5.5(ii) determina:

"Os dados comunicados a outras entidades públicas ou privadas, bem como a autoridades estrangeiras, não deverão ser utilizados para outros fins que não os especificados no pedido de comunicação de dados.

A utilização dos dados para outros fins deverá, sem prejuízo dos números 5.2 a 5.4 deste Princípio, ser submetida à concordância da entidade autora da comunicação.

Concluiu-se já, concretamente no que respeita à comunicação internacional de dados policiais, que o "princípio da limitação dos fins" deverá ser rigorosamente aplicado nesse contexto.

Interligação de ficheiros e acesso *on-line* a ficheiros

O Princípio 5.6 incide sobre a "interligação de ficheiros e acesso *on-line* a ficheiros". O primeiro ponto deste Princípio permite, em primeiro lugar, "a interligação de ficheiros com ficheiros guardados para outros fins", quer com base numa autorização para este efeito, concedida pela autoridade de controlo, "*para efeitos de um inquérito específico*", quer "em conformidade com uma disposição legal clara". Este ponto incide sobre:

"A situação particular em que a polícia pode procurar *recolher* dados [junto de outros serviços *não policiais*], ligando os seus ficheiros a ficheiros [desses outros serviços] para fins diferentes, como por exemplo, os ficheiros dos serviços de segurança social, as listas de passageiros das companhias aéreas, os ficheiros das companhias de seguros, os ficheiros de sócios de sindicatos, etc."

Poderia parecer, por conseguinte, que este primeiro ponto não se aplica à interligação de ficheiros policiais, desde que todos os ficheiros envolvidos sejam utilizados para "fins policiais": tais interligações intra-polícia estão abrangidas apenas pela regras gerais da comunicação de dados pessoais dentro do sector da polícia e pelas regras mais específicas sobre a comunicação internacional de dados policiais, atrás desenvolvida.

O segundo ponto incide sobre o acesso (*on-line*) directo e informatizado a ficheiros. Este parágrafo abrange o acesso *on-line* a bases de dados dentro do sector policial, bem como o acesso *on-line* da polícia a bases de dados não policiais. O Princípio em apreço exige que tal acesso seja *apenas* autorizado no seguinte caso:

"Nos termos do direito interno, que deverá ter conta os Princípios 3 a 6 da referida Recomendação".

Período de armazenamento de dados pessoais e actualização de dados

Tal como o Memorandum Explicativo sublinha, "é fundamental realizar um controlo periódico dos ficheiros policiais, a fim de garantir o expurgo de dados supérfluos e incorrectos e a actualização dos mesmos" (n.º 96). O Princípio 7 estabelece alguns requisitos importantes para esse fim. O Princípio 7.1 exige, em primeiro lugar, que:

"Sejam tomadas medidas para que os dados pessoais guardados para fins policiais sejam eliminados quando deixarem de ser necessários para os fins para os quais foram armazenados.

"Para este efeito, é preciso ter especial atenção aos seguintes critérios: necessidade de manter dados, tendo em conta a conclusão de um

inquérito específico, decisões judiciais finais, em especial, de absolvição, de reinserção, tendo em conta condenações anteriores, amnistias, a idade do indivíduo objecto dos dados, bem como as categorias específicas de dados."

É preciso não esquecer estas considerações, no momento de determinar se os dados continuam ou não a ser necessários para a prevenção e repressão criminal ou para a manutenção da ordem pública (n.º 96 do Memorandum Explicativo).

Em segundo lugar, o Princípio 7.2 estabelece:

"As regras destinadas a estabelecer o período de armazenamento das várias categorias de dados pessoais, bem como as verificações regulares da sua qualidade, deverão ser fixadas por acordo com a autoridade de controlo ou nos termos do direito interno."

Manutenção de registos

Tal como já referido, a Recomendação estabelece, em vários pontos, requisitos substantivos e processuais destinados a garantir que no tratamento de dados pessoais pela polícia haja um equilíbrio entre as necessidades da sociedade e os direitos individuais e que não haja abuso no referido tratamento. Mesmo que nem sempre conste expressamente nos Princípios pertinentes é, em nosso entender, óbvio que, para que estes requisitos sejam efectivamente *implementados*, será necessário manter um *registo* detalhado das operações relevantes.

Segurança dos dados

O Princípio 8, que reflecte o artigo 7º da Convenção de Protecção de Dados, exige a adopção das medidas de segurança adequadas:

"A entidade responsável deverá adoptar todas as medidas necessárias para garantir a segurança física e lógica adequada dos dados e evitar o acesso, comunicação ou alteração não autorizados.

Neste sentido, é necessário ter em conta as diferentes características e conteúdo dos ficheiros."

Controlo e notificação

Para além das medidas internas da polícia, a Recomendação exige, também, o *controlo externo* e a *supervisão* rigorosos da utilização dos dados policiais. Efectivamente, a Recomendação refere estas importantes garantias no primeiro Princípio:

"Princípio 1 - Controlo e notificação

- 1.1 Cada Estado-membro deverá ter uma autoridade de controlo externa ao sector policial, responsável por garantir o respeito dos princípios contidos nesta Recomendação.
- 1.2 As novas tecnologias de tratamento de dados só poderão ser introduzidas se tiverem sido tomadas todas as medidas razoáveis, com vista a garantir que o uso dessas tecnologias é conforme ao espírito da legislação existente sobre protecção de dados.
- 1.3 A Entidade responsável deverá consultar previamente a autoridade de controlo, sempre que a introdução de técnicas de tratamento automático suscite questões acerca da aplicação desta Recomendação.
- 1.4 Os ficheiros automatizados permanentes deverão ser notificados à autoridade de controlo. A notificação deverá especificar a natureza de cada ficheiro declarado, a entidade responsável pelo seu tratamento, os fins a que se destina, o tipo de dados contidos no ficheiro e as pessoas a quem os dados são comunicados.

Os ficheiros *ad hoc*, criados no âmbito de inquéritos específicos, deverão ser igualmente notificados à autoridade de controlo, quer nos termos das disposições acabadas de referir, tendo em conta a natureza específica desses ficheiros, quer em conformidade com a legislação nacional."

Tendo em vista a elaboração de regras internas para implementação da Recomendação, a autoridade de controlo deverá ter o máximo de informação sobre actividades policiais específicas, aquando da criação e configuração de novas bases de dados (incluindo *logs*, etc.) e aquando da inspecção das forças policiais, relativamente ao manuseamento e segurança de dados (pessoais).

Além disso, tal como já referido nos pontos anteriores, a autoridade pode dispor de competências alargadas para autorizar transferências de dados para serviços não policiais, no sector público ou privado. Tal como refere o Memorandum Explicativo:

"Foi com este papel em mente que no Princípio 1 se deu ênfase à necessidade de a autoridade de controlo ser independente do sector policial." (n.º 60)

Finalmente, tal como veremos mais adiante, no ponto final deste capítulo, a autoridade de controlo tem um papel fundamental a desempenhar, em matéria de salvaguarda dos direitos do cidadão face aos ficheiros policiais.

Publicidade, direito de acesso aos ficheiros policiais, direito de rectificação e direito de recurso

Os direitos do cidadão formam a pedra angular do edifício da protecção de dados. Assentam na noção de que o indivíduo tem o direito à "autodeterminação em matéria de informação", que ninguém tem o direito de "possuir" dados pessoais de outra pessoa. Estas noções são talvez um pouco exageradas e ideais: na prática, a "soberania" do indivíduo, em qualquer ordem jurídica, é rigorosamente circunscrita e o "direito à autodeterminação", em matéria de protecção de dados, não é excepção. No direito internacional, trata-se de mais um passo no sentido do reforço do estatuto do indivíduo como sujeito do direito internacional.

É, por conseguinte, de grande importância esclarecer até que ponto a cláusula derogatória, contida na Convenção de Protecção de Dados, permite restrições ou derrogações a estes direitos, no que se refere aos ficheiros policiais. Eliminar a derrogação nesta área, tornaria a protecção do indivíduo ineficaz, precisamente na área em que o mesmo tem mais a perder em termos de liberdade individual. Assim, devemos congratular-nos pelo facto de a Recomendação ser, a este respeito, detalhada e estrita.

Os direitos do indivíduo objecto dos dados são definidos pelo Princípio 6, nos seguintes termos:

"Princípio 6 - Publicidade, direito de acesso aos ficheiros policiais, direito de rectificação e direito de recurso

- 6.1 A autoridade de controlo deverá tomar as medidas necessárias para se certificar de que o público está informado da existência dos ficheiros, objecto da notificação, bem como dos respectivos direitos em relação a estes ficheiros. A implementação deste princípio deverá ter em conta a natureza específica dos ficheiros *ad hoc*, nomeadamente a necessidade de evitar prejuízos graves para o desempenho de uma tarefa legítima dos serviços policiais.
- 6.2 O indivíduo objecto dos dados deverá poder ter acesso a um ficheiro policial, em intervalos regulares, e sem demoras excessivas, em conformidade com o direito interno.
- 6.3 O indivíduo objecto dos dados deverá, sempre que conveniente, poder exigir a rectificação dos dados contidos no ficheiro.

Os dados pessoais, cujo exercício do direito de acesso, revele serem incorrectos, excessivos ou irrelevantes, em aplicação de qualquer outro princípio contido nesta Recomendação, deverão ser eliminados, rectificadados ou objecto de uma declaração de rectificação anexa ao ficheiro.

Estas medidas de eliminação ou de rectificação deverão estender-se, tanto quanto possível, a todos os documentos que acompanhem o ficheiro policial e, caso tal não seja feito imediatamente, deverá sê-lo no momento do tratamento subsequente dos dados ou da sua próxima comunicação.

- 6.4 O exercício dos direitos de acesso, rectificação e eliminação só deverá ser limitado quando a limitação for imprescindível para a realização de uma tarefa legítima da polícia, ou quando tal for necessário para a protecção do indivíduo objecto dos dados, ou dos direitos e liberdades de terceiros.
No interesse do indivíduo objecto dos dados, a legislação aplicável a casos específicos pode prescindir de declaração escrita.
- 6.5 A recusa ou limitação desses direitos deverá ser fundamentada por escrito. Só deverá ser possível recusar a comunicação da fundamentação quando tal for indispensável para a realização de uma tarefa legítima da polícia, ou quando tal for necessário para a protecção dos direitos e liberdades de terceiros.
- 6.6 Em caso de recusa de acesso, o indivíduo objecto dos dados deverá poder apelar para a autoridade de controlo, ou para outra entidade independente, que verificará se a recusa se encontra bem fundamentada."

Mais uma vez, o Memorandum Explicativo é muito útil e detalhado, mas por questões de espaço não é possível transcrever, na íntegra, os respectivos comentários. É conveniente referir, pelo menos, os pontos mais importantes.

Em primeiro lugar, a Recomendação revela claramente que a disposição de derrogação, contida na Convenção de Protecção de Dados, não permite a recusa taxativa dos direitos do indivíduo objecto dos dados, no que respeita aos dados policiais - é exactamente o oposto:

"O requisito da publicidade da existência de ficheiros policiais, bem como no que se refere aos direitos do indivíduo face aos ficheiros policiais, é de importância fundamental." (n.º 81)

Além disso, a Recomendação é mais específica e estrita do que a cláusula derogatória contida na Convenção de Protecção de Dados, quando prevê restrições ao princípio da publicidade e ao exercício do direito de acesso, rectificação e eliminação, em benefício da própria polícia. Assim, a publicidade acerca da existência de determinados ficheiros policiais pode ser limitada, mas apenas com base na "necessidade de evitar um *prejuízo grave* à realização de uma tarefa legítima" da polícia. Sem revelar pormenores operacionais, que é preciso proteger, deverá estar disponível o máximo de informação.

É muito importante que as restrições ao direito de acesso aos ficheiros policiais sejam "*indispensáveis* para a realização de uma tarefa legítima da polícia": trata-se claramente de uma comprovação mais estrita do que o requisito geral contido na alínea a) do n.º 2 do artigo 9º da Convenção de Protecção de Dados (derivado do n.º 2 das disposições substantivas da Convenção dos Direitos Humanos, incluindo o n.º 2 do artigo 8º da mesma Convenção), que a derrogação aos direitos do indivíduo objecto dos dados,

no interesse da "repressão criminal" tem que ser "*necessária* numa sociedade democrática" para atingir esses fins.

A mesma comprovação estrita se aplica, também, à recusa de fundamentar a recusa do acesso. As duas questões deverão ser avaliadas em separado. Quando o acesso é recusado (porque tal se torna imprescindível para a tarefa em curso) continua a ser necessário uma decisão judicial separada, relativa à questão de saber se o indivíduo objecto dos dados, que apresenta o pedido de acesso, pode ser informado do motivo da recusa de acesso.

É preciso sublinhar a importância de apresentar os motivos que levam à recusa de acesso: tal demonstra, como referido no Memorandum Explicativo:

"que o dever conferido à polícia pelo Princípio 6.4.- ponderar os direitos do indivíduo objecto dos dados em relação com interesses superiores contidos naquele Princípio - foi exercido." (n.º 91)

A Recomendação introduz, também, medidas compensatórias claras, em circunstâncias em que a informação acerca da existência de um ficheiro, do acesso a um ficheiro, ou de uma decisão fundamentada a justificar a recusa de acesso, ou um pedido de rectificação ou eliminação, são definidas. Nestes casos:

"O indivíduo objecto dos dados deverá poder apelar para a autoridade de controlo, ou para qualquer outra entidade independente, que verificará se a recusa se encontra bem fundamentada." (Princípio 6.6)

A Recomendação prevê claramente a "autoridade de controlo" como a primeira instância para tais recursos. A referência contida no Princípio 6.6, a "outra entidade independente", não deverá ser entendida como significando que poderão ser criadas outras entidades de supervisão, idênticas às autoridades de protecção geral de dados de um país, para tratar dos pedidos de acesso, etc., relativamente aos ficheiros policiais. Os autores da Recomendação consideraram que não era conveniente criar uma entidade de protecção de dados concorrente, para o sector policial (n.º 31 do Memorandum Explicativo). Em vez disso, é preferível que em alguns países, os recursos das recusas de acesso, etc. aos ficheiros policiais sejam resolvidos directamente pelos tribunais (p. ex. tribunais administrativos). De facto, o Memorandum Explicativo sublinha que, quando os Estados apresentam um primeiro recurso à autoridade de controlo, tal não deverá substituir uma nova reanálise ou a análise judicial:

"Mas, independentemente desta possibilidade (de recorrer para a autoridade de controlo), o indivíduo objecto dos dados goza, efectivamente, do direito de recorrer a um tribunal para poder rectificar ou completar um ficheiro, quando tal lhe tenha sido recusado." (n.º 94)

É precisamente essa ligação tão directa com a prática, que torna a Recomendação tão poderosa: as regras acabadas de referir não são apenas ideais, princípios teóricos, mas sim níveis práticos, muitas vezes já em vigor

nos Estados-membros do Conselho da Europa, aplicáveis também no âmbito de Schengen e em breve no âmbito da Europol.

4. Conceitos internacionais de influência no quadro europeu

4.1. Considerações gerais

A cooperação policial na Europa resultou numa multiplicidade de órgãos consultivos, internacionalmente activos, assim como em práticas formais e informais de cooperação policial/aduaneira transfronteiriça. As estruturas de cooperação divergem em termos de competências territoriais, áreas criminais, bem como de qualidade e intensidade da cooperação. À medida que se estuda a substituição do antigo pelo novo sistema de cooperação policial europeia, é óbvio que as estruturas descoordenadas da cooperação policial europeia vão sendo gradualmente substituídas por uma estrutura institucional mais firmemente integrada, apoiada por um processo de formalização e centralização. Além disso, existe uma valorização, cada vez maior, da responsabilidade, aumentando a sensibilidade para a protecção de dados no domínio policial.

Para ilustrar estas considerações apresentarei, em seguida, algumas observações relativas a questões de protecção de dados com que me deparei ao estudar os conceitos da Interpol, Schengen e Europol. Os focos de preocupação estão relacionados com as seguintes questões:

- Eventual inadequação da protecção de dados pessoais sensíveis, susceptíveis de serem objecto de uma ampla circulação,
- Falta de soluções eficazes para os indivíduos que podem sofrer em consequência do processamento incorrecto ou não autorizado de dados pessoais.

Por razões óbvias, este estudo é limitado à Interpol, Schengen e Europol, embora outros sistemas (tais como a UCLAF e os Oficiais de Ligação nas Embaixadas) mereçam a mesma atenção.

4.2. A Interpol e o seu Grupo de Trabalho Europeu "Protecção de Dados"

Em 1990, na Assembleia Geral da Interpol, a Delegação dos Países Baixos levantou a questão da emergência de legislação de protecção de dados na Europa e manifestou o seu receio de que a violação dessa legislação pudesse representar uma séria ameaça para a cooperação policial internacional através dos canais da Interpol. O Grupo de Trabalho Europeu "Protecção de Dados" foi constituído na sequência da 20ª Conferência Regional Europeia, realizada em Londres, em 1991.

O Grupo de Trabalho identificou três áreas principais para uma investigação mais aprofundada:

1. Os desenvolvimentos europeus, nomeadamente o artigo 8º da Convenção Europeia dos Direitos Humanos, a Convenção de Protecção de Dados de 1981, do Conselho da Europa, a Recomendação R (87)

15, do Conselho da Europa, que regula a utilização de dados pessoais no sector da polícia, a Convenção de Aplicação do Acordo de Schengen, o próprio Sistema de Informação Schengen, o projecto de directiva do Conselho da Comunidade Europeia relativa à protecção de dados e as propostas de criação da Europol.

2. As implicações para a protecção de dados, da introdução da *Automated Search Facility (ASF)*, da Interpol.
3. Problemas específicos da protecção de dados, incluindo:
 - a) Respeito das restrições impostas aos países receptores da informação;
 - b) Ausência de uma distinção exacta entre a informação enviada para fins policiais e judiciais;
 - c) Incerteza no que se refere ao direito de acesso do indivíduo objecto dos dados;
 - d) Observação do nível de protecção dos dados pessoais, atribuído por um país receptor antes da transmissão;
 - e) A questão de saber se a ausência de legislação de protecção de dados num país receptor pode constituir um impedimento à cooperação;
 - f) A questão de saber se as disposições em matéria de protecção de dados, no âmbito da Interpol, são suficientes à luz dos desenvolvimentos em curso, em matéria de níveis internacionais de protecção de dados.

O Grupo de Trabalho analisou as questões identificadas de 1 a 3 supra, à excepção das alíneas e) e f) do ponto 3. O Grupo de Trabalho concluiu que, embora todas essas questões fossem relevantes e importantes não as podia abordar, nesta fase.

O Grupo de Trabalho concluiu que as áreas problemáticas se podem sintetizar do seguinte modo:

- (1) Existe divergência de interpretação da terminologia amplamente utilizada no trabalho da Interpol;
- (2) Existe falta de controlo da utilização da informação policial como prova em processos judiciais;
- (3) Existe falta de controlo ao nível do direito de acesso dos indivíduos objecto dos dados à informação transmitida entre os Gabinetes Centrais Nacionais através dos canais da Interpol;

- (4) Existem incertezas acerca da existência ou da natureza da legislação em matéria de protecção de dados nos países receptores da informação;
- (5) Existem incertezas quanto à existência ou à natureza de outros requisitos legais nacionais, que afectam a utilização da informação transmitida entre os Gabinetes Centrais Nacionais através dos canais da Interpol;
- (6) Tal como já referido, a emergência, ao nível internacional, de requisitos básicos em termos de protecção de dados, no que respeita à utilização da informação policial;
- (7) Requisitos específicos a respeitar, quanto à divulgação automatizada da informação policial.

O Grupo de Trabalho apresentou as suas conclusões na Assembleia Regional Europeia de Berna, em 1993. Essas conclusões incluíam recomendações destinadas a abordar, a curto prazo, as áreas problemáticas e uma proposta de solução a longo prazo, a qual consistia na elaboração de uma convenção que providenciasse o quadro legal para o intercâmbio de informações da Interpol.

Sempre foi reconhecido que as recomendações não tinham efeito vinculativo sobre os Gabinetes Centrais Nacionais, dado que estes se encontram vinculados pelo seu direito nacional, mas era, pelo menos, um começo para abordar algumas das limitações do intercâmbio de informações da Interpol. A elaboração de uma convenção era, em princípio, uma proposta atractiva, embora fosse, na verdade, uma tentativa impressionante de chegar a um consenso global. A Assembleia Europeia de 1993 adoptou este ponto de vista e rejeitou a opção. A Assembleia apreciou, contudo, a abordagem de curto prazo, a qual foi posteriormente adoptada, por unanimidade, na Assembleia Geral de 1993.

4.3 Schengen

Como princípio fundamental, a Convenção de Aplicação do Acordo de Schengen exige a conformidade com a Convenção do Conselho da Europa e a Recomendação R (87) 15, através das legislações nacionais dos Estados-membros.

A abordagem consiste em se apoiar, tanto quanto possível, no direito nacional para elaborar disposições específicas relativas à Convenção, para fazer face a situações que são do domínio das jurisdições nacionais ou em caso de diferendo. A Convenção oferece os mecanismos para a resolução de diferendos e para garantir a adequada supervisão da protecção de dados na globalidade do sistema. A Convenção contém disposições específicas relativas à qualidade dos dados e princípios de segurança, definindo os dados que podem ser conservados para os fins estabelecidos na Convenção, definindo regras para a manutenção ou eliminação de dados e regras para a divulgação de dados, especificando as medidas de controlo do acesso, bem como as medidas de segurança. A responsabilidade pela qualidade dos dados é também claramente definida. Os direitos do cidadão são

salvaguardados através de mecanismos que permitem ao cidadão exercer os seus direitos e interpor recurso. A Convenção de Aplicação do Acordo de Schengen contém também disposições relativas à cooperação entre autoridades de supervisão da protecção de dados através de uma autoridade de controlo comum.

A Convenção de Aplicação do Acordo de Schengen é muitas vezes referida como um modelo para parcerias de cooperação, nas áreas policiais e em áreas afins. É, contudo, um modelo não totalmente adequado para a Europol. Em primeiro lugar, a arquitectura do Sistema de Informação Schengen, que prevê a existência de uma cópia da base de dados Schengen em cada Estado Parte, facilita a aplicação das regras internas de protecção de dados. Em segundo lugar, e mais importante ainda, Schengen só tem a ver com o intercâmbio de dados, mesmo que um sistema central se ocupe da transferência dos dados armazenados para as bases de dados nacionais. A Europol também tem essa função de intercâmbio, mas foi instituída concretamente com uma função de análise, que leva a produzir novos dados que não eram anteriormente "propriedade" de nenhum Estado-membro participante. O modelo Schengen de protecção de dados não é adequado a esta situação e ficou demonstrado não ser possível garantir a efectiva protecção de dados com a simples adopção do modelo Schengen.

4.4 Interpol e Europol: abordagens diferentes para as mesmas questões

Interpol versus Europol

As preocupações, em termos de protecção de dados, identificadas e abordadas pelo Grupo de Trabalho da Europol, entre 1991 e 1993, não diferem, na essência das preocupações manifestadas no debate sobre a Convenção Europol. É importante verificar que o Grupo de Trabalho da Europol considerou que o desenvolvimento de um nível europeu para a utilização de dados policiais, através dos canais Schengen e Europol, representaria uma ameaça para o intercâmbio de dados pessoais através dos canais da Interpol. Considerou-se que se a Interpol funcionasse com um nível inferior de protecção de dados na Europa, colocar-se-ia em desvantagem e sob ameaça. Este aspecto é algo perturbador, na medida em que se calculou que mais de 80% dos intercâmbios de informação da Interpol têm origem na Europa ou alguma ligação à Europa. A dificuldade em chegar a um consenso, quanto a uma Convenção Europol (dentro da União Europeia, com a sua elevada concentração de legislação em matéria de protecção de dados), é prova das complicações existentes. Convém ter em mente que a Interpol presta assistência na implementação de acordos bilaterais e multilaterais e do princípio da reciprocidade. Afirma-se, talvez com alguma justificação, que a força da Interpol reside no seu carácter informal. A Interpol é uma organização movida pela polícia e em nome da polícia.

Por outro lado, a Europol tinha que assentar num acordo político apoiado por uma convenção. A criação da Europol permitiu que os Estados-membros enfrentassem as questões que a Interpol escolheu evitar: a criação de uma convenção legalmente vinculativa, contendo artigos relativos ao intercâmbio

de informação e à protecção de dados. Neste contexto, é interessante verificar que recentemente a Interpol considerou a possibilidade de alterar a sua constituição, de modo a que os Estados, e não as forças policiais, fossem membros da sua organização. Esta abordagem foi largamente entendida como uma tentativa de alargar o estatuto da Interpol, talvez a par do estatuto da Europol, atribuindo-lhe o estatuto de organização intergovernamental. Supõe-se que esta proposta abortou, porque um Estado só pode ser vinculado desta maneira mediante a conclusão de um acordo. Se tal proposta tivesse sido adoptada, talvez implicasse a exigência, por parte de alguns Estados, de uma convenção relativa às questões da protecção de dados. Dada a história recente da Interpol, em matéria de protecção de dados, esta proposta não era de modo nenhum atractiva e a questão parece ter sido votada ao fracasso.

O papel da Europol no quadro europeu da aplicação da lei

Intelligence (Informação)

A Europol obtém, a partir de uma variedade de fontes, informações relativas à actividade criminal. Através da compilação e análise desta e de outra informação, a Europol produzirá nova informação e um novo conhecimento, designado *intelligence* (informação), para uso potencial de investigadores ou de decisores políticos.

As actividades da Europol, no âmbito da informação, baseiam-se, antes de mais, nos dados e na informação fornecidos pelos serviços de aplicação da lei dos Estados-membros, e acessíveis em conformidade com a Convenção Europol e regulamentação afim. Os dados e a informação adequados são armazenados no Sistema de Informação da Europol e, para efeitos de um projecto específico, nos Ficheiros de Trabalho Analítico, apoiados pelo Sistema Index, sob o controlo específico dos princípios "necessidade de saber" e "direito a utilizar", à luz das actividades e objectivos da Europol.

O processo de informação relativo a projectos pode implicar o envolvimento de alguns ou de todos os serviços de aplicação da lei e organizações dos Estados-membros, junto dos quais poderá ser obtida toda a informação disponível, através das Unidades Nacionais Europol.

A Europol terá que resolver as dificuldades que possam surgir, no que respeita à partilha da informação obtida de fontes sensíveis. Da mesma maneira, e de forma prioritária, é necessário desenvolver soluções para estes problemas, acordadas pelos Estados-membros, à medida que a Europol evolui. Encontrar as soluções convenientes exige um pensamento um tanto radical, em articulação com uma abordagem flexível.⁷

Os dados e a informação da Europol são desenvolvidos numa abordagem proactiva, por agentes de informação, analistas e oficiais de ligação Europol,

⁷ Esta questão, e muitas outras relacionadas com a informação, foi objecto de discussão aprofundada na Conferência "Intellex" (Noordwijk, Maio de 1997).

que trabalharão em projectos estratégicos e operacionais, no âmbito de quatro categorias principais de actividade:

- Relatórios anuais sobre áreas de criminalidade contidas no mandato da Europol, incidindo sobre os problemas da criminalidade organizada internacional;
- Pedidos *ad hoc* de assistência, apresentados por serviços de aplicação da lei dos Estados-membros, com vista a fornecer uma perspectiva da União Europeia sobre a actividade criminal e a aplicação da lei, nomeadamente de natureza operacional, mas também, em alguns casos, sob uma perspectiva estratégica (por exemplo, novos fenómenos, etc.), mantendo os vários pontos de vista de cada Estado-membro;
- Questões identificadas ao nível interno, tais como novas tendências, padrões e principal actividade criminal de grupos específicos;
- Actividades específicas em nome dos diferentes *fora*, como o Conselho, Grupos de Trabalho, Conselho de Administração, etc.

O modelo de informação

O modelo de informação está actualmente em fase de desenvolvimento e tem que respeitar os cinco princípios que se seguem:

1. As actividades e os produtos da Europol têm que ter uma finalidade e um objectivo claros. Não se pretende manter grandes quantidades de dados antigos na esperança de que um dia possam vir a ser úteis, não fazendo o melhor uso da informação e dos recursos disponíveis;
2. Em consequência, a Europol tem que saber e ser capaz de especificar qual a informação necessária, aceder ao material adequado (os oficiais de ligação Europol têm acesso indirecto às bases de dados dos vários Estados-membros) e utilizar da melhor forma esta informação, segundo a sua própria perspectiva ou a dos seus parceiros;
3. Tem que funcionar de forma organizada com as devidas avaliações e decisões, sempre que necessário;
4. A flexibilidade é um aspecto de extrema importância. O ambiente em que a Europol funciona estará em permanente mutação (ou seja, o mundo físico, as pessoas, os criminosos, a tecnologia, a sociedade, os negócios, os governos, as leis, etc.). As solicitações feitas à Europol continuarão a mudar. A experiência ensinará à Europol a melhor forma e a forma mais eficaz de realizar as suas tarefas. O modelo tem que ser capaz de fazer face à mudança, de se adaptar a ela e de identificar a necessidade de mudar. A este respeito, seria útil uma abordagem de projecto, de modo a ir ao encontro das necessidades dos "consumidores da Europol";
5. Uma abordagem modelar facilitaria a concepção de uma estrutura flexível. Consistiria em componentes facilmente adaptáveis, tal como as relações entre eles.

Estes princípios ditam a estrutura do modelo - o modelo de informação - que é a base da forma como toda a organização funciona.

No cerne do modelo estará um ciclo de actividades (recepção da informação, análise da informação, produtos, etc.), que terá implicações para a Europol, na medida em que:

- Embora a Europol não seja um depósito de dados antigos, para desempenhar devidamente as funções atrás enunciadas é preciso haver um conhecimento adequado de base e alguma especialização;
- A Europol não pode depender apenas das ideias e iniciativas que venham do exterior. Tem que ter mecanismos internos que facilitem a emergência de novas ideias. Isto passa pela criação de um ambiente adequado, que favoreça a inovação e uma nova forma de pensar. Tal reflecte-se, por sua vez, nos métodos de recrutamento, formação e gestão e exige uma visão partilhada dos objectivos que a Europol se propõe alcançar;
- Cada um dos componentes do ciclo da informação exige um trabalho pormenorizado. É necessário identificar, em especial, os fluxos de informação, a par das implicações humanas e técnicas (respondendo à questão "quantas pessoas, quais as competências, fazer o quê, como, porquê, com que tecnologia?");
- Sem dados não há processo de informação. A Europol depende grandemente do que os outros lhe fornecem. Todavia, a dependência total poderia conduzir ao colapso. A Europol tem que ter a capacidade de procurar e explorar continuamente fontes de informação alternativas, quer para si própria, quer para os seus parceiros. Um exemplo do primeiro caso são as fontes abertas a que a Europol pode aceder directamente. Um exemplo do segundo caso são as novas tecnologias, os novos métodos de trabalho, as parcerias com outros serviços, que a Europol pode sugerir aos Estados-membros, de modo a permitir aos respectivos serviços policiais ou aduaneiros obterem dados que de outra forma não seria possível.

Análise

A Europol foi criada para desempenhar tarefas específicas em cooperação ou em representação dos Estados-membros da União Europeia, com ênfase para a análise de dados e de informação. Esta ênfase na análise é conseguida através do empenho da Europol num Gabinete de Análise forte, onde a Análise de Informação é a função central.

A forma como a Europol realiza a análise é regulada pela Convenção e pelas regras acordadas (por todos os Estados-membros), tais como as regulamentações sobre ficheiros de trabalho analítico e as linhas de orientação em matéria de análise.

Em qualquer projecto ou tarefa de análise, será tida em conta a informação recebida de Estados terceiros e de entidades terceiras, bem como a informação proveniente de fontes abertas.

A Europol reconhece também que outras organizações nacionais e internacionais desenvolvem um trabalho analítico valioso no âmbito da aplicação da lei e, nessa medida, desenvolverá todos os esforços para que esse trabalho seja tido em conta, a fim de evitar duplicação de esforços. A Europol procurará, também, desenvolvimentos de técnicas de análise, exemplos de boas práticas e novos sistemas dentro dos Estados-membros, quer com vista a utilizá-los no futuro, quer para informar outros analistas da União Europeia. Uma pequena ideia, ou um conceito novo, pode conduzir a novas formas de combater os meandros e a sofisticação das redes criminosas. É, por conseguinte, fundamental que estas ideias sejam promovidas pela Europol, em benefício de todos os serviços de aplicação da lei da União Europeia.

Cada aspecto específico do trabalho de análise será cuidadosamente estudado, de forma a determinar se deverá ser realizado no âmbito da Europol. As actividades realizadas pela Europol serão influenciadas pelas Unidades Nacionais Europol, pelo Conselho de Administração ou pelos políticos. Além disso, a Europol identificará áreas problemáticas, em resultado da compilação de relatórios estratégicos, ou da informação contida no sistema informático da Europol. Porém, a este respeito, um produto desenvolvido pela Europol tem que ter um cliente claramente identificado, com o envolvimento de outros. Sem este requisito, um documento "perfeito" pereceria nas caves da Europol.

Protecção de dados Europol

Dada a abordagem ambiciosa da recolha e utilização da informação, não constitui qualquer surpresa que cerca de metade das disposições da Convenção Europol incidam sobre a protecção de dados pessoais. Os requisitos de base são estabelecidos pelo artigo 3º. Tal como no Sistema de Informação Schengen, cada Estado-membro deverá implementar, na sua legislação nacional, um nível de protecção de dados pelo menos idêntico ao exigido pela Convenção de 1981, do Conselho da Europa. Ao legislarem, os Estados-membros têm também que ter em conta a Recomendação R (87) 15. Os Estados-membros não podem tomar parte nos acordos propostos para o intercâmbio de dados pessoais, enquanto não tiver entrado em vigor a respectiva legislação nacional na matéria.

A Europol deverá "ter em conta os princípios" da Convenção e da Recomendação do Conselho da Europa. O artigo 15º restringe a utilização dos dados obtidos a partir do sistema de informação, excepto quando a sua utilização permita às autoridades competentes dos Estados-membros prevenir ou reprimir crimes graves. Mediante consentimento prévio da unidade de proveniência e nos termos estipulados pela mesma, os dados poderão ser utilizados para outros fins, nomeadamente para efeitos de informação e para serviços secretos. O artigo 18º prevê a correcção ou a

eliminação dos dados incorrectos ou que violem as regras da Convenção. O artigo 19º estabelece os períodos de conservação dos dados e o controlo da necessidade de manter esses dados armazenados. O artigo 20º prevê um controlo idêntico dos dados contidos em ficheiros de papel.

Para além da Convenção, haverá regras específicas, adaptadas exclusivamente à actividade operacional da Europol. Do ponto de vista da protecção de dados, as regras mais importantes são as relativas aos Ficheiros de Trabalho Analítico, que requerem a aprovação do Conselho, com base no artigo 10º da Convenção. Estas regras incidem sobre os principais elementos dos níveis internacionalmente acordados, como a Recomendação do Conselho da Europa, e conterão obrigações legais vinculativas.

A existência de regras de protecção de dados suficientes, é fundamental para a criação de um sentimento de confiança na Europol. O direito do indivíduo à protecção dos dados mantidos a seu respeito tem que ser cuidadosamente ponderado, em função da necessidade efectiva para a aplicação da lei.

O artigo 19º da Convenção concede ao indivíduo objecto dos dados, a pedido, o direito a ser informado sobre os dados mantidos a seu respeito. As decisões relativas aos pedidos são tomadas no prazo de três meses. A informação pode ser recusada nos seguintes casos:

1. Para efeitos de desempenho adequado das tarefas da Europol,
2. Para salvaguarda da segurança dos Estados-membros, da segurança pública ou para combater actos criminosos,
3. Para protecção dos direitos e liberdades de terceiros.

Assim, o artigo 19º da Convenção, relativo ao direito à informação do indivíduo objecto dos dados, é uma disposição chave. É fundamental ponderar o direito regular de um indivíduo objecto de dados, com as garantias, de modo a assegurar que o objectivo global da função da Europol não seja minado.

O n.º 3 exige a recusa da informação quando tal seja necessário para o desempenho adequado da tarefa da Europol, para protecção da segurança dos Estados-membros, para preservação da segurança pública, para combater actos criminosos ou para protecção dos direitos e liberdades de terceiros. Embora o texto não seja idêntico, corresponde, em termos globais, às excepções e restrições ao direito de acesso, por parte do indivíduo objecto dos dados, previstas na Convenção do Conselho da Europa.

Quando os dados são fornecidos por um Estado-membro, esse Estado-membro goza do direito de tomar uma posição. Não é exigida qualquer justificação para a recusa de fornecer informação, caso a justificação possa comprometer o objectivo da recusa. Neste caso, o indivíduo objecto dos dados deverá ser informado de que poderá dirigir-se à autoridade de controlo

comum. O artigo 20º oferece ao indivíduo objecto dos dados o direito à correcção ou à eliminação dos dados incorrectos ou indevidamente armazenados.

O artigo 23º da Convenção exige que cada Estado-membro designe uma instância nacional de controlo, com a tarefa de controlar, de forma independente, nos termos da lei nacional, a introdução e recuperação de dados da Europol, e de analisar se tais procedimentos violam os direitos do indivíduo objecto dos dados. A instância de controlo terá acesso, através da Unidade Nacional, ao Sistema de Informação da Europol, aos gabinetes e aos documentos dos oficiais de ligação nacionais, bem como aos ficheiros de análise. O artigo 24º estabelece a criação de uma instância de controlo comum, destinada a controlar as actividades da Europol e dos oficiais de ligação, com vista a verificar se há violação dos direitos do indivíduo objecto dos dados. A instância de controlo comum será composta por dois representantes, no máximo, de cada instância nacional de controlo, e cada Estado-membro tem direito a um voto. Os cidadãos têm o direito a requerer, quer à instância nacional de controlo, quer à instância de controlo comum, a análise dos aspectos relevantes do processamento dos dados que lhes dizem respeito. Um outro aspecto importante é o facto de terem sido conferidos poderes à instância de controlo comum, para tomar a decisão final sobre recursos apresentados por indivíduos objecto de dados, relativamente aos seus direitos individuais.

Foi criada, por conseguinte, uma instância independente de controlo, para a Europol que, além disso, dispõe de competências e poderes idênticos aos das autoridades nacionais de protecção de dados. Os principais poderes são os seguintes:

- Poderes de investigação, tais como o direito a aceder aos dados e a obter toda a informação necessária ao desempenho das suas funções;
- Poderes de intervenção, como ordenar a eliminação de dados ou a suspensão do processamento que viola a Convenção.

Relativamente aos poderes da instância de controlo comum, o n.º 2 do artigo 24º determina que a Europol deverá prestar-lhe assistência, fornecer-lhe informação e conceder-lhe a oportunidade de verificar os documentos, bem como conceder-lhe acesso aos dados e às instalações. A Convenção confere poderes de investigação à instância de controlo comum. O artigo 24º estabelece também que a Europol tem que respeitar as decisões da instância de controlo comum, relativamente a processos de recurso.

A instância de controlo comum poderá intervir também no âmbito do n.º 3 e do n.º 5 do artigo 24º. Pode apresentar propostas ao director da Europol, para melhoria da protecção de dados, ou queixas referentes a qualquer violação das disposições relevantes da Convenção. Pode, também, informar o Conselho de Administração da Europol sobre quaisquer problemas de protecção de dados e nos casos em que haja divergência de opinião com o director da Europol.

Outro aspecto importante da instância de controlo comum é o facto de ter que dar o seu parecer sobre cada ordem de abertura de um Ficheiro de Trabalho de Análise, em conformidade com o artigo 12º da Convenção. Estas ordens são aprovadas pelo Conselho de Administração, antes que tal ficheiro possa ser criado, e as ordens deverão conter todas as características importantes do ficheiro em questão, como os fins e as categorias dos dados a introduzir. O Conselho de Administração tem que ter o parecer da instância de controlo comum, antes da aprovação dessas ordens.

É lógico que, neste contexto, tenham sido levantadas questões acerca da rigidez das regras, face ao intercâmbio de dados entre a Europol e outras organizações internacionais, como a Interpol, e o intercâmbio de dados entre a Europol e outras bases de dados internacionais, tais como o Sistema de Informação Schengen, o Sistema de Informação Europeu e o Sistema de Informação Aduaneira. Embora a Convenção não estabeleça regras muito precisas nesta matéria, as negociações recentemente havidas em Bruxelas revelaram que os Estados-membros estão bem conscientes das dificuldades neste domínio e o primeiro trabalho sobre as regras de tal cooperação mostra que há um consenso geral, quanto a garantir o respeito dos princípios contidos na Convenção de Protecção de Dados e na Recomendação.

As disposições em matéria de protecção de dados são exaustivas em teoria, mas o verdadeiro desafio que se poderá colocar reside na sua aplicação. Dentro da União Europeia, o sistema dependerá, fundamentalmente, do grau de respeito da protecção de dados e dos direitos individuais por parte de cada agente policial envolvido. Tal exigirá uma formação rigorosa, mas também, em muitos casos, uma mudança radical da cultura e da força nacional em questão. Quando se junta este aspecto ao sentimento que reina entre alguns agentes policiais (tanto aqui, como no estrangeiro), de que os fins podem justificar os meios para apanhar os criminosos, torna-se evidente o perigo potencial. Nenhum regulamento terá muita utilidade se as forças nacionais não garantirem o cumprimento rigoroso do mesmo.

4. Conclusões

A ameaça que representam todas as formas de criminalidade organizada tem conduzido a uma necessidade, cada vez maior, de informação, em especial, quando se trata de acções de aplicação da lei. Daqui resulta uma ameaça para as liberdades cívicas do indivíduo, em matéria de dados pessoais.

Além das convenções que têm grande impacto na utilização e intercâmbio de dados pessoais, foram e continuam a ser desenvolvidas regulamentações específicas, aplicáveis às actividades de aplicação da lei.

A Convenção de Aplicação do Acordo de Schengen e, em especial, a Convenção Europol, introduziram pré-requisitos cada vez mais fortes. Considero que tal facto conduzirá a níveis mais elevados de protecção de dados, que serão aplicados, não só no âmbito das actividades da Europol,

mas também em outros *fora* e em âmbitos que dominam a cena internacional da aplicação da lei. Penso que, com estes desenvolvimentos, está a ficar mais claro que se prevalecer esta tendência para formalizar e proteger o armazenamento e intercâmbio de informação, por parte das autoridades (internacionais) de aplicação da lei, todos os sistemas informais de recolha e divulgação de informação têm os dias contados.

Sistemas de informação policial na União Europeia

Charles Elsen

Director Geral da DG H – Justiça e Assuntos Internos
Secretariado do Conselho da União Europeia

1. É minha intenção limitar-me a fazer algumas reflexões (em sentido lato) sobre questões de cooperação policial no âmbito do terceiro pilar e problemas de protecção de dados relacionados com estas questões. Gostaria de chamar a atenção para o facto de as minhas observações serem meramente pessoais e não reflectirem qualquer posição oficial da instituição a que pertenço.

2. A protecção de dados tem sido um tema importante da cooperação europeia, fora do âmbito da União Europeia, desde a elaboração do primeiro instrumento pelo Conselho da Europa (Convenção nº108 de 1981). Com a expansão das actividades, no seio do terceiro pilar, no âmbito daquilo a que se pode chamar as áreas sensíveis da protecção de dados, torna-se fundamental garantir que os instrumentos acordados no seio da União Europeia, não só tenham em conta a necessidade de respeitar a legislação em matéria de protecção de dados, mas dêem particular atenção às modalidades da criação de autoridades de controlo comuns, independentes.

3. No âmbito da União Europeia, foram elaborados três instrumentos principais no combate à criminalidade internacional. O mais importante desses instrumentos é, sem dúvida, a Convenção Europol, assinada em 1995; o processo de ratificação ficou concluído em Junho de 1998, durante a presidência do Reino Unido, e a Convenção Europol entrará em vigor a 1 de Outubro de 1998. Durante as negociações que conduziram à assinatura da Convenção, as delegações empenharam-se em proteger o direito dos cidadãos europeus à vida privada, porque não podemos esquecer que a Europol irá lidar com dados muito sensíveis e, nessa medida, é necessário proteger o direito à vida privada. Por essa razão, a Europol contém artigos específicos sobre a protecção de dados pessoais.

4. O segundo instrumento, que é preciso referir, é a Convenção da Cooperação Aduaneira de 1995 relativa à cooperação neste domínio. A Convenção foi assinada em Dezembro de 1995 e o processo de ratificação está em curso. Também no âmbito da cooperação aduaneira internacional se procede a uma troca de dados muito sensíveis entre as várias autoridades envolvidas. Mais uma vez, a premente necessidade de proteger os dados pessoais levou à inclusão de artigos específicos sobre protecção de dados na Convenção.

5. A terceira das Convenções referidas, que ainda não foi assinada, é a Convenção Eurodac, que tem por objectivo criar um sistema de prevenção da violação das disposições em matéria de asilo da Convenção de Dublin. Também no âmbito da Convenção de Dublin se procede a uma compilação

de dados sensíveis relativos aos requerentes de asilo, tornando imperativa a protecção de dados pessoais.

6. É preciso referir, também, a Convenção de Schengen. Embora continue fora da UE, a Convenção de Schengen está estreitamente ligada ao terceiro pilar. As medidas paralelas, implementadas a par da abertura das fronteiras internas, envolve um forte intercâmbio de dados. O Sistema de Informação Schengen, embora de âmbito limitado, foi concebido para tornar possível o rápido intercâmbio de dados entre os serviços europeus de aplicação da lei. Também no âmbito de Schengen foi definido um sistema de protecção de dados pessoais.

7. Se analisarmos estes quatro sistemas, podemos concluir o seguinte:

a) Todos os sistemas foram definidos, essencialmente, para facilitarem o intercâmbio de informação entre os serviços europeus de aplicação da lei e os órgãos administrativos; tal intercâmbio de dados pessoais exigiu a criação de mecanismos que assegurassem a protecção dos cidadãos europeus;

b) As quatro Convenções prevêm sistemas de protecção da vida privada do cidadão europeu e a estrutura de todos estes sistemas é claramente idêntica.

8. No seguimento desta última conclusão, gostaria de sublinhar que, embora as estruturas não sejam muito diferentes, as normas substantivas, aplicáveis a cada entidade, não são idênticas. Sem querer entrar numa discussão exaustiva sobre as normas substantivas, passarei a desenvolver algumas reflexões sobre um determinado número de questões estruturais.

9. Gostaria de acrescentar que parece necessário, pelo menos do ponto de vista de alguns Estados-membros, a inclusão de normas de protecção de dados em outros instrumentos que se encontram actualmente em discussão.

Tal pode ser demonstrado, por exemplo, em negociações como as relativas à Convenção sobre inibição do direito de conduzir e a Convenção relativa à assistência judiciária. Para cada nova Convenção é criada uma nova instância de protecção de dados. Embora o raciocínio que está por trás desta evolução seja compreensível, a situação pode criar problemas no futuro.

a) Em primeiro lugar, é inquestionável que existe uma clara relação entre os dados transferidos no âmbito das quatro Convenções: trata-se sempre de informação policial/aplicação da lei. Para os cidadãos europeus, poderia ser muito confuso verem-se confrontados com, pelo menos, quatro instâncias europeias diferentes de protecção de dados. Por exemplo, a que autoridade o Sr. Janvier, de Bordéus, deverá recorrer quando tiver um problema com a Europol, sobre uma questão relacionada com os serviços aduaneiros e que envolva, também, requerentes de asilo? No interesse da transparência, é importante que

as pessoas tenham a noção clara dos seus direitos e da forma como tais direitos podem ser exercidos.

b) Em segundo lugar, seria possível que quatro instâncias diferentes dessem origem a jurisprudência diferente? Embora os problemas estejam mais ou menos relacionados, não há, actualmente, qualquer garantia de que as quatro instâncias dêem respostas idênticas a problemas idênticos, uma situação que poderia conduzir ao "forum-shopping".

c) Finalmente, durante um período de cortes nas despesas, quer ao nível nacional, quer ao nível da União Europeia, a criação de quatro instâncias diferentes poderia ser entendida como um exagero. Sem coordenação, as quatro instâncias necessitariam de quatro (pequenos) secretariados e, mais importante ainda, de quatro infra-estruturas de tradução e interpretação.

1. Olhando para as quatro instâncias de protecção de dados, cada qual com tarefas diferentes, mas com uma composição idêntica, é preciso tentar resolver alguns dos problemas estruturais. Para ser directo, porque é que não se opta por fundir as quatro instâncias de que acabei de falar, passando essa entidade final a exercer as suas competências em conformidade com as disposições das Convenções Europol, Cooperação Aduaneira, Eurodac e Schengen? Desta forma, poderíamos ter uma única instância com diferentes tarefas e com diferentes membros. As vantagens desta solução são inegáveis:

a) Uma instância, ou seja, um endereço para todos os assuntos relacionados com a protecção de dados, no âmbito da protecção policial.

b) Uma estrutura que facilitaria a coordenação e a harmonização da jurisprudência.

c) Uma estrutura que implicaria a criação de um único secretariado e de uma única infra-estrutura.

d) Uma tal solução permitiria à instância única funcionar sem afectar as normas substantivas contidas nas quatro Convenções; essa instância funcionaria com base num simples Tratado Fusão, sem ser necessário entrar nos pormenores dos princípios da protecção de dados, contidos nas Convenções Europol, Cooperação Aduaneira, Eurodac e Schengen.

11. É certo que poderá argumentar-se que esta instância única representaria um fardo pesado para os seus membros, implicando um regime de trabalho quase a tempo inteiro. Embora, em meu entender, tal situação não venha a apresentar-se num futuro próximo, não vejo qualquer problema em que seja criada uma entidade especializada em protecção de dados, ao nível europeu.

12. É preciso ter em conta que a existência de uma única instituição, provavelmente implicaria a sua localização num único lugar, simplificando, assim, as questões de infra-estrutura, como por exemplo, as instalações para funcionamento do secretariado e para as reuniões.

13. Na última reunião do Conselho, o ministro italiano apresentou um documento no qual sublinhava a necessidade de uma reflexão sobre a coordenação dos trabalhos no âmbito da protecção de dados. O Conselho solicitou ao K4 que estudasse esta questão, tendo os trabalhos tido início na semana passada. Tratou-se, apenas, de uma discussão preliminar, que continuará na próxima reunião do K4, com base no documento anunciado, do gabinete jurídico do Conselho.

14. Eu, pessoalmente, acredito que, uma vez iniciada a discussão, haverá várias opiniões quanto ao procedimento a adoptar, ou seja:

- os que são a favor de um único instrumento horizontal de protecção de dados e de uma única instância de protecção de dados, mas que reconhecem as especificidades dos vários instrumentos;
- os que, pelo contrário, consideram que as diferenças entre os vários instrumentos são tão grandes que uma única abordagem parece inútil;
- os que consideram que, mesmo que seja necessário haver diferentes instrumentos, devido aos seus objectivos, existem princípios comuns e alguma necessidade de as instâncias comuns lidarem com este tipo de questões.

15. A proposta italiana, descrita no documento 8321/98 JAI 15, coloca as questões pertinentes, que passo a citar: "Seria necessário uma análise com vista a:

- analisar se existem, efectivamente, inconsistências ao nível da protecção, apesar de as circunstâncias serem idênticas;
- definir, com mais exactidão, os níveis aplicáveis a cláusulas de protecção de dados, a incluir em acordos futuros;
- reunir informação mais precisa relativa às relações existentes entre as diferentes bases de dados utilizadas, a nível nacional e internacional, para fins judiciais e de aplicação da lei, com vista a evitar duplicações e inconsistências no que respeita às características comuns dos vários sistemas informáticos;
- avaliar a viabilidade, a médio prazo, da redução do número, ou da fusão, das diferentes instâncias comuns de supervisão no sector da protecção de dados."

16. A resolução de Dublin, dos comissários da protecção de dados, de "acolherem todas as iniciativas que contribuam para um nível elevado de harmonização" vai no mesmo sentido. É de louvar a intenção dos comissários de cooperarem neste âmbito.

17. As regras de protecção de dados estão a crescer como cogumelos depois de um dia chuvoso de Outono. Deveríamos concentrar os nossos esforços na elaboração de regras claras e exaustivas, no interesse dos nossos cidadãos,

e criar instrumentos que garantam os direitos dos cidadãos, que respondam a critérios de uma gestão sã e de uma abordagem coerente.