



**01248/07/PT
WP 136**

Parecer 4/2007 sobre o conceito de dados pessoais

Adoptado em 20 de Junho

O Grupo de Trabalho foi instituído pelo artigo 29.º da Directiva 95/46/CE. Trata-se de um órgão consultivo europeu independente em matéria de protecção de dados e de privacidade. As suas atribuições estão descritas no artigo 30.º da Directiva 95/46/CE e no artigo 15.º da Directiva 2002/58/CE.

O secretariado é assegurado pela Direcção C (Justiça Civil, Direitos Fundamentais e Cidadania) da Direcção-Geral Justiça, Liberdade e Segurança da Comissão Europeia, B-1049 Bruxelas, Bélgica, Gabinete nº LX-46 01/43.

Sítio Web: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

**O GRUPO DE TRABALHO SOBRE A PROTECÇÃO DAS PESSOAS SINGULARES NO QUE DIZ
RESPEITO AO TRATAMENTO DE DADOS PESSOAIS**

instituído pela Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995¹,

Tendo em conta o artigo 29.º e a alínea a) do n.º1 e o n.º3 do artigo 30.º da referida directiva, bem como o n.º 3 do artigo 15.º da Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002,

Tendo em conta o artigo 255.º do Tratado CE e o Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de Maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão,

Tendo em conta o seu Regulamento Interno,

ADOPTOU O PRESENTE PARECER:

¹ Jornal Oficial L 28 de 23.11.1995, p. 31, disponível em:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

I. INTRODUÇÃO	3
II. CONSIDERAÇÕES GERAIS E QUESTÕES DE POLÍTICA	4
III. ANÁLISE DA DEFINIÇÃO DE “DADOS PESSOAIS” DE ACORDO COM A DIRECTIVA PROTECÇÃO DE DADOS	6
1. PRIMEIRO ELEMENTO: “QUALQUER INFORMAÇÃO”	6
2. SEGUNDO ELEMENTO: “RELATIVA A”	9
3. TERCEIRO ELEMENTO: “IDENTIFICADA OU IDENTIFICÁVEL [PESSOA SINGULAR]”	13
4. QUARTO ELEMENTO: “PESSOA SINGULAR”	23
IV. O QUE ACONTECE QUANDO OS DADOS ESTÃO EXCLUÍDOS DO ÂMBITO DA DEFINIÇÃO?	25
V. CONCLUSÕES	26

I. INTRODUÇÃO

O Grupo de Trabalho está consciente da necessidade de realizar uma análise aprofundada do conceito de dados pessoais. As informações sobre as práticas actuais nos Estados-Membros da UE apontam para alguma incerteza e diversidade entre os Estados-Membros no que toca a aspectos importantes deste conceito que poderão afectar o correcto funcionamento do actual quadro de protecção de dados em contextos diferentes. O resultado da análise de um elemento central na aplicação e interpretação das regras de protecção de dados, terá um profundo impacto em toda uma série de questões relevantes e será especialmente importante para temas como a Gestão da Identidade no contexto da Administração em linha (*e-Government*) e da Saúde em linha (*e-Health*), bem como no contexto da RFID (identificação por radiofrequência).

O objectivo do presente parecer do Grupo de Trabalho é chegar a um entendimento comum acerca do conceito de dados pessoais, das situações em que se deverá aplicar a legislação nacional de protecção de dados e da forma como esta deverá ser aplicada. É essencial dispor-se de uma definição comum da noção de dados pessoais para se poder definir o que está incluído e o que está excluído do âmbito de aplicação das regras de protecção de dados. Um corolário do presente trabalho é fornecer orientações sobre o modo como as regras nacionais de protecção de dados deverão ser aplicadas a certos tipos de situações que ocorrem em toda a Europa, contribuindo assim para uma aplicação uniforme dessas mesmas normas, o que constitui uma função central do Grupo de Trabalho do artigo 29.º.

O presente documento utiliza exemplos retirados da prática nacional das APD europeias para apoiar e ilustrar a análise desenvolvida. A maioria dos exemplos foi editada apenas para melhor se adaptar ao presente objectivo.

II. CONSIDERAÇÕES GERAIS E QUESTÕES DE POLÍTICA

A Directiva contém uma noção ampla de dados pessoais

A definição de dados pessoais constante da Directiva 95/46/CE (a seguir designada por a “Directiva de protecção de dados” ou a “Directiva”) refere o seguinte:

Entende-se por “Dados pessoais, qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social”.

Convém notar que esta definição reflecte a intenção do legislador comunitário de uma noção ampla de “dados pessoais”, que se manteve em todo o processo legislativo. A proposta inicial da Comissão explicava que “*tal como na Convenção 108, é adoptada uma definição ampla para abranger todas as informações que possam ser ligadas a determinada pessoa*”². A proposta alterada da Comissão referia que “*a proposta alterada vai ao encontro do desejo do Parlamento de que a definição de “dados pessoais” seja o mais geral possível para incluir toda a informação respeitante a uma pessoa identificável*”³, um desejo também tido em consideração pelo Conselho na posição comum⁴.

O objectivo das regras contidas na Directiva é a protecção das pessoas singulares.

O artigo 1.º tanto da Directiva 95/46/CE como da Directiva 2002/58/CE indica claramente o fim último das regras nele contidas: proteger as liberdades e os direitos fundamentais das pessoas singulares e, em especial, o direito à vida privada, no que diz respeito ao tratamento de dados pessoais. Trata-se de um elemento muito importante a ter em conta na interpretação e aplicação das regras de ambos os instrumentos que poderá ser decisivo para determinar o modo como as disposições da Directiva são aplicadas a várias situações em que os direitos das pessoas singulares não estão em risco e que poderá alertar contra qualquer interpretação das mesmas regras que privaria as pessoas singulares da protecção dos seus direitos.

O âmbito de aplicação da Directiva exclui determinadas actividades e o texto consagra uma certa flexibilidade para permitir uma resposta jurídica adequada às diferentes circunstâncias.

Apesar do conceito amplo de “dados pessoais” e de “tratamento” contido na Directiva, o simples facto de uma determinada situação poder ser considerada como envolvendo o “tratamento de dados pessoais” na acepção da definição não determina por si só que esta situação seja abrangida pelas regras da Directiva, nomeadamente pelo disposto no seu artigo 3.º. Para além das derrogações decorrentes do âmbito de aplicação do direito

² COM (90) 314 final, 13.9.1990, p. 19 (comentário sobre o artigo 2.º).

³ COM (92) 422 final, 28.10.1992, p. 10 (comentário sobre o artigo 2.º).

⁴ Posição comum (CE) n.º 1/95, adoptada pelo Conselho em 20 de Fevereiro de 1995, JO C 93 de 13.4.1995, p. 20.

comunitário, as derrogações ao abrigo do artigo 3.º têm em consideração o meio técnico de tratamento (de uma forma manual e não estruturada) e a intenção de uso (para actividades exclusivamente pessoais ou domésticas de uma pessoa singular). Mesmo nos casos em que o tratamento de dados pessoais é abrangido pelo âmbito da Directiva, nem todas as regras desta serão aplicáveis no caso em apreço. Algumas das disposições da Directiva prevêem um grau considerável de flexibilidade por forma a consagrar o equilíbrio adequado entre, por um lado, a protecção dos direitos da pessoa em causa e, por outro, os interesses legítimos dos responsáveis pelo tratamento, terceiros e o interesse público que poderá existir. A título de exemplo de disposições deste tipo, pode referir-se o artigo 6.º (período de conservação em função da necessidade dos dados), a alínea f) do artigo 7.º (avaliação do interesse para justificar o tratamento), último parágrafo da alínea c) do artigo 10.º e a alínea c) do n.º 1 do artigo 11.º (informação da pessoa em causa, quando necessário, para garantir tratamento justo) ou o artigo 18.º (derrogações aos requisitos de notificação), para mencionar apenas alguns casos.

O âmbito das regras de protecção de dados não deverá ser inadequadamente ampliado

Um resultado indesejável seria acabar por aplicar regras de protecção de dados a situações que não se pretendia contemplar e que não foram previstas pelo legislador. As derrogações materiais ao abrigo do artigo 3.º acima mencionadas e os esclarecimentos dados nos considerandos 26 e 27 da Directiva mostram a forma como o legislador pretendia que a protecção de dados fosse aplicada.

Uma limitação prende-se com a forma como os dados são tratados. É útil relembrar que as razões que levaram à aprovação das primeiras leis de protecção de dados, nos anos 70, residiam no facto de as novas tecnologias, sob forma de tratamento electrónico de dados, permitirem um acesso mais fácil e mais generalizado a dados pessoais do que as formas tradicionais de tratamento. Consequentemente, a protecção de dados ao abrigo da Directiva pretende proteger as formas de tratamento que tipicamente apresentam um maior risco de “acesso fácil aos dados pessoais” (considerando 27). O tratamento de dados não automatizado só está incluído no âmbito da Directiva quando os dados fazem parte de um sistema de arquivo ou quando se destinam a fazer parte de um sistema desse tipo (artigo 3.º).

Uma outra limitação geral à aplicação da protecção de dados ao abrigo da Directiva reside no tratamento de dados em circunstâncias em que os meios de identificação da pessoa em causa não são “susceptíveis de serem razoavelmente utilizados” (considerando 26), uma questão que será tratada posteriormente.

Mas deverá evitar-se igualmente uma restrição indevida da interpretação do conceito de dados pessoais

Nos casos em que uma aplicação mecânica de absolutamente todas as disposições da Directiva teria, à primeira vista, consequências excessivamente pesadas ou mesmo até absurdas, deverá primeiro verificar-se 1) se a situação é abrangida pelo âmbito da Directiva, nomeadamente tendo em conta o disposto no seu artigo 3.º; e 2) em caso afirmativo, se a própria Directiva ou a legislação nacional adoptada ao abrigo da mesma, não permitem derrogações ou simplificações em situações específicas por forma a proporcionar uma resposta jurídica apropriada e, ao mesmo tempo, assegurar a protecção dos direitos das pessoas singulares e dos interesses em causa. Será mais

conveniente não restringir indevidamente a interpretação da definição de dados pessoais, mas notar que existe considerável flexibilidade na aplicação das regras aos dados.

As Autoridades Nacionais de Supervisão da Protecção de Dados desempenham um papel essencial nesta área, no âmbito da sua missão de controlo da aplicação da legislação de protecção de dados, que inclui assegurar a interpretação das disposições legais e dar orientações concretas aos responsáveis pelo tratamento e às pessoas em causa. Estas autoridades deverão defender uma definição que seja suficientemente ampla para permitir antecipar evoluções futuras e abarcar todas as “zonas cinzentas”, utilizando de forma legítima a flexibilidade prevista na Directiva. De facto, o texto da Directiva convida ao desenvolvimento de uma política que combine uma interpretação ampla da noção de dados pessoais e um equilíbrio adequado na aplicação das regras da Directiva.

III. ANÁLISE DA DEFINIÇÃO DE “DADOS PESSOAIS” DE ACORDO COM A DIRECTIVA DE PROTECÇÃO DE DADOS

A definição contida na Directiva assenta em quatro pilares que, para efeitos do presente documento, serão analisados separadamente:

- “qualquer informação”
- “relativa a”
- “identificada ou identificável”
- “pessoa singular”

Estes quatro pilares estão intimamente relacionados e apoiam-se uns nos outros. No entanto, por uma questão de metodologia, cada um será tratado separadamente.

1. PRIMEIRO ELEMENTO: “QUALQUER INFORMAÇÃO”

A expressão “qualquer informação” contida na Directiva indica claramente a intenção do legislador de prever um conceito de dados pessoais alargado. Esta redacção suscita uma interpretação ampla.

Da perspectiva da natureza da informação, o conceito de dados pessoais inclui qualquer tipo de declarações sobre uma pessoa. Abrange informação “objectiva”, tal como a presença de determinada substância no sangue dessa pessoa, mas abrange também informação, opiniões e avaliações “subjectivas”. Este último tipo de declarações constitui uma parte considerável do tratamento de dados pessoais em sectores como a banca, para avaliação da fiabilidade dos requerentes de empréstimos (“O Tito é um requerente fiável”), os seguros (“não é previsível que o Tito morra em breve”) ou o emprego (“O Tito é um bom trabalhador e merece ser promovido”).

Para que a informação seja considerada como “dados pessoais” não é necessário que seja verdadeira ou comprovada. Na verdade, as regras de protecção de dados já

contemplam a possibilidade de a informação ser incorrecta e prevêem o direito da pessoa em causa avaliar a informação e contestá-la através dos meios apropriados⁵.

Da perspectiva do conteúdo da informação, o conceito de dados pessoais inclui dados que fornecem qualquer tipo de informação. Isto abrange, como é evidente, informação pessoal que, devido à sua natureza especial de risco, é considerada como “dados sensíveis” no artigo 8.º da Directiva, mas também tipos mais gerais de informação. A expressão “dados pessoais” inclui informação que toca a esfera da vida privada e familiar da pessoa *stricto sensu*, mas inclui também informação sobre qualquer tipo de actividade realizada pela pessoa, tal como a que diz respeito às relações de trabalho ou ao seu comportamento económico e social. Inclui, assim, informação sobre pessoas singulares, independentemente do seu estatuto ou papel (consumidor, paciente, empregado, cliente, etc.).

Exemplo n.º 1: Práticas e hábitos profissionais

A informação sobre a prescrição de medicamentos (ex. número de identificação do medicamento, nome do medicamento, dose do medicamento, fabricante, preço de venda, novo ou recarga, razões de uso, razões de não autorização de substitutos, nome e apelido de quem receita, número de telefone, etc.), seja sob forma de uma receita individual ou sob forma de um tratamento que se infere de várias receitas, pode ser considerada como dados pessoais sobre o médico que receita este medicamento, mesmo que o paciente seja anónimo. Desta forma, fornecer informação sobre receitas passadas por médicos identificados ou identificáveis a fabricantes de medicamentos constitui uma comunicação de dados pessoais a terceiros na acepção da Directiva.

Esta interpretação é apoiada pela redacção da própria Directiva. Por um lado, o conceito de vida privada e familiar deve ser um conceito amplo, tal como deixou claro o Tribunal Europeu dos Direitos do Homem⁶. Por outro lado, as regras de protecção de dados pessoais ultrapassam a protecção do conceito lato de direito ao respeito pela vida privada e familiar. Convém notar que a Carta dos Direitos Fundamentais da União Europeia consagra a protecção dos dados pessoais no artigo 8.º enquanto direito autónomo, separado e diferente do direito à vida privada referido no seu artigo 7.º, o mesmo se verificando a nível nacional em alguns Estados-Membros. Isto é coerente com o n.º 1 do artigo 1.º, que visa proteger “as liberdades e os direitos fundamentais das pessoas singulares, nomeadamente [mas não exclusivamente] o direito à vida privada”. Do mesmo modo, a Directiva faz especial referência ao tratamento de dados pessoais em contextos fora do lar e da família, tais como no domínio da legislação do trabalho (alínea b) do n.º 2 do artigo 8.º), das condenações penais, sanções

⁵ A rectificação poderia ser feita através do aditamento de comentários de refutação ou utilizando os meios jurídicos adequados, tais como os mecanismos de recurso.

⁶ Acórdão do Tribunal Europeu dos Direitos do Homem no processo Amann / Suíça de 16.2.2000, parágrafo 65 : “[...]o conceito “vida privada” não deverá ser interpretado de forma restritiva. Nomeadamente, o respeito pela vida privada inclui o direito de estabelecer e desenvolver relações com outros seres humanos; para além disso, não existe nenhuma razão de princípio que justifique a exclusão de actividades de natureza profissional ou comercial do conceito de “vida privada” (ver o acórdão Niemietz / Alemanha de 16 de Dezembro de 1992, Série A, n.º 251-B, págs. 33-34, § 29, e o acórdão Halford acima referido, págs. 1015-16, § 42). Essa interpretação ampla corresponde à da Convenção de 28 de Janeiro de 1981, do Conselho da Europa [...]”

administrativas e decisões cíveis (n.º 5 do artigo 8.º), ou de *marketing* directo (alínea b) do artigo 14.º). O Tribunal de Justiça Europeu⁷ apoiou esta abordagem lata.

Do ponto de vista do formato, ou do meio, de que consta a informação, o conceito de dados pessoais inclui informação disponível em qualquer formato, alfabético, numérico, gráfico, fotográfico ou acústico, por exemplo. Inclui informação em suporte papel, bem como informação armazenada, por exemplo, na memória de um computador através do código binário ou numa vídeo cassete. Isto é uma consequência lógica de se incluir o tratamento automatizado de dados pessoais no seu âmbito. Nomeadamente, deste ponto de vista, os dados de som e imagem são considerados como dados pessoais, na medida em que possam representar informação sobre uma pessoa singular. Neste contexto, a referência específica a dados de som e imagem no artigo 33.º da Directiva deve ser entendida como uma confirmação e esclarecimento de que este tipo de dados está, de facto, abrangido pelo âmbito de aplicação da Directiva (desde que todas as outras condições estejam preenchidas), e que esta lhes é aplicável. Na realidade, trata-se de uma conclusão lógica da disposição contida neste artigo, o qual tenta avaliar se a regras da Directiva dão uma resposta jurídica adequada nestas áreas. Este aspecto é ainda esclarecido no considerando 14, que refere que “*tendo em conta a importância do desenvolvimento que, no âmbito da sociedade de informação, sofrem actualmente as técnicas de captação, transmissão, manipulação, gravação, conservação ou comunicação de dados de som e de imagem relativos às pessoas singulares, há que aplicar a presente directiva ao tratamento desses dados*”. Por outro lado, para que a informação seja considerada como dados pessoais, não é necessário que esteja incluída num ficheiro ou numa base de dados estruturada. A informação que conste de um texto livre inscrito num documento electrónico poderá também ser considerada como dados pessoais, desde que os outros critérios constantes da definição de dados pessoais estejam preenchidos. Uma mensagem de correio electrónico, por exemplo, conterà “dados pessoais”.

Exemplo n.º 2: Operações bancárias pelo telefone:

Nas operações bancárias pelo telefone, onde é gravada a voz do cliente a dar instruções ao banco, estas instruções gravadas devem ser consideradas como dados pessoais.

Exemplo n.º 3: Videovigilância

As imagens de pessoas, captadas por um sistema de videovigilância podem constituir dados pessoais desde que as pessoas sejam reconhecíveis.

Exemplo n.º 4: O desenho de uma criança

Como resultado de um teste neuropsiquiátrico feito por uma menina no contexto de um processo em tribunal relativo à sua custódia, é apresentado um desenho feito pela menina representando a sua família. O desenho fornece informação sobre o seu estado de espírito e sobre o que ela sente em relação a diferentes membros da sua família. Como tal, poderá ser considerado como “dados pessoais”. De facto, o desenho irá revelar informação sobre a criança (o seu estado de saúde do ponto de vista

⁷ Acórdão do Tribunal de Justiça Europeu C-101/2001 de 6.11.2003 (Lindqvist), §24: “*O conceito dados pessoais utilizado no n.º 1 do artigo 3º da Directiva 95/46 abrange, de acordo com a definição da alínea (a) do artigo 2º, qualquer informação relativa a uma pessoa singular identificada ou identificável. O conceito abrange claramente o nome de uma pessoa em conjunto com o seu número de telefone ou informação sobre as suas condições de trabalho ou tempos livres*”.

psiquiátrico) e também sobre, por exemplo, o comportamento do seu pai ou da sua mãe. Consequentemente, os pais neste caso poderão ter a possibilidade de exercer o seu direito de acesso a esta informação específica.

Deverá ser feita uma referência especial aos dados biométricos. Estes dados podem ser definidos como propriedades biológicas, características fisiológicas, traços físicos ou acções reproduzíveis, na medida em que essas características e/ou acções sejam simultaneamente únicas a essa pessoa e mensuráveis, mesmo que os padrões utilizados na prática para medi-las tecnicamente envolvam um certo grau de probabilidade. Exemplos típicos deste tipo de dados biométricos são as impressões digitais, os padrões da retina, a estrutura facial, a voz, mas também a geometria das mãos, os padrões das veias ou mesmo uma habilidade profundamente enraizada ou outra característica comportamental (tal como a assinatura manual, caligrafia, forma particular de andar ou falar, etc...)

Uma particularidade dos dados biométricos é que estes podem ser considerados como *conteúdo* da informação sobre uma determinada pessoa (Tito tem estas impressões digitais), bem como um elemento para estabelecer uma *ligação* entre uma informação e a pessoa (este objecto foi tocado por alguém com estas impressões digitais e estas impressões digitais correspondem ao Tito; como tal, este objecto foi tocado pelo Tito). Assim sendo, podem funcionar como “identificadores”. De facto, devido à sua ligação única com uma determinada pessoa, os dados biométricos podem ser utilizados para identificar a pessoa. Este carácter duplo também surge no caso de dados de ADN que fornecem informação sobre o corpo humano e permitem uma identificação clara e única da pessoa.

As amostras de tecidos humanos (tal como uma amostra de sangue) são fontes de que se podem extrair dados biométricos, mas não são em si dados biométricos (tal como, por exemplo, um padrão de impressões é um dado biométrico mas o próprio dedo não o é). Como tal, a extracção de informação das amostras é uma recolha de dados pessoais à qual são aplicáveis regras da Directiva. A recolha, armazenamento e utilização das próprias amostras de tecido poderão ser sujeitas a regras separadas⁸.

2. SEGUNDO ELEMENTO: “RELATIVA A”

Este elemento da definição é crucial uma vez que é muito importante identificar, com precisão, quais as relações/ligações relevantes e como distingui-las.

Em termos gerais, a informação pode considerar-se como “relativa” a uma pessoa quando é *sobre* essa pessoa.

Em muitas situações, esta relação pode ser estabelecida facilmente. Por exemplo, os dados registados no ficheiro pessoal de determinada pessoa, no Departamento de Pessoal, são claramente “relativos” à situação dessa pessoa enquanto empregado. O mesmo se passa com os dados sobre os resultados dos exames médicos de determinado doente contidos no seu registo médico ou com a imagem de uma pessoa filmada numa entrevista vídeo.

⁸ Ver Recomendação do Conselho da Europa n.º Rec (2006) 4 do Comité de Ministros dos Estados-Membros sobre investigação em materiais biológicos de origem humana, de 15.3.2006.

Existe, no entanto, toda uma série de outras situações em que, ao contrário dos exemplos anteriores, nem sempre é tão óbvio decidir se a informação é “relativa” a uma pessoa.

Em algumas situações, a informação veiculada pelos dados está relacionada primeiramente com objectos e não com pessoas. Estes objectos normalmente pertencem a alguém, ou podem ser sujeitos a uma influência particular por parte de pessoas ou exercerem nestas uma influência particular, ou podem manter algum tipo de vizinhança física ou geográfica com pessoas ou com outros objectos. Assim, só indirectamente se pode considerar que a informação diz respeito a essas pessoas ou objectos.

Exemplo n.º 5: o valor de uma casa

O valor de uma determinada casa é uma informação sobre um objecto. As regras de protecção de dados claramente não serão de aplicação quando esta informação for utilizada apenas para ilustrar o nível dos preços do imobiliário numa determinada zona. No entanto, em certas circunstâncias esta informação poderá ser também considerada como dados pessoais. De facto, a casa é um activo do seu proprietário, que servirá assim, por exemplo, para determinar o alcance da obrigação desta pessoa em pagar determinados impostos. Neste contexto, será indiscutível que esta informação deverá ser considerada como dados pessoais.

Uma análise semelhante aplica-se quando os dados são primeiramente sobre processos ou eventos, por exemplo, informação sobre o funcionamento de uma máquina quando é necessária intervenção humana. Em certas circunstâncias, esta informação pode ser também considerada como “relativa” a uma pessoa.

Exemplo n.º 6: registo de oficina de um carro

O registo de serviço de uma oficina sobre um carro, detido por um mecânico ou uma garagem, contém a informação sobre o carro, a quilometragem, as datas das revisões, os problemas técnicos e a condição do material. No registo, esta informação está associada a uma matrícula e a um número de motor, que por sua vez podem ser relacionados com o proprietário. Quando a garagem estabelece uma ligação entre o veículo e o proprietário, para fins de facturação, a informação será “relativa” ao proprietário ou ao veículo. Se a ligação for feita com o mecânico que trabalhou no carro, para fins de determinar a sua produtividade, esta informação será “relativa” também ao mecânico.

O Grupo de Trabalho também já analisou a questão de quando é que a informação pode ser considerada como “relativa” a uma pessoa. No contexto dos debates sobre questões de protecção de dados suscitadas pelos dispositivos RFID, o Grupo de Trabalho referiu que *“os dados referem-se a uma pessoa se se referirem à identidade, características ou comportamento de uma pessoa ou se tal informação for utilizada para determinar ou influenciar a forma como essa pessoa é tratada ou avaliada”*⁹.

Face aos casos acima mencionados e seguindo a mesma lógica, poderia ser assinalado que, para considerar que os dados são “relativos” a uma pessoa, um elemento de

⁹ Documento do Grupo de Trabalho, nº WP 105: “Documento de trabalho sobre questões relativas à protecção de dados no âmbito da tecnologia RFID”, adoptado em 19.1.2005, p. 8.

“**conteúdo**” OU um elemento de “**finalidade**” OU um elemento de “**resultado**” deverá estar presente.

O elemento de “**conteúdo**” está presente nos casos em que – no sentido mais óbvio e comum da expressão “relativa a” – se dá informação sobre determinada pessoa, independentemente de qualquer objectivo por parte do responsável pelo tratamento ou de um terceiro, ou do impacto dessa informação na pessoa em causa. Uma informação é “relativa” a uma pessoa quando é “sobre” essa pessoa e isto tem de ser avaliado à luz de todas as circunstâncias do caso. Por exemplo, os resultados de análises clínicas são claramente relativos ao doente e a informação contida numa pasta de uma empresa com o nome de determinado cliente é-lhe, claramente, relativa. Ou a informação contida num dispositivo RFID ou num código de barras incorporado num documento de identificação de determinada pessoa é relativa a essa pessoa, como acontecerá em futuros passaportes com um chip RFID.

O facto de a informação ser “relativa” a determinada pessoa pode derivar igualmente de um elemento de “**finalidade**”. Pode considerar-se que este elemento de “finalidade” existe quando os dados são utilizados, tendo em conta todas as circunstâncias do caso específico, com a finalidade de avaliar, tratar de determinada forma ou influenciar o estatuto ou o comportamento de uma pessoa.

Exemplo n.º 7: registo de chamadas de um telefone

O registo de chamadas de um telefone do escritório de uma empresa fornece informação sobre as chamadas que foram feitas daquele telefone que está ligado a determinada linha. Esta informação pode ser relacionada com diferentes sujeitos. Por um lado, a linha foi disponibilizada à empresa e a empresa está contratualmente obrigada a pagar essas chamadas. Durante o período de trabalho, o aparelho telefónico está sob o controlo de um determinado empregado e é ele que efectua as chamadas. O registo de chamadas pode também fornecer informação sobre a pessoa a quem se telefonou. O telefone pode ainda ser utilizado por qualquer pessoa a quem seja permitida a entrada na ausência do empregado (por exemplo, o pessoal de limpeza). Com diferentes finalidades, a informação sobre o uso deste aparelho telefónico pode ser relativa à empresa, ao empregado ou ao pessoal de limpeza (por exemplo, para verificar a hora de saída do pessoal de limpeza, uma vez que é suposto que confirmem por telefone a hora a que vão sair antes de trancarem as instalações). É de referir que o conceito de dados pessoais abrange neste caso tanto as chamadas recebidas como as efectuadas, na medida em que todas elas contêm informação que diz respeito à vida privada, relações pessoais e comunicações de pessoas.

Um terceiro tipo de “relativa a” pessoas específicas surge quando está presente um elemento de “**resultado**”. Apesar da ausência de um elemento de “conteúdo” ou de “finalidade”, os dados podem ser considerados como “relativos” a uma pessoa porque é provável que o seu uso tenha um impacto nos direitos e interesses dessa determinada pessoa, tendo em consideração todas as circunstâncias do caso específico. É de notar que não é necessário que o resultado potencial tenha um grande impacto. É suficiente que a pessoa possa ser tratada de forma diferente de outras pessoas como resultado do tratamento desses dados.

Exemplo n.º 8: controlo do posicionamento dos táxis para optimizar o serviço, com impacto nos motoristas.

Um sistema de localização por satélite é instalado por uma empresa de táxis e torna possível determinar em tempo real a posição dos táxis disponíveis. A finalidade do tratamento é fornecer um melhor serviço e poupar combustível, atribuindo a cada cliente que peça um táxi, o carro que estiver mais próximo do endereço do cliente. Em sentido estrito, os dados necessários para este sistema são dados relativos aos carros e não aos motoristas. A finalidade do tratamento não é avaliar o desempenho dos motoristas através da optimização dos seus itinerários. No entanto, o sistema permite controlar o desempenho dos motoristas e verificar se respeitam os limites de velocidade, se procuram itinerários adequados, se estão ao volante ou fora do veículo a descansar, etc. Pode assim ter um impacto considerável nestas pessoas, e como tal os dados podem ser considerados como relativos também a pessoas singulares. O tratamento deverá ser sujeito a regras de protecção de dados.

Estes três elementos (conteúdo, finalidade, resultado) devem ser considerados como condições alternativas e não cumulativas. Nomeadamente, quando está presente o elemento de conteúdo, não é necessário que os outros elementos estejam presentes para se considerar que a informação é relativa à pessoa. Um corolário disto é que a mesma informação pode ser simultaneamente relativa a várias pessoas, dependendo de qual elemento está presente em relação a cada uma delas. A mesma informação pode ser relativa à pessoa Tito devido ao elemento de “conteúdo” (os dados são claramente sobre o Tito) E ao Gaio devido ao elemento “finalidade” (vão ser usados para tratar o Gaio de uma certa forma) E ao Semprónio devido ao elemento “resultado” (é provável que tenham um impacto nos direitos e interesses do Semprónio). Isto significa também que não é necessário que os dados se “concentrem” em alguém para se considerar que são relativos a essa pessoa. Consequentemente, a questão de saber se os dados são relativos a determinada pessoa é algo que tem de ser determinado individualmente para cada dado em causa. Da mesma forma, o facto de a informação pode ser relativa a diferentes pessoas deverá ser tido em consideração na aplicação de disposições materiais (ex: o âmbito do direito de acesso).

Exemplo n.º 9: informação contida na acta de uma reunião.

Um exemplo da necessidade de se realizar individualmente, para cada informação, a análise anterior, é o da informação contida na acta de uma reunião, que regista normalmente a presença dos participantes Tito, Gaio e Semprónio; as declarações feitas por Tito e Gaio; e um relato da sessão sobre determinados tópicos tal como sintetizado pelo autor da acta, o Semprónio. Como dados pessoais relativos ao Tito, só se pode considerar a informação de que esteve presente na reunião, em determinado local e hora, e que fez determinadas declarações. A presença na reunião do Gaio, as suas declarações e o relato da sessão sobre determinado assunto tal como sintetizado pelo Semprónio, NÃO são dados pessoais relativos ao Tito. Isto verifica-se, mesmo que esta informação esteja contida no mesmo documento e mesmo que tenha sido o Tito a lançar o assunto discutido na reunião. Portanto, é algo que está excluído do direito de acesso do Tito aos seus próprios dados pessoais. Saber se, e em que medida, esta informação pode ser considerada como dados pessoais do Gaio e do Semprónio, terá de ser determinado separadamente, utilizando a análise descrita anteriormente.

3. TERCEIRO ELEMENTO: “IDENTIFICADA OU IDENTIFICÁVEL” [PESSOA SINGULAR]

A Directiva exige que a informação seja relativa a uma pessoa singular “identificada ou identificável”. Tal facto suscita as seguintes considerações:

Em termos gerais, uma pessoa singular pode ser considerada “identificada” quando, de entre um grupo de pessoas, ele ou ela é “distinguido” de todos os outros membros do grupo. Da mesma forma, uma pessoa singular é “identificável” quando, apesar da pessoa ainda não ter sido identificada, é possível fazê-lo (é o sentido do sufixo “-vel”). Esta segunda alternativa constitui assim, na prática, o limiar que determina se a informação recai no âmbito do terceiro elemento.

A identificação é normalmente obtida através de informações especiais que poderemos designar por “identificadores” e que têm uma relação especialmente privilegiada e próxima com a pessoa em causa. A título de exemplo, podemos referir os sinais exteriores relativos ao aspecto da pessoa tais como a altura, cor do cabelo, vestuário, etc. ou uma característica da pessoa que não pode ser vista de forma imediata tal como a profissão, a função, o nome, etc. A Directiva menciona esses “identificadores” na definição de “dados pessoais” no artigo 2.º quando declara que uma pessoa singular é todo aquele que “*possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social*”.

"Directamente" ou "indirectamente" identificável

Esclarecimentos suplementares constam dos comentários aos artigos da proposta alterada da Comissão, no sentido em que “*uma pessoa pode ser identificada directamente pelo nome ou indirectamente por um número de telefone, uma matrícula, um número de segurança social, um número de passaporte ou por uma combinação de critérios significativos que permitem o reconhecimento da pessoa por eliminação dos elementos do grupo a que ela pertence (idade, profissão, local de residência, etc.)*”. Os termos desta declaração indicam claramente que a medida em que determinados identificadores são suficientes para obter a identificação é algo que depende do contexto da situação em causa. Um apelido muito comum não será suficiente para identificar alguém – isto é, para a distinguir – de toda a população de um país, enquanto é provável que permita a identificação de um aluno numa sala de aula. Até informação acessória, tal como “o homem com um fato preto” pode identificar alguém de entre um grupo de transeuntes parados junto a um semáforo. Assim, a questão de saber se a pessoa a que a informação é relativa, está identificada ou não, depende das circunstâncias do caso.

Relativamente às pessoas “directamente” identificadas ou identificáveis, o **nome** da pessoa é, de facto, o identificador mais comum e, na prática, a noção de “pessoa identificada” implica na maioria das vezes a referência ao seu nome.

De forma a determinar esta identidade, o nome da pessoa por vezes tem de ser combinado com outras informações (data de nascimento, nome dos pais, endereço ou uma fotografia) para evitar confusão entre essa pessoa e possíveis homónimos. Por exemplo, a informação de que um determinado montante é devido pelo Tito pode ser considerada como relativa a uma pessoa identificada porque está ligada ao nome da pessoa. O nome é uma informação que revela que o indivíduo utiliza aquela

combinação de letras e sons para se distinguir e para que os outros com quem se relaciona o distingam. O nome pode também ser o ponto de partida para determinar o domicílio ou o paradeiro de uma pessoa, podendo ainda dar informação sobre as pessoas da sua família (através do apelido) e toda uma série de diferentes relações jurídicas e sociais associadas a esse nome (registos escolares, registos médicos, contas bancárias). Poderá inclusivamente ser possível conhecer o aspecto físico da pessoa se a sua fotografia estiver associada a esse nome. Todas estas novas informações ligadas ao nome podem permitir a alguém destacar de um grupo a pessoa específica e, desta forma, através dos identificadores a informação original é associada a uma pessoa singular, a qual pode ser distinguida de outras pessoas.

Relativamente às pessoas identificadas ou identificáveis “indirectamente”, esta categoria diz respeito tipicamente ao fenómeno das “combinações únicas”, sejam estas de grande ou pequena dimensão. Nos casos em que, *prima facie*, o alcance dos identificadores disponíveis não permite a ninguém isolar uma determinada pessoa, essa pessoa poderá ainda assim ser “identificável” porque essa informação combinada com outras informações (independentemente destas últimas estarem ou não à disposição do responsável pelo tratamento) permitirá distinguir a pessoa. É por isso que a Directiva refere “um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social”. Algumas características são tão únicas que determinada pessoa pode ser identificada sem qualquer esforço (“o actual Primeiro Ministro de Espanha”), mas uma combinação de pormenores de diferentes categorias (grupo etário, origem geográfica, etc.) pode ser igualmente muito conclusiva em algumas circunstâncias, sobretudo se se tem acesso a certas informações adicionais. Este fenómeno foi exaustivamente estudado por peritos de estatística, sempre interessados em evitar uma quebra da confidencialidade.

Exemplo n.º 10: informação fragmentada na imprensa

É publicada informação na imprensa sobre um antigo crime que, no passado, suscitou grande interesse por parte do público. Da presente publicação não constam nenhuns dos identificadores tradicionais apresentados, não há nome nem data de nascimento de nenhuma das pessoas envolvidas.

Não será extraordinariamente difícil obter informação adicional que permita descobrir quem são os principais envolvidas, por exemplo, consultando jornais do período em causa. De facto, pode presumir-se que não é completamente improvável que alguém tome essas medidas (consultando antigos jornais) que, muito provavelmente, forneceriam nomes e outros identificadores para as pessoas referidas no exemplo. Parece assim justificado que se considere a informação referida no exemplo como sendo “informação sobre pessoas identificáveis” e, como tal, “dados pessoais”.

Neste ponto, deverá notar-se que, enquanto a identificação a partir do nome é o caso mais comum na prática, um nome pode não ser necessário em todos os casos para identificar uma pessoa. Isto poderá acontecer quando são utilizados outros “identificadores” para distinguir alguém. De facto, ficheiros informáticos que registam dados pessoais atribuem normalmente um identificador único às pessoas registadas para evitar confusão entre duas pessoas no mesmo ficheiro. Igualmente, na Internet, as ferramentas de supervisão do tráfego tornam mais fácil identificar o comportamento de uma máquina e, por detrás da máquina, do seu utilizador. Desta forma, a personalidade da pessoa é “construída” de forma a atribuir-lhe determinadas decisões. Sem sequer indagar sobre o nome e endereço da pessoa é possível categorizá-la com base em

critérios socioeconómicos, psicológicos, filosóficos ou outros e atribuir-lhe determinadas decisões, uma vez que o ponto de contacto da pessoa (um computador) já não requer a apresentação da sua identidade em sentido estrito. Por outras palavras, a possibilidade de identificar uma pessoa já não implica necessariamente a capacidade para descobrir o seu nome. A definição de dados pessoais reflecte este facto¹⁰.

O Tribunal de Justiça Europeu pronunciou-se neste sentido quando considerou que “*a referência a várias pessoas, numa página da Internet e a sua identificação pelo nome ou por outros meios, designadamente a indicação do número de telefone ou de informação relativa às suas condições de trabalho e tempos livres, constitui tratamento de dados pessoais [...] no sentido [...] da Directiva 95/46/CE*”¹¹.

Exemplo n.º 11: requerentes de asilo

Nas instituições de acolhimento, foram atribuídos códigos numéricos para fins administrativos aos requerentes de asilo que escondem os seus nomes verdadeiros. Este número servirá de identificador para que sejam atribuídas ao requerente de asilo diferentes informações relativas à sua estadia na instituição e, através de uma fotografia ou outro indicador biométrico, o código numérico terá uma ligação estreita e imediata com a pessoa física, permitindo-lhe desta forma ser distinguida dos outros requerentes de asilo e serem-lhe atribuídas diferentes informações que se referirão então a uma pessoa singular “identificada”.

O n.º 7 do artigo 8.º também estabelece que “Cabe aos Estados-Membros determinar as condições em que um número nacional de identificação ou qualquer outro elemento de identificação de aplicação geral poderá ser objecto de tratamento”. Vale a pena notar o sentido desta disposição, que não dá qualquer indicação sobre o tipo de condições que os Estados-Membros devem adoptar, mas que, no entanto, se encontra integrada no artigo relativo aos que trata de dados sensíveis. O considerando 33 refere este tipo de dados como “*dados susceptíveis, pela sua natureza, de pôr em causa as liberdades fundamentais ou o direito à vida privada*”. É razoável pensar que o legislador possa ter tido uma preocupação semelhante relativamente a números de identificação nacionais dado o seu forte potencial para ligar de forma fácil e inequívoca diferentes informações sobre determinada pessoa.

Meios para identificar

O considerando 26 da Directiva atribui especial atenção à palavra “identificável” ao dizer “*que, para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa*”. Isto significa que uma mera possibilidade hipotética de distinguir o indivíduo não é suficiente para considerar a pessoa “identificável”. Se, tendo em consideração “*o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa*”, essa possibilidade não existir ou for negligenciável, a pessoa não deverá ser considerada “identificável” e a informação não será considerada como “dados pessoais”. O critério de “*o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento,*

¹⁰ Relatório sobre a aplicação dos princípios da protecção de dados às redes de telecomunicações mundiais, de Yves POULLET e sua equipa, para a Comissão T-PD do Conselho da Europa, ponto 2.3.1, T-PD (2004) 04 final.

¹¹ Acórdão do Tribunal de Justiça Europeu C-101/2001 de 6.11.2003 (Lindqvist), ponto 27.

seja por qualquer outra pessoa” deverá nomeadamente ter em consideração todos os factores em causa. O custo de proceder à identificação é um factor, mas não o único. O objectivo pretendido, a forma como o tratamento está estruturado, a vantagem esperada pelo responsável pelo tratamento, os interesses em causa para as pessoas, bem como o risco de disfunções organizacionais (ex: quebra do dever de confidencialidade) e falhas técnicas, deverão todos ser tidos em consideração. Por outro lado, trata-se de um critério dinâmico que deverá ter em consideração o estado de desenvolvimento da tecnologia no momento do tratamento e as possibilidades de evolução durante o período para o qual os dados serão tratados. A identificação poderá não ser possível hoje com o conjunto dos meios susceptíveis de serem razoavelmente utilizados hoje. Se os dados são para armazenar durante um mês, pode não se prever a possibilidade de identificação durante o período de “vida” da informação e não deverão ser considerados como dados pessoais. No entanto, se o armazenamento está previsto por 10 anos, o responsável pelo tratamento deverá considerar a possibilidade de identificação que pode surgir no nono ano de vida dos dados e que, nessa altura, os poderá tornar dados pessoais. O sistema deverá ter a capacidade de se adaptar a estas evoluções à medida que elas ocorrem, permitindo incorporar, em tempo útil, as medidas técnicas e organizacionais que se imponham.

Exemplo n.º 12: Publicação de radiografias juntamente com o nome próprio do doente

Foi publicada numa revista científica uma radiografia de uma senhora, juntamente com o seu nome próprio que era muito fora do comum. O nome próprio da pessoa, combinado com o conhecimento por parte dos seus familiares ou conhecidos de que ela sofria de certa doença, tornaram a pessoa identificável por um grupo de pessoas. Desta forma, a radiografia será considerada como um dado pessoal.

Exemplo n.º 13: Dados de investigação farmacêutica

Determinados hospitais ou médicos transferem dados de registos médicos dos seus doentes para uma empresa para fins de investigação médica. Não são utilizados os nomes dos doentes, apenas os números de série, atribuídos aleatoriamente a cada caso clínico, de forma a assegurar a coerência e evitar confusão entre a informação sobre diferentes doentes. Os nomes dos doentes mantêm-se exclusivamente na posse dos respectivos médicos vinculados pelo sigilo profissional. Os dados não contêm qualquer informação adicional que possa tornar a identificação dos doentes possível por combinação. Adicionalmente, foram tomadas todas as medidas, sejam elas jurídicas, técnicas ou organizacionais, para evitar que as pessoas em causa sejam identificadas ou se tornem identificáveis. Nestas circunstâncias, uma Autoridade de Protecção de Dados poderá considerar que, no tratamento efectuado pela empresa farmacêutica, não existem meios susceptíveis de serem razoavelmente utilizados para identificar as pessoas em causa.

Outro factor relevante, já referido, para avaliar “*o conjunto dos meios susceptíveis de serem razoavelmente utilizados*” para identificar as pessoas, será de facto a finalidade pretendida pelo responsável durante o tratamento dos dados. As Autoridades Nacionais de Protecção de Dados já se viram confrontadas com casos em que, por um lado, o responsável pelo tratamento invoca que só são tratadas informações dispersas, sem referência a nomes ou qualquer outro identificador directo, e defende que os dados não devem ser considerados como dados pessoais e não devem estar sujeitos às regras de protecção de dados. Por outro lado, o tratamento da informação só faz sentido se permitir a identificação de pessoas específicas e o seu tratamento de determinada forma. Nestes casos, em que a finalidade do tratamento implica a identificação das pessoas, pode

presumir-se que o responsável pelo tratamento ou qualquer outra pessoa envolvida tem ou terá os meios “susceptíveis de serem razoavelmente utilizados” para identificar a pessoa em causa. De facto, invocar que as pessoas não são identificáveis quando o objectivo do tratamento é precisamente o de as identificar, seria uma clara contradição. Como tal, a informação deve ser considerada como relativa a pessoas identificáveis e o tratamento deve estar sujeito às regras de protecção de dados.

Exemplo n.º 14: Videovigilância

Isto é especialmente relevante no contexto da videovigilância, em que os responsáveis pelo tratamento frequentemente invocam que a identificação só aconteceria numa pequena percentagem do material recolhido e, como tal, antes da identificação ser efectivamente realizada nestes poucos casos, não há lugar a tratamento de dados pessoais. No entanto, uma vez que o objectivo da videovigilância é identificar as pessoas que surgem nas imagens vídeo em todos os casos em que essa identificação é considerada necessária pelo responsável pelo tratamento, toda a operação enquanto tal deve ser considerada um tratamento de dados sobre pessoas identificáveis, mesmo se, na prática, algumas pessoas filmadas não são identificáveis.

Exemplo n.º 15: endereços IP dinâmicos

O Grupo de Trabalho considerou os endereços IP como dados relativos a uma pessoa identificável e declarou que *“os fornecedores de serviço de Internet e os administradores de redes locais podem, utilizando meios razoáveis, identificar os utilizadores de Internet a quem tenham atribuído endereços IP visto que, por norma, registam sistematicamente num ficheiro a data, hora, duração e endereço IP dinâmico atribuído ao utilizador. O mesmo acontece com os fornecedores de serviço de Internet que mantêm um registo no servidor http. Nestes casos, não há dúvida de que se trata de dados pessoais na acepção da alínea a) do artigo 2º da Directiva ...”*¹².

Especialmente nos casos em que o tratamento dos endereços IP é realizado com o objectivo de identificar os utilizadores do computador (por exemplo, pelos detentores de direitos de autor com o objectivo de levar a tribunal os utilizadores de computadores por violação dos direitos de propriedade intelectual), o responsável pelo tratamento prevê que os “meios susceptíveis de serem razoavelmente utilizados” para identificar as pessoas estarão disponíveis, por exemplo, através dos tribunais a que se recorreu (caso contrário a recolha dos dados não faz sentido), e, como tal, a informação deverá ser considerada como dados pessoais.

Um caso particular seria o de alguns tipos de endereços IP que, em determinadas circunstâncias, não permitem de facto a identificação do utilizador, por diversas razões técnicas e organizacionais. Um exemplo poderia ser o endereço IP atribuído a um computador num cibercafé, onde não é exigida a identificação dos clientes. Poderá alegar-se que os dados recolhidos sobre a utilização do computador X durante um certo período de tempo não permitem a identificação do utilizador através de meios razoáveis, e, como tal, não são dados pessoais. No entanto, é de notar que os Fornecedores de Serviço de Internet provavelmente não saberão se o endereço IP em causa permite a identificação ou não, e que irão tratar os dados associados a esse IP da mesma forma que tratam a informação associada a endereços IP de utilizadores que

¹² WT 37: “Privacidade na Internet – Uma abordagem integrada comunitária à protecção de dados on-line”, adoptado em 21.11.2000

estão devidamente registados e são identificáveis. Assim, a menos que o Fornecedor de Serviço esteja em posição de distinguir com certeza absoluta que os dados correspondem a utilizadores que não podem ser identificados, terá de tratar toda a informação IP como dados pessoais, por uma questão de precaução.

Exemplo n.º 16: danos causados por graffiti

Uma empresa de transportes vê os seus veículos de passageiros serem repetidamente vandalizados com graffiti. Para poder avaliar os estragos e para facilitar o pedido de indemnização aos autores, a empresa organiza um registo contendo informação sobre as circunstâncias dos danos, bem como imagens dos bens danificados e das “marcas” ou “assinatura” do autor. No momento de introduzir a informação no registo, os autores dos danos não são conhecidos nem se sabe a quem pertence a “assinatura”. Pode mesmo acontecer que nunca se venha a saber. No entanto, o objectivo do tratamento é precisamente identificar as pessoas a que a informação diz respeito como autores dos danos, de forma a poder interpor um processo de indemnização contra elas. Este tipo de tratamento faz sentido se o responsável pelo tratamento considerar como “razoavelmente susceptível” que um dia existam os meios para identificar a pessoa. A informação contida nas fotografias deverá ser considerada como relativa a pessoas “identificáveis”, a informação do registo como “dados pessoais” e o tratamento deverá estar sujeito às regras de protecção de dados, as quais, em determinadas circunstâncias e com determinadas salvaguardas, permitem e consideram legítimo este tipo de tratamento.

Quando a identificação da pessoa em causa não está incluída na finalidade do tratamento, as medidas técnicas para impedir a identificação desempenham um papel muito importante. Organizar as medidas técnicas e organizacionais mais actualizadas e apropriadas para proteger os dados contra a identificação poderá ser determinante para se considerar que as pessoas não são identificáveis, tendo presente *o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa* para identificar as pessoas. Neste caso, a execução destas medidas não é a *consequência* de uma obrigação jurídica decorrente do artigo 17.º da Directiva (que só é aplicável se, à partida, a informação constituir dados pessoais), mas sim uma *condição* para que a informação precisamente não seja considerada como dados pessoais e para que o seu tratamento não seja abrangido pela Directiva.

Dados sob pseudónimo

Criar pseudónimos é um processo de camuflar identidades. O objectivo deste tipo de processo é permitir recolher dados adicionais relativos à mesma pessoa sem necessitar de conhecer a sua identidade. Isto é de particular importância no contexto da investigação e da estatística.

A criação de pseudónimos pode ser realizada mantendo a possibilidade de reidentificação, utilizando listas de identidades e os seus respectivos pseudónimos ou utilizando algoritmos de criptografia de duplo sentido. A camuflagem das identidades também pode ser feita de forma a tornar impossível a reidentificação, por exemplo, através da criptografia de sentido único que, em geral, cria dados anónimos.

A eficácia do processo de criação de pseudónimos depende de vários factores (a fase em que é utilizado, o grau de segurança contra a possibilidade de reidentificação, a dimensão

da população em que se esconde a pessoa, a capacidade de ligar transacções ou registos individuais à mesma pessoa, etc.). Os pseudónimos deverão ser aleatórios e imprevisíveis. O número de pseudónimos possíveis deverá ser tão grande que o mesmo pseudónimo nunca seja aleatoriamente escolhido duas vezes. Se for necessário um alto nível de segurança, o conjunto de pseudónimos potenciais deverá ser pelo menos igual à gama de valores de funções criptográficas numéricas seguras¹³.

Os dados sob pseudónimo reidentificáveis podem ser considerados como informação sobre pessoas que são *indirectamente identificáveis*. De facto, utilizar um pseudónimo significa que é possível remontar até à pessoa, de modo que a identidade da pessoa pode ser descoberta, mas isto apenas em circunstâncias pré-definidas. Nesse caso, apesar de se aplicarem as regras de protecção de dados, os riscos existentes para as pessoas no que toca ao tratamento dessa informação indirectamente identificável serão na maioria dos casos reduzidos, de forma que a aplicação destas regras será justificadamente mais flexível do que informação tratada sobre pessoas directamente identificáveis.

Dados codificados com chave

Dados codificados com chave são um exemplo clássico da criação de pseudónimos. A informação é relativa a pessoas que são individualizadas com um código, enquanto a chave que estabelece a correspondência entre o código e os identificadores comuns das pessoas (como o nome, data de nascimento, endereço) é mantida em separado.

Exemplo n.º 17: dados não agregados para estatísticas

Um exemplo para ilustrar a importância de se ponderar todas as circunstâncias para avaliar se os meios de identificação são “razoavelmente susceptíveis” de ser utilizados, poderá ser o da informação pessoal tratada pelo instituto nacional de estatística, onde, em determinada fase, a informação é mantida no formato não agregado e diz respeito a pessoas específicas, mas estas são designadas por um código em vez de um nome (ex: o código individual X1234 bebe um copo de vinho mais de 3 vezes por semana). O instituto de estatística mantém em separado a chave para estes códigos (a lista que associa os códigos aos nomes das pessoas). Esta chave pode ser considerada como “susceptível de ser razoavelmente utilizada” pelo instituto de estatística e, como tal, o conjunto de informação relativa a pessoas pode ser considerada como dados pessoais e deverá estar sujeita às regras de protecção de dados pelo instituto. Agora, podemos imaginar que uma lista com dados sobre os hábitos de consumo de bebidas dos consumidores é transferida para o organismo nacional dos produtores de vinho para lhes permitir fundamentar as suas posições públicas em dados estatísticos. Para determinar se essa lista de informação ainda constitui dados pessoais deverá avaliar-se se os consumidores de vinho podem ser identificados individualmente, tendo em consideração “*o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa*”.

Se os códigos utilizados são únicos para cada pessoa específica, o risco de identificação ocorre sempre que é possível ter acesso à chave utilizada para a codificação. Portanto, os riscos de pirataria externa, a probabilidade de alguém do seio da organização do remetente – não obstante o seu dever de segredo profissional –

¹³ Ver o Documento de Trabalho “Tecnologias de protecção da privacidade” do Grupo de Trabalho sobre tecnologias de protecção da privacidade da Comissão sobre aspectos técnicos e organizacionais da protecção de dados do Commissariado federal e estatal para a protecção de dados da Alemanha (Outubro 1997), publicado em http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm

disponibilizar a chave e a exequibilidade de identificação indirecta, são factores que têm de ser tidos em consideração para determinar se as pessoas podem ser identificadas considerando *o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa*, e, como tal, se a informação deverá ser considerada como “dados pessoais”. Em caso afirmativo, as regras de protecção de dados serão aplicáveis. Uma questão diferente é se essas regras de protecção de dados poderão ter em consideração o facto de os riscos para as pessoas serem reduzidos e tornarem o tratamento sujeito a condições mais ou menos rigorosas, com base na flexibilidade permitida pelas regras da Directiva.

Se, pelo contrário, os códigos não são únicos mas o mesmo número de código (ex: “123”) é utilizado para designar pessoas em cidades diferentes e para dados de anos diferentes (fazendo a distinção de uma pessoa específica apenas para determinado ano e para a amostra relativa à mesma cidade), o responsável pelo tratamento ou um terceiro só poderá identificar uma pessoa específica se souber a que ano e a que cidade se referem os dados. Se esta informação adicional desapareceu, e não é susceptível de ser razoavelmente recuperada, poderá considerar-se que a informação não se refere a pessoas identificáveis e não esta sujeita às regras de protecção de dados.

Este tipo de dados é habitualmente utilizado em ensaios clínicos com medicamentos. A Directiva 2001/20, de 4 de Abril de 2001, relativa à aplicação de boas práticas clínicas e à condução dos ensaios clínicos¹⁴ define um enquadramento jurídico para a condução destas actividades. O profissional/investigador médico (“investigador”) que testa os medicamentos recolhe a informação sobre os resultados clínicos em cada doente, individualizando-o com um código. O investigador disponibiliza a informação à empresa farmacêutica ou a outras partes envolvidas (“patrocinadores”) apenas no formato codificado, uma vez que estas só estão interessadas na informação bio-estatística. No entanto, o investigador mantém em separado uma chave que associa o código à informação comum para identificar os doentes individualmente. O investigador é obrigado a manter esta chave para proteger a saúde dos doentes no caso de os medicamentos virem a apresentar riscos e para que, em caso de necessidade, os doentes possam ser identificados e possam receber tratamento adequado.

A questão aqui consiste em saber se os dados utilizados para os ensaios clínicos podem ser considerados como relativos a pessoas singulares “identificáveis” e, assim, estarem sujeitos às regras de protecção de dados. De acordo com a análise descrita anteriormente, para determinar se uma pessoa é identificável *importa considerar o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa*. Neste caso, a identificação das pessoas (para aplicação do tratamento adequado em caso de necessidade) é um dos objectivos do tratamento dos dados codificados com chave. A empresa farmacêutica estruturou os meios para o tratamento, incluindo as medidas organizacionais e a sua relação com o investigador que detém a chave de tal forma que a identificação das pessoas não é apenas uma coisa que *pode* acontecer mas sim uma coisa que *deve* acontecer em determinadas circunstâncias. A identificação dos pacientes está assim imbuída na finalidade e nos meios do tratamento. Neste caso, pode concluir-se que este tipo de dados codificados com chave constituem informação relativa a pessoas singulares identificáveis para todas as partes que podem estar envolvidas na possível identificação e deverão estar sujeitos às regras da legislação sobre protecção de dados. Isto não significa, no entanto, que qualquer

¹⁴ JO L 121 de 1.5.2001, p. 34.

outro responsável pelo tratamento que trate o mesmo grupo de dados codificados esteja a tratar dados pessoais se, no regime específico em que esses outros responsáveis pelo tratamento estão a operar, a reidentificação está explicitamente excluída e tiverem sido tomadas neste sentido as medidas técnicas apropriadas.

Em outras áreas da investigação ou do mesmo projecto, a reidentificação da pessoa em causa pode ter sido excluída na concepção dos protocolos e procedimentos, por exemplo devido a não existirem aspectos terapêuticos envolvidos. Por razões técnicas ou outras, poderá ainda existir uma forma de descobrir a que pessoas correspondem que dados clínicos, mas não é suposto ou esperado que se venha a realizar a identificação em circunstância alguma e as medidas técnicas apropriadas (ex: *hashing* criptográfico irreversível) foram instituídas para evitar que isso aconteça. Neste caso, mesmo que ocorra a identificação de algumas das pessoas em causa apesar de todos os protocolos e medidas (devido a circunstâncias imprevisíveis tais como a combinação accidental de características da pessoa em causa que revelem a sua identidade), a informação tratada pelo responsável original pelo tratamento pode não ser considerada como relativa a pessoas identificadas ou identificáveis tendo em consideração *o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa*. O seu tratamento pode assim não estar sujeito às disposições da Directiva. Uma questão diferente é a que se prende com o novo responsável pelo tratamento que obteve um acesso efectivo à informação identificável, e que deve claramente ser considerada como “dados pessoais”.

Pergunta frequente (FAQ) 14-7 do Regime de “Porto Seguro”

A questão dos dados codificados com chave na investigação farmacêutica foi tratada no âmbito do Regime de “Porto Seguro”¹⁵. A pergunta frequente (FAQ) 14-7 diz o seguinte:

FAQ 14 – Produtos farmacêuticos e medicinais

7. P: Invariavelmente, os dados da investigação são codificados, na sua origem, com uma chave única pelo investigador principal, de modo a não revelar a identidade das pessoas em causa. As empresas farmacêuticas que patrocinam essa investigação não recebem a chave. O código original é conhecido apenas pelo investigador, pelo que apenas este pode identificar a pessoa em causa em circunstâncias especiais (por exemplo, quando é necessário um acompanhamento médico). Uma transferência de dados codificados desta forma, da UE para os EUA, constitui um caso de transferência de dados pessoais sujeita aos princípios de "porto seguro"?

7. R: Não, não se trata de uma transferência de dados pessoais sujeita aos referidos princípios.

O Grupo de Trabalho considera que esta declaração no Regime de “Porto Seguro” não está em contradição com o raciocínio acima apresentado de se considerar esse tipo de informação como dados pessoais sujeitos à Directiva. Na verdade, esta Pergunta Frequente não é suficientemente precisa uma vez que não refere para quem e em que condições os dados são transferidos. O Grupo de Trabalho entende que a pergunta se refere ao caso em que os dados codificados com chave são enviados a um destinatário

¹⁵ Decisão 2000/520/CE da Comissão de 26.7.2000 – JO L 215 de 25.8.2000, p. 7.

nos EUA (por exemplo, uma empresa farmacêutica), que recebe apenas dados codificados com chave e nunca estará ao corrente da identidade dos doentes, a qual, no caso de necessidade de tratamento, é conhecida e será conhecida apenas do médico/investigador na UE mas nunca da empresa nos EUA.

Dados anónimos

“Dados anónimos”, na acepção da Directiva, podem ser definidos como toda a informação relativa a uma pessoa singular quando a pessoa não pode ser identificada, seja pelo responsável pelo tratamento seja por qualquer outra pessoa, considerando *o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa* para identificar aquela pessoa. “Dados tornados anónimos” seriam então dados anónimos que anteriormente diziam respeito a uma pessoa identificada mas em que essa identificação deixou de ser possível. O considerando 26 também faz referência a este conceito quando diz que “*os princípios da protecção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável*”. Mais uma vez, a avaliação se os dados permitem a identificação de uma pessoa e se a informação pode ser considerada ou não como anónima depende das circunstâncias e deverá ser realizada uma análise caso a caso, sobretudo no que diz respeito à medida em que os meios são susceptíveis de serem razoavelmente utilizados para identificação tal como descrito no considerando 26. Isto é especialmente importante no caso de informação estatística, onde apesar da informação poder ser apresentada como dados agregados, a amostra original não é suficientemente grande e outras informações poderão permitir a identificação de pessoas.

Exemplo n.º 18: Inquéritos estatísticos e combinação de informação dispersa

Para além da obrigação geral de respeitarem as regras de protecção de dados, por forma a assegurar o carácter anónimo dos inquéritos estatísticos, os responsáveis pelas estatísticas estão sujeitos a um dever específico de segredo profissional e ao abrigo dessas regras é-lhes proibido publicar dados que não sejam anónimos. Isto obriga-os a publicarem dados estatísticos agregados que simplesmente não podem ser atribuídos a uma pessoa identificada que faça parte dessas estatísticas. Esta regra é especialmente importante no âmbito da publicação de dados de censo. Em cada situação deverá ser determinado um limiar abaixo do qual é considerado possível identificar as pessoas em causa. Se surgir um critério que parece levar à identificação em determinada categoria de pessoas, por maior que seja (ex: apenas um médico opera numa cidade de 6000 habitantes), este critério “discriminatório” deverá ser pura e simplesmente retirado ou acrescentados outros critérios para “diluir” os resultados sobre determinada pessoa e permitir a confidencialidade das estatísticas.

Exemplo n.º 19: Publicação de videovigilância

O dono de uma loja instala um sistema de videovigilância com câmaras. Na loja publica as fotos de ladrões que foram apanhados graças ao sistema de videovigilância. Após intervenção policial, apaga os rostos dos ladrões, escurecendo-os. No entanto, mesmo após esta operação, ainda existe a possibilidade de as pessoas nas fotos poderem vir a ser reconhecidas pelos amigos, parentes ou vizinhos, porque, por exemplo, a sua constituição, penteado e roupa ainda são reconhecíveis.

4. QUARTO ELEMENTO: “PESSOA SINGULAR”

A protecção oferecida pelas regras da Directiva aplica-se a pessoas singulares, isto é, a seres humanos. O direito à protecção dos dados pessoais é, neste sentido, universal, não se restringindo a nacionais ou residentes de um determinado país. O considerando 2 da Directiva indica-o expressamente ao referir que “os sistemas de tratamento de dados estão ao serviço do Homem” e que eles “devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência.”

O conceito de pessoa singular é referido no artigo 6.º da Declaração Universal dos Direitos do Homem, segundo a qual “Todas as pessoas têm o direito a serem reconhecidas como sujeitos perante a Lei”. A legislação dos Estados-Membros, normalmente na área do Direito Civil, sublinha de forma mais precisa o conceito de personalidade dos seres humanos, entendida como a capacidade de ser sujeito de relações jurídicas, desde o momento do nascimento da pessoa até à sua morte. Os dados pessoais são assim, em princípio, dados relativos a pessoas vivas identificadas ou identificáveis. Isto suscita uma série de questões no âmbito da presente análise.

Dados sobre pessoas mortas

A informação relativa a pessoas mortas, em princípio, não deverá assim ser considerada como dados pessoais sujeitos às regras da Directiva, uma vez que, efeitos do Direito Civil, os mortos já não são pessoas singulares. No entanto, em alguns casos, os dados sobre pessoas mortas poderão ainda receber protecção indirectamente.

Por um lado, o responsável pelo tratamento pode não estar em posição de determinar se a pessoa a que diz respeito a informação ainda é viva ou já está morta. Ou mesmo que o possa fazer, a informação sobre os mortos pode ser tratada ao abrigo do mesmo regime que o aplicado aos vivos, sem distinção. Uma vez que o responsável pelo tratamento está sujeito às obrigações de protecção de dados impostas pela Directiva relativamente aos dados sobre pessoas vivas, na prática, provavelmente para ele será mais fácil tratar os dados sobre os mortos da mesma forma imposta pelas regras de protecção de dados, em vez de separar os dois grupos de dados.

Por outro lado, a informação sobre pessoas mortas pode também fazer referência a pessoas vivas. Por exemplo, a informação que a falecida Gaia sofria de hemofilia indica que o seu filho Tito também sofre da mesma doença, uma vez que está ligada a um gene contido no cromossoma X. Assim, quando a informação que constitui dados sobre os mortos puder ser considerada como igualmente relativa aos vivos e constituir dados pessoais sujeitos à Directiva, os dados pessoais dos mortos podem indirectamente usufruir da protecção das regras de protecção de dados.

Em terceiro lugar, a informação sobre pessoas mortas pode ser sujeita a protecção específica atribuída por um grupo de regras para além da legislação sobre protecção de dados, delineando o que alguns designam por “*personalitas praeterita*”. A obrigação de confidencialidade do pessoal médico não termina com a morte do doente. A legislação nacional sobre o direito à honra e à imagem pode atribuir também protecção à memória dos mortos.

E, em quarto lugar, nada impede um Estado-Membro de alargar o âmbito da legislação nacional de execução das disposições da Directiva 95/46/CE a áreas não incluídas no âmbito da mesma, desde que nenhuma outra disposição de direito comunitário o impeça, como relembado pelo TJE¹⁶. É possível que um legislador nacional decida alargar as disposições da legislação nacional sobre protecção de dados a alguns aspectos relativos ao tratamento de dados de pessoas mortas, quando um interesse legítimo o justifique¹⁷.

Nascituros

A aplicação das regras de protecção de dados antes do nascimento irá depender do posicionamento geral dos sistemas jurídicos nacionais sobre a protecção dos nascituros. Pensando sobretudo nos direitos de sucessão, alguns Estados-Membros reconhecem o princípio de que crianças concebidas mas ainda não nascidas são consideradas como se tivessem nascido no que respeita aos benefícios (e assim podem receber uma herança ou aceitar uma doação), na condição de que efectivamente possam nascer. Noutros Estados-Membros, é dada protecção especial através de disposições jurídicas específicas, também sujeito à mesma condição. Para determinar se as disposições nacionais de protecção de dados protegem também informação sobre nascituros, deverá ser considerada a abordagem geral do sistema jurídico nacional, juntamente com a ideia de que o objectivo das regras de protecção de dados é proteger a pessoa.

Uma segunda questão é suscitada pelo facto de a resposta geral do sistema jurídico se basear na expectativa de que a situação dos nascituros é limitada no tempo ao período da gravidez. Não tem em consideração o facto de esta situação poder na verdade durar consideravelmente mais tempo, tal como no caso de embriões congelados. Por último, poderão encontrar-se respostas jurídicas específicas em disposições especiais sobre técnicas de reprodução, que tratem do uso de informação médica ou genética sobre embriões.

Pessoas colectivas

Uma vez que a definição de dados pessoais faz referência a pessoas, isto é, pessoas singulares, a informação relativa a pessoas colectivas em princípio não é abrangida pela Directiva e a protecção por ela atribuída não lhes é aplicável¹⁸.

No entanto, algumas regras de protecção de dados poderão ainda, em determinadas circunstâncias, aplicar-se indirectamente a informação relativa a empresas ou a pessoas colectivas.

Algumas disposições da Directiva 2002/58/CE sobre privacidade das comunicações electrónicas estendem-se às pessoas colectivas. O seu artigo 1º dispõe que “2. *Para os efeitos do n.º 1, as disposições da presente directiva especificam e complementam a Directiva 95/46/CE. Além disso, estas disposições asseguram a protecção dos*

¹⁶ Acórdão do Tribunal Europeu de Justiça C-101/2001 de 06/11/2003 (Lindqvist), § 98

¹⁷ Actas do Conselho da União Europeia, 8.2.1995, documento 4730/95: "Re artigo 2(a) "O Conselho e a Comissão confirmam que cabe aos Estados-Membros definirem se, e em que medida, se deverá aplicar a presente Directiva a pessoas mortas."

¹⁸ Considerando 24 da Directiva: "Considerando que a legislação para a protecção das pessoas colectivas relativamente ao tratamento de dados que lhes dizem respeito não é afectada pela presente directiva;"

legítimos interesses dos assinantes que são pessoas colectivas.”. Do mesmo modo, os artigos 12º e 13º estendem a aplicação de algumas disposições relativas a listas de assinantes e comunicações não solicitadas também a pessoas colectivas.

A informação sobre pessoas colectivas pode também ser considerada como “relativa a” pessoas singulares, por si só, de acordo com os critérios definidos neste documento. Poderá ser o caso quando o nome de uma pessoa colectiva derive do de uma pessoa singular. Outro caso poderá ser o do correio electrónico das empresas, o qual é normalmente utilizado por um determinado empregado, ou o da informação sobre pequenas empresas (juridicamente falando um “objecto” mais do que uma “pessoa colectiva”), a qual pode descrever o comportamento do seu proprietário. Em todos estes casos, quando o critério do “conteúdo”, da “finalidade” ou do “resultado” permitirem que a informação sobre a pessoa colectiva ou sobre a empresa seja considerada como “relativa” a uma pessoa singular, esta deverá ser considerada como dados pessoais e as regras de protecção de dados deverão aplicar-se.

O Tribunal de Justiça Europeu deixou claro que nada impede os Estados-Membros de alargarem o âmbito da legislação nacional de execução das disposições da Directiva a áreas não incluídas no âmbito da mesma, desde que nenhuma outra disposição do direito comunitário o impeça¹⁹. Consequentemente, alguns Estados-Membros, como a Itália, a Áustria ou o Luxemburgo, alargaram a aplicação de determinadas disposições da legislação nacional adoptada no seguimento da Directiva (tais como as relativas às medidas de segurança) ao tratamento de dados de pessoas colectivas.

Tal como no caso da informação sobre pessoas mortas, pode acontecer que as medidas práticas aplicadas por parte do responsável pelo tratamento possam igualmente fazer com que os dados sobre pessoas colectivas sejam sujeitos a regras de protecção de dados. Quando o responsável pelo tratamento recolhe dados sobre pessoas singulares e colectivas indistintamente e os inclui nos mesmos grupos de dados, a concepção dos mecanismos de tratamento de dados e o sistema de auditoria podem estar definidos de forma a cumprirem as regras de protecção de dados. Na realidade, poderá ser mais fácil para o responsável pelo tratamento aplicar as regras de protecção de dados a todos os tipos de informação constante dos seus ficheiros do que tentar distinguir o que se refere a pessoas singulares do que se refere a pessoas colectivas.

IV. O QUE ACONTECE QUANDO OS DADOS NÃO SÃO ABRANGIDOS PELA DEFINIÇÃO?

Como temos visto ao longo deste documento, em determinadas circunstâncias a informação pode ser considerada como não constituindo dados pessoais. Tal acontece quando os dados não podem ser considerados como relativos a uma pessoa ou porque a pessoa não pode ser considerada como identificada ou identificável. Quando a informação tratada não se enquadra no conceito de “dados pessoais”, a consequência é que a Directiva não é aplicável de acordo com o disposto no seu artigo 3.º. Isto não significa, no entanto, que as pessoas nesta situação particular fiquem desprovidas de qualquer tipo de protecção. Devemos ter em conta as seguintes considerações.

Se a Directiva não se aplica, pode acontecer que a legislação nacional de protecção de dados seja aplicável. Tal como disposto no artigo 34.º, a Directiva dirige-se aos Estados-Membros. Fora do seu âmbito, os Estados-Membros não estão sujeitos às

¹⁹ Acórdão do Tribunal Europeu de Justiça C-101/2001 de 06.11.2003 (Lindqvist), § 98

obrigações por ela impostas, basicamente executar as suas disposições através de disposições legislativas, regulamentares ou administrativas necessárias para que seja cumprida. No entanto, tal como o Tribunal de Justiça Europeu deixou claro, nada impede os Estados-Membros de alargarem o âmbito da legislação nacional de execução das disposições da Directiva a áreas não incluídas no âmbito da mesma, desde que nenhuma outra disposição do direito comunitário o impeça. Como tal, pode muito bem acontecer que determinadas situações que não envolvem o tratamento de dados pessoais na acepção da Directiva sejam sujeitas a medidas de protecção ao abrigo da legislação nacional. Isto poderá aplicar-se, por exemplo, a um tema como os dados codificados com chave, independentemente de se tratar ou não de dados pessoais.

Quando as regras de protecção de dados não se aplicam, algumas actividades podem mesmo assim interferir com o artigo 8.º da Convenção Europeia dos Direitos do Homem, o qual protege o direito à família e à vida familiar, à luz da jurisprudência muito abrangente da Convenção. Outros grupos de regras, tais como o direito penal ou a legislação antidiscriminação, podem igualmente dar protecção a pessoas nos casos em que as regras de protecção de dados não se aplicam mas estejam em causa vários interesses legítimos.

V. CONCLUSÕES

No presente parecer, o Grupo de Trabalho dá orientações sobre a forma como deverá entender-se o conceito de dados pessoais da Directiva 95/46/CE e a legislação comunitária relacionada e como este conceito deve ser aplicado em diferentes situações.

Enquanto consideração geral, foi referido que o legislador comunitário pretendeu adoptar uma noção lata de dados pessoais, mas esta noção não é ilimitada. Deverá sempre ter-se em consideração que o objectivo das regras contidas na Directiva é o de proteger os direitos e liberdades fundamentais das pessoas, nomeadamente o seu direito à vida privada, no que toca ao tratamento dos dados pessoais. Estas regras foram assim concebidas para serem aplicadas a situações em que os direitos das pessoas podem estar em risco e, como tal, podem necessitar de protecção. O âmbito das regras de protecção de dados não deverá ser inadequadamente ampliado, mas deverá igualmente evitar-se uma restrição indevida do conceito de dados pessoais. A Directiva definiu o seu próprio âmbito de aplicação, excluindo diversas actividades, e permite uma certa flexibilidade na aplicação das regras a actividades que estão incluídas no seu âmbito. As autoridades de protecção de dados desempenham um papel essencial na identificação do equilíbrio mais adequado a nível da aplicação. (ver Capítulo II).

A análise do Grupo de Trabalho baseou-se nos quatro “pilares” principais que podem ser distinguidos na definição de “dados pessoais”: isto é, “qualquer informação”, “relativa a”, “identificada ou identificável”, “pessoa singular”. Estes elementos estão intimamente ligados e apoiam-se uns nos outros, e juntos determinam se uma informação deverá ser ou não considerada como “dados pessoais”. A análise apoia-se em exemplos retirados da prática nacional das APD europeias.

- O primeiro elemento – “qualquer informação” – apela a uma interpretação ampla do conceito, independentemente da natureza ou do conteúdo da informação, e do formato técnico em que é apresentada. Isto significa que tanto a informação objectiva como a subjectiva sobre uma pessoa, seja em que capacidade for, pode ser considerada como “dados pessoais”, e isto independentemente do meio técnico em

que está contida. O parecer debate ainda os dados biométricos e as distinções jurídicas sobre as amostras humanas das quais estes podem ser extraídos (ver Capítulo III.1).

- O segundo elemento – “relativa a” – tem sido frequentemente negligenciado, mas desempenha um papel crucial na determinação do âmbito material do conceito, especialmente em relação a objectos e novas tecnologias. O parecer apresenta três elementos alternativos – isto é, conteúdo, finalidade ou resultado – para determinar se uma informação é “relativa a” uma pessoa. Tal abrange igualmente informação que possa ter um claro impacto na forma como é tratada ou avaliada determinada pessoa. (ver Capítulo III.2).
- O terceiro elemento – “identificada ou identificável” –centra-se nas condições ao abrigo das quais uma pessoa deverá ser considerada como “identificável”, e sobretudo nos “meios susceptíveis de serem razoavelmente utilizados” pelo responsável pelo tratamento ou por qualquer outra pessoa na identificação da pessoa em causa. O contexto e circunstâncias especiais de um caso específico desempenham um papel importante nesta análise. O parecer trata também dos “dados tornados pseudónimos” e do uso de “dados codificados com chave” na investigação estatística ou farmacêutica (ver Capítulo III.3).
- O quarto elemento – “pessoa singular” – trata do requisito de que “dados pessoais” são relativos a “pessoas vivas”. O parecer debate igualmente a interacção com dados sobre pessoas mortas, nascituros e pessoas colectivas (ver Capítulo III.4).

Por último, o parecer debate o que acontece se os dados estão excluídos do âmbito da definição de “dados pessoais”. Nestes casos, poderão estar disponíveis diferentes soluções, designadamente legislação nacional fora do âmbito da directiva, desde que o direito comunitário seja respeitado (ver Capítulo IV).

O Grupo de Trabalho convida todas as partes interessadas a estudarem atentamente a orientação prestada neste parecer e a terem-na em consideração aquando da interpretação e aplicação das disposições da legislação nacional em consonância com a Directiva 95/46/CE.

Os membros do Grupo de Trabalho, na maioria representantes das autoridades de supervisão da protecção de dados a nível nacional, estão empenhados em aprofundar a orientação fornecida neste parecer nas suas próprias jurisdições e a assegurar uma aplicação adequada da sua legislação nacional em consonância com a Directiva 95/46/CE.

O Grupo de Trabalho pretende aplicar e desenvolver a orientação fornecida neste parecer, sempre que apropriado, e a tê-la em atenta consideração no seu trabalho futuro, nomeadamente no tratamento de tópicos como a Gestão da Identidade no contexto da Administração em linha e da Saúde em linha, bem como no contexto da identificação por rádio frequência (RFID). Quanto a este último tema, o Grupo de Trabalho pretende contribuir para uma posterior análise sobre a forma como as regras de protecção de dados podem ter um impacto na utilização de RFID e da eventual necessidade de medidas adicionais para assegurar o adequado respeito dos direitos e interesses de protecção de dados nesse contexto.

Por último, o Grupo de Trabalho gostaria de convidar à apresentação de reacções por parte dos interessados e das autoridades de supervisão, sobre a sua experiência prática com as orientações fornecida no presente parecer, incluindo quaisquer exemplos adicionais aos já mencionados neste documento. Pretende-se revisitar o tema em tempo útil, com o objectivo de melhorar o entendimento comum do conceito chave de dados pessoais, e nessa base assegurar uma aplicação harmonizada e uma melhor execução da Directiva 95/46/CE e da legislação comunitária relacionada

Pelo Grupo de Trabalho

O Presidente
Peter SCHAAR