



844/14/PT
WP 217

Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE

Adotado em 9 de abril de 2014

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

O secretariado é assegurado pela Direção C (Direitos Fundamentais e Cidadania da União) da Direção-Geral da Justiça da Comissão Europeia, B-1049 Bruxelas, Bélgica, Gabinete n.º MO-59 02/013.

Sítio Web: http://ec.europa.eu/justice/dados-proteção/index_pt.htm

Índice

Síntese	3
I. Introdução	5
II. Observações gerais e questões estratégicas	8
II.1. Síntese histórica.....	8
II.2. Papel do conceito	13
II.3. Conceitos relacionados.....	15
II.4. Contexto e consequências estratégicas.....	17
III. Análise das disposições	20
III.1. Síntese do artigo 7.º.....	20
III.1.1. Consentimento ou «necessário para [...]»	20
III.1.2. Relação com o artigo 8.º.....	22
III.2. Artigo 7.º, alíneas a) a e)	24
III.2.1. Consentimento.....	25
III.2.2. Contrato	25
III.2.3. Obrigação legal	29
III.2.4. Interesse vital.....	32
III.2.5. Missão pública.....	33
III.3. Artigo 7.º, alínea f): interesses legítimos	36
III.3.1. Interesses legítimos do responsável pelo tratamento (ou de terceiros)	37
III.3.2. Interesses ou direitos da pessoa em causa.....	45
III.3.3. Introdução à aplicação do teste da ponderação	47
III.3.4. Fatores-chave a ter em conta na aplicação do teste da ponderação	52
III.3.5. Responsabilidade e transparência.....	68
III.3.6. Direito de oposição e outros	70
IV. Observações finais	76
IV.1. Conclusões	76
IV. 2. Recomendações	81
Anexo 1. Guia rápido para a realização do teste da ponderação previsto no artigo 7.º, alínea f) 87	
Anexo 2. Exemplos práticos para ilustrar a aplicação do teste da ponderação previsto no artigo 7.º, alínea f)	91

Síntese

O presente parecer analisa os critérios estabelecidos no artigo 7.º da Diretiva 95/46/CE, que legitimam o tratamento de dados. Centrando-se nos interesses legítimos do responsável pelo tratamento, fornece orientações sobre a forma como o artigo 7.º, alínea f), deve ser aplicado no atual quadro jurídico e formula recomendações para futuros melhoramentos.

O artigo 7.º, alínea f), é o último de seis fundamentos para o tratamento lícito de dados pessoais. Com efeito, esta disposição exige a ponderação dos interesses legítimos do responsável pelo tratamento, ou de terceiros a quem os dados sejam comunicados, em relação aos interesses ou aos direitos fundamentais da pessoa em causa. O resultado deste teste de ponderação determinará se o artigo 7.º, alínea f), pode ser invocado como fundamento jurídico para o tratamento de dados.

O Grupo de Trabalho do artigo 29.º (a seguir designado por «GT29») reconhece o significado e a utilidade do critério previsto no artigo 7.º, alínea f), o qual, nas condições certas e sob reserva de garantias adequadas, pode ajudar a evitar a invocação excessiva de outros fundamentos jurídicos. O artigo 7.º, alínea f), não deve ser tratado como “último recurso” para situações raras ou inesperadas nas quais se considere que os outros fundamentos para o tratamento legítimo não são aplicáveis. No entanto, não deve ser escolhido automaticamente nem a sua utilização deve ser indevidamente alargada com base na perceção de que é menos restritivo do que os restantes fundamentos.

Uma avaliação adequada nos termos do artigo 7.º, alínea f), não é um simples teste de ponderação que consiste apenas em ponderar dois “valores” facilmente quantificáveis e comparáveis em relação um ao outro. Pelo contrário, o teste exige uma análise completa de uma série de fatores, de forma a assegurar que os interesses e os direitos fundamentais das pessoas em causa sejam devidamente tidos em conta. Ao mesmo tempo, o teste é modulável, podendo ser mais simples ou mais complexo, e não necessita de ser demasiado moroso. Os fatores a analisar na realização do teste de ponderação são, entre outros:

- a natureza e a origem do interesse legítimo e a questão de saber se o tratamento de dados é necessário para o exercício de um direito fundamental, se de outro modo é de interesse

público ou se é reconhecido na comunidade em causa;

- o impacto na pessoa em causa e as suas expectativas razoáveis quanto ao que acontecerá aos seus dados, bem como a natureza dos dados e a forma como são tratados;

- as garantias complementares que podem limitar o impacto indevido na pessoa em causa, tais como a minimização dos dados, a utilização de tecnologias para reforçar a proteção da privacidade, maior transparência, o direito generalizado e incondicional de optar por não permitir o tratamento (*opt-out*) e a portabilidade dos dados.

Para o futuro, o GT29 recomenda que se inclua na proposta de regulamento um considerando sobre os fatores-chave a analisar na aplicação do teste da ponderação. O GT29 recomenda igualmente que se acrescente um considerando que exija que o responsável pelo tratamento, quando necessário, documente a sua avaliação no sentido de garantir uma maior responsabilidade. Por último, o GT29 apoia a introdução de uma disposição substantiva que determine que os responsáveis pelo tratamento devem explicar às pessoas em causa as razões pelas quais consideram que os interesses ou os direitos e liberdades fundamentais da pessoa em causa não prevalecem sobre os seus interesses.

O GRUPO DE TRABALHO PARA A PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS

Instituído pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995,

Tendo em conta os artigos 29.º e 30.º, n.º 1, alínea a), e n.º 3, da referida diretiva,

Tendo em conta o seu regulamento interno,

ADOTOU O PRESENTE PARECER:

I. Introdução

O presente parecer analisa os critérios estabelecidos no artigo 7.º da Diretiva 95/46/CE¹ (a seguir designada por «diretiva»), que legitimam o tratamento de dados. Centra-se, em especial, nos interesses legítimos do responsável pelo tratamento, nos termos do artigo 7.º, alínea f).

Os critérios elencados no artigo 7.º estão relacionados com o princípio mais abrangente da «licitude», enunciado no artigo 6.º, n.º 1, alínea a), o qual exige que os dados pessoais sejam «[o]bjeto de um tratamento leal e lícito».

O artigo 7.º exige que o tratamento de dados pessoais só possa ser efetuado se pelo menos um dos seis fundamentos jurídicos elencados nesse artigo for aplicável. Em especial, o tratamento de dados pessoais só será efetuado a) com base no consentimento inequívoco da pessoa em causa²; ou se – sucintamente³ - for necessário para:

b) A execução de um contrato com a pessoa em causa;

¹ Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281, de 23.11.1995, p. 31).

² Ver o Parecer 15/2011 do Grupo de Trabalho do artigo 29.º para a proteção de dados sobre a definição de consentimento, adotado em 13.7.2011 (WP187).

³ Estas disposições serão analisadas pormenorizadamente mais adiante.

- c) O cumprimento de uma obrigação legal imposta ao responsável pelo tratamento;
- d) A proteção de interesses vitais da pessoa em causa;
- e) A execução de uma missão de interesse público; ou
- f) A prossecução de interesses legítimos do responsável pelo tratamento, sob reserva da aplicação de um teste da ponderação complementar em relação aos direitos e aos interesses da pessoa em causa.

Este último fundamento permite que o tratamento seja efetuado se for «necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou⁴ os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do n.º 1 do artigo 1.º». Por outras palavras, o artigo 7.º, alínea f), permite o tratamento sob reserva da aplicação de um teste da ponderação, que pondere os interesses legítimos do responsável pelo tratamento - ou do terceiro ou terceiros a quem os dados sejam comunicados – em relação aos interesses ou aos direitos fundamentais das pessoas em causa⁵.

Necessidade de uma abordagem mais coerente e harmonizada em toda a Europa

Os estudos realizados pela Comissão no âmbito da revisão da Diretiva⁶, bem como a cooperação e o intercâmbio de opiniões entre as autoridades nacionais responsáveis pela proteção de dados (a seguir designadas por «ARPD»), revelaram a falta de harmonização na interpretação do artigo 7.º, alínea f), da diretiva, que conduziu a aplicações divergentes nos Estados-Membros. Em especial, embora a aplicação de um verdadeiro teste da ponderação seja exigida em vários Estados-Membros, o artigo 7.º, alínea f), é por vezes incorretamente

⁴ Tal como explicado na secção III. 3.2, a versão em língua inglesa da diretiva parece conter um erro tipográfico: a redação correta é «interests or fundamental rights» e não «interests for fundamental rights».

⁵ A referência ao artigo 1.º, n.º 1, não deve ser interpretada no sentido de que limita o âmbito dos interesses e dos direitos e liberdades fundamentais da pessoa em causa. Pelo contrário, essa referência visa realçar o objetivo geral da legislação em matéria de proteção de dados e da própria diretiva. De facto, o artigo 1.º, n.º 1, refere não apenas a proteção do direito ao respeito pela vida privada mas igualmente a proteção do conjunto «das liberdades e dos direitos [...] das pessoas singulares», do qual o direito ao respeito pela vida privada é apenas um elemento.

⁶ Em 25 de janeiro de 2012, a Comissão Europeia adotou um pacote legislativo para a reforma do quadro europeu de proteção de dados. O pacote inclui i) uma «comunicação», COM (2012) 9 final, ii) uma proposta de «regulamento geral sobre a proteção de dados» (a seguir designada por «proposta de regulamento»), COM (2012) 11 final e iii) uma proposta de «diretiva» relativa à proteção de dados no domínio da aplicação do direito penal, COM (2012) 10 final. A respetiva «avaliação de impacto», que contém 10 anexos, é apresentada num documento de trabalho da Comissão, SEC (2012) 72 final. Ver, em especial, o estudo intitulado «Avaliação da aplicação da diretiva relativa à proteção de dados», que constitui o anexo 2 da avaliação de impacto que acompanha o pacote de reformas da Comissão Europeia em matéria de proteção de dados.

considerado uma «porta aberta» para legitimar quaisquer tratamentos de dados que não se enquadrem em nenhum dos restantes fundamentos jurídicos.

A inexistência de uma abordagem coerente pode ter como consequência a falta de segurança jurídica e de previsibilidade, pode enfraquecer a posição das pessoas em causa e pode igualmente impor uma sobrecarga regulatória desnecessária às empresas e organizações que desenvolvam atividades transnacionais. Tais incoerências já deram origem a litígios no Tribunal de Justiça da União Europeia (a seguir designado por «TJUE»).

⁷

Por conseguinte, é especialmente pertinente, uma vez que prosseguem os trabalhos com vista à adoção de um novo regulamento geral sobre a proteção de dados, que o sexto fundamento para o tratamento (relativo aos «interesses legítimos») e a sua relação com os restantes fundamentos para o tratamento sejam mais fáceis de compreender. Em especial, o facto de estarem em jogo direitos fundamentais das pessoas em causa implica que a aplicação de todos esses fundamentos deva ter – devida e igualmente - em conta o respeito por esses direitos. O artigo 7.º, alínea f), não deve tornar-se uma forma fácil de obviar ao cumprimento da legislação em matéria de proteção de dados.

Por essa razão, o Grupo de Trabalho do artigo 29.º para a proteção de dados (a seguir designado por «Grupo de Trabalho») decidiu analisar cuidadosamente esta questão como parte do seu programa de trabalho para 2012-2013 e – em cumprimento desse programa de trabalho⁸ - comprometeu-se a elaborar o presente parecer.

Aplicação do quadro jurídico atual e preparação do futuro

O próprio programa de trabalho estabelecia claramente dois objetivos: «[a]ssegurar uma aplicação coerente e correta do quadro jurídico atual» e «preparar o futuro».

Nesse sentido, o primeiro objetivo do presente parecer é garantir uma interpretação uniforme do quadro jurídico existente. Este objetivo vem na sequência de pareceres anteriores sobre

⁷ Ver a página 7, com a epígrafe «II.1 Síntese histórica», «Aplicação da diretiva; acórdão ASNEF e FECEMD».

⁸ Ver o programa de trabalho para 2012-2013 do Grupo de Trabalho do artigo 29.º para a proteção de dados, adotado em 1 de fevereiro de 2012 (WP190).

outras disposições-chave da diretiva⁹. Em segundo lugar, a partir dessa análise, o presente parecer formulará igualmente recomendações de ação a ter em conta durante a revisão do quadro jurídico em matéria de proteção de dados.

Estrutura do parecer

Após uma breve síntese, no Capítulo II, da história e do papel dos interesses legítimos e dos restantes fundamentos para o tratamento de dados, no Capítulo III analisar-se-á e interpretar-se-á as disposições pertinentes da diretiva, tendo em conta os pontos em comum da sua aplicação a nível nacional. Esta análise é ilustrada com exemplos práticos baseados nas experiências nacionais. A análise serve de base para as recomendações formuladas no Capítulo IV, quer no que respeita à aplicação do quadro jurídico atual quer no contexto da revisão da diretiva.

II. Observações gerais e questões estratégicas

II.1. Síntese histórica

A presente síntese centra-se na forma como os conceitos de licitude e de fundamentos jurídicos para o tratamento de dados, incluindo o de interesses legítimos, evoluíram. Em especial, explica como a necessidade de uma base jurídica foi utilizada pela primeira vez como requisito no contexto das derrogações ao direito ao respeito pela vida privada e posteriormente se tornou um requisito distinto no contexto da proteção de dados.

Convenção Europeia dos Direitos do Homem (a seguir designada por «CEDH»)

O artigo 8.º da Convenção Europeia dos Direitos do Homem, assinada em 1950, consagra o direito ao respeito pela vida privada – ou seja, o direito de qualquer pessoa ao respeito pela sua vida privada e familiar, pelo seu domicílio e pela sua correspondência. Proíbe qualquer ingerência no exercício desse direito, exceto se essa ingerência «estiver prevista na lei» e

⁹ Tais como o Parecer 3/2013 sobre a limitação da finalidade, adotado em 3.4.2013 (WP203), o Parecer 15/2011 sobre a definição de consentimento (referido na nota 2), o Parecer 8/2010 sobre a lei aplicável, adotado em 16.12.2010 (WP179) e o Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante», adotado em 16.2.2010 (WP169).

«constituir uma providência que, numa sociedade democrática, seja necessária» para satisfazer determinados tipos de interesses públicos preponderantes e especificamente previstos.

O artigo 8.º da CEDH centra-se na proteção da vida privada e exige que qualquer ingerência na vida privada seja justificada. Esta abordagem baseia-se numa proibição geral de ingerência no direito ao respeito pela vida privada e apenas permite exceções em condições rigorosamente definidas. Nos casos em que haja «ingerência na vida privada» é exigida uma base jurídica, bem como a especificação de uma finalidade legítima como condição para a avaliação da necessidade da ingerência. Esta abordagem explica que a CEDH não preveja uma lista dos fundamentos jurídicos possíveis mas se concentre na necessidade de uma base jurídica e nas condições que essa base jurídica deve satisfazer.

Convenção 108

A Convenção 108 do Conselho da Europa¹⁰, aberta à assinatura em 1981, apresenta a proteção de dados pessoais como um conceito distinto. A ideia subjacente, na altura, não era a de que o tratamento de dados pessoais devia ser sempre visto como uma «ingerência na vida privada» mas a de que para *proteger* os direitos e as liberdades fundamentais de todas as pessoas, nomeadamente o seu direito ao respeito pela vida privada, o tratamento de dados pessoais devia satisfazer sempre determinadas condições. Assim, o artigo 5.º estabelece os princípios fundamentais da legislação em matéria de proteção de dados, incluindo o requisito de que «[o]s dados de carácter pessoal que sejam objeto de um tratamento automatizado devem ser: **a)** Obtidos e tratados de forma leal e lícita». No entanto, a convenção não previa fundamentos precisos para o tratamento¹¹.

¹⁰ Convenção 108 para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal.

¹¹ O projeto da versão atualizada da convenção, adotado na reunião plenária do T-PD (Comité Consultivo do Conselho da Europa para o tratamento de dados pessoais) de novembro de 2012, dispõe que o tratamento de dados pode ser realizado com base no consentimento da pessoa em causa ou com base «nalgum fundamento legítimo previsto na lei», à semelhança da Carta dos Direitos Fundamentais da União Europeia referida na página 8 adiante.

*Diretrizes da OCDE*¹²

As diretrizes da OCDE, preparadas em paralelo com a Convenção 108 e adotadas em 1980, partilham ideias semelhantes sobre «licitude», embora o conceito seja expresso de forma diferente. As diretrizes foram atualizadas em 2013, sem alterações substanciais ao princípio da licitude. O artigo 7.º das diretrizes da OCDE, em especial, dispõe que «a coleta de dados pessoais deve ser limitada e qualquer desses dados deveria ser obtido através de meios legais e justos e, caso houver, informando e pedindo o consentimento do sujeito dos dados». Neste caso, o fundamento jurídico do consentimento é expressamente referido como uma opção, a utilizar «caso houver». Tal exigirá a apreciação dos interesses e dos direitos em jogo, bem como a avaliação do quão invasivo é o tratamento. Neste sentido, a abordagem da OCDE revela algumas semelhanças com os critérios - muito mais desenvolvidos - previstos na Diretiva 95/46/CE.

Diretiva 95/46/CE

Quando foi adotada, em 1995, a diretiva alicerçou-se nos primeiros instrumentos de proteção de dados, incluindo a Convenção 108 e as diretrizes da OCDE. Foi igualmente tomada em consideração a experiência inicial de alguns Estados-Membros em matéria de proteção de dados.

Para além do requisito mais abrangente estabelecido no artigo 6.º, n.º 1, alínea a), de que os dados pessoais devem ser objeto de um tratamento «leal e lícito», a diretiva acrescentou um conjunto específico de requisitos suplementares que ainda não constavam da Convenção 108 nem das diretrizes da OCDE: o tratamento de dados pessoais deve basear-se num dos seis fundamentos jurídicos previstos no artigo 7.º.

*Aplicação da diretiva; acórdão ASNEF e FECEMD*¹³

O relatório da Comissão intitulado «Avaliação da aplicação da diretiva relativa à proteção de dados»¹⁴ sublinha que a aplicação das disposições da diretiva no direito nacional foi, por

¹² Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, de 11 de julho de 2013.

¹³ Acórdão do Tribunal de Justiça de 24 de novembro de 2011, ASNEF e FECEMD, nos processos apensos C-468/10 e C-469/10.

vezes, insatisfatória. Na análise técnica da transposição da diretiva nos Estados-Membros¹⁵, a Comissão acrescenta alguns pormenores sobre a aplicação do artigo 7.º. Nessa análise, a Comissão explica que, embora a legislação da maioria dos Estados-Membros tenha estabelecido os seis fundamentos jurídicos em termos relativamente semelhantes aos utilizados na diretiva, a verdade é que a flexibilidade destes princípios conduziu a aplicações divergentes.

Neste contexto, é especialmente relevante que o Tribunal de Justiça, no seu acórdão ASNEF e FECEMD, de 24 de novembro de 2011, tenha declarado que a Espanha não transpôs corretamente o artigo 7.º, alínea f), da diretiva ao exigir que - na inexistência do consentimento da pessoa em causa - quaisquer dados relevantes utilizados constem de fontes acessíveis ao público. Nesse acórdão, o Tribunal de Justiça declarou igualmente que o artigo 7.º, alínea f), tem um efeito direto. O acórdão limita a margem de apreciação de que os Estados-Membros dispõem na aplicação do artigo 7.º, alínea f). Em especial, não devem ultrapassar a linha ténue que separa o esclarecimento, por um lado, do estabelecimento de requisitos suplementares que alterem o âmbito de aplicação do artigo 7.º, alínea f), por outro.

Ao deixar claro que os Estados-Membros não estão autorizados a impor restrições e exigências suplementares unilaterais no que respeita aos fundamentos jurídicos para o tratamento lícito de dados nas respetivas legislações nacionais, o acórdão tem consequências significativas. Os tribunais nacionais e demais órgãos relevantes devem interpretar as disposições nacionais à luz deste acórdão e, se necessário, afastar quaisquer normas e práticas nacionais contrárias.

À luz do acórdão, é ainda mais importante que as autoridades nacionais responsáveis pela proteção de dados (a seguir designadas por «ARPD») e/ou os legisladores da União Europeia cheguem a um entendimento claro e comum quanto à aplicabilidade do artigo 7.º, alínea f). Tal deve ser efetuado de forma equilibrada, sem restringir indevidamente, ou alargar indevidamente, o âmbito de aplicação desta disposição.

Carta dos Direitos Fundamentais

¹⁴ Ver o anexo 2 da Avaliação de Impacto do pacote de reformas da Comissão Europeia em matéria de proteção de dados, já referido na nota 6.

¹⁵ Análise e estudo de impacto sobre a aplicação da Diretiva CE/95/46 nos Estados-Membros. Ver http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf.

Desde que o Tratado de Lisboa entrou em vigor, em 1 de dezembro de 2009, a Carta dos Direitos Fundamentais da União Europeia (a seguir designada por «Carta») tem «o mesmo valor jurídico que os Tratados»¹⁶. A Carta consagra a proteção de dados pessoais como um direito fundamental nos termos do artigo 8.º, que se distingue do respeito pela vida privada e familiar nos termos do artigo 7.º. O artigo 8.º estabelece o requisito de um fundamento legítimo para o tratamento. Em especial, dispõe que o tratamento de dados pessoais deve ser efetuado «com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei»¹⁷. Estas disposições reforçam quer a importância do princípio da licitude quer a necessidade de uma base jurídica adequada para o tratamento de dados pessoais.

Proposta de regulamento sobre a proteção de dados

No contexto do processo de revisão em matéria proteção de dados, o alcance dos fundamentos para a licitude nos termos do artigo 7.º, em especial o âmbito de aplicação do artigo 7.º, alínea f), é presentemente objeto de discussão.

O artigo 6.º da proposta de regulamento elenca os fundamentos para o tratamento lícito de dados pessoais. Salvo algumas exceções (descritas mais adiante), os seis fundamentos possíveis permanecem, em grande medida, inalterados face aos previstos atualmente no artigo 7.º da diretiva. Contudo, a Comissão propôs-se fornecer mais orientações sob a forma de atos delegados.

É interessante observar que, no contexto do trabalho realizado pela comissão competente do Parlamento Europeu¹⁸, procurou-se esclarecer o conceito de interesses legítimos na própria proposta de regulamento. Foi elaborada uma lista de casos nos quais os interesses do responsável pelo tratamento de dados, por norma, prevalecem sobre os interesses legítimos e os direitos e liberdades fundamentais da pessoa em causa, e outra lista de casos nos quais

¹⁶ Ver o artigo 6.º, n.º 1, do TUE.

¹⁷ Ver o artigo 8.º, n.º 2, da Carta.

¹⁸ Projeto de relatório da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos (LIBE) sobre a Proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), de 16.1.2013 (a seguir «projeto de relatório da Comissão LIBE»). Ver, em especial, as alterações n.ºs 101 e 102. Ver igualmente as alterações adotadas no relatório final da referida comissão, em 21.10.2013 (a seguir «relatório final da Comissão LIBE»).

acontece o contrário. Essas listas – constantes de disposições ou de considerandos - são um importante contributo para a avaliação do equilíbrio entre os direitos e os interesses do responsável pelo tratamento e da pessoa em causa, e são tidas em conta no presente parecer¹⁹.

II.2. Papel do conceito

Interesses legítimos do responsável pelo tratamento: teste da ponderação como última opção?

O artigo 7.º, alínea f), é elencado como última opção entre seis fundamentos que permitem o tratamento lícito de dados pessoais. Requer a realização de um teste da ponderação: o que for necessário para prosseguir interesses legítimos do responsável pelo tratamento (ou de terceiros) deve ser ponderado em relação aos interesses ou aos direitos e liberdades fundamentais da pessoa em causa. O resultado do teste da ponderação determina se o artigo 7.º, alínea f), pode ser invocado como fundamento jurídico para o tratamento.

A natureza aberta desta disposição suscita muitas questões importantes relativamente ao seu alcance e âmbito de aplicação exatos, as quais serão, por sua vez, analisadas no presente parecer. No entanto, como será explicado mais adiante, tal não significa necessariamente que se deva considerar que esta opção só pode ser utilizada com parcimónia, como «último recurso» para colmatar lacunas em situações raras e imprevistas, ou como última possibilidade quando nenhum outro fundamento seja aplicável. De igual modo, não deve ser considerada uma opção preferencial nem a sua utilização deve ser indevidamente alargada por ser considerada menos restritiva do que os restantes fundamentos.

Pelo contrário, é bem possível que o artigo 7.º, alínea f), tenha o seu próprio domínio natural de relevância e possa desempenhar um papel muito útil como fundamento para o tratamento lícito de dados, desde que estejam reunidas algumas condições essenciais.

¹⁹ Ver a secção III.3.1, em especial os pontos das páginas 24 e 25, que contêm uma lista não exaustiva de alguns contextos mais comuns nos quais pode ser suscitada a questão do interesse legítimo nos termos do artigo 7.º, alínea f).

A utilização correta do artigo 7.º, alínea f), nas condições certas e sob reserva de garantias adequadas, pode igualmente ajudar a evitar a utilização abusiva, e a invocação excessiva, de outros fundamentos jurídicos.

Os primeiros cinco fundamentos previstos no artigo 7.º assentam no consentimento da pessoa em causa, num contrato, numa obrigação legal ou noutra motivo especificamente identificado como fundamento para o tratamento legítimo. Quando o tratamento se baseie num desses cinco fundamentos, é considerado legítimo *a priori*, pelo que fica apenas sujeito ao cumprimento das demais disposições legais aplicáveis. Por outras palavras, presume-se que existe um equilíbrio entre os diferentes direitos e interesses em jogo – incluindo os do responsável pelo tratamento e os da pessoa em causa - partindo, naturalmente, do princípio de que todas as outras disposições da legislação em matéria de proteção de dados são respeitadas. Por outro lado, o artigo 7.º, alínea f), exige a realização de um teste *específico* nos casos que não se enquadrem nos cenários predefinidos nos fundamentos previstos nas alíneas a) a e). Tal permite assegurar que, fora desses cenários, qualquer tratamento tenha de cumprir o requisito do teste da ponderação, tendo devidamente em conta os interesses e os direitos fundamentais da pessoa em causa.

Em determinados casos, este teste pode levar à conclusão de que o equilíbrio é favorável aos interesses e aos direitos fundamentais das pessoas em causa e que, conseqüentemente, a atividade de tratamento não pode realizar-se. Por outro lado, noutros casos, uma avaliação adequada do equilíbrio nos termos do artigo 7.º, alínea f), muitas vezes com a possibilidade de optar por não permitir o tratamento, pode ser uma alternativa válida à utilização incorreta, por exemplo, do fundamento do «consentimento» ou da necessidade «para a execução de um contrato». Neste sentido, o artigo 7.º, alínea f), apresenta garantias complementares - que exigem medidas adequadas – em comparação com os restantes fundamentos predeterminados. Por conseguinte, não deve ser considerado o «elo mais fraco» ou uma porta aberta para legitimar todas as atividades de tratamento de dados que não sejam abrangidas por nenhum dos outros fundamentos jurídicos.

O Grupo de Trabalho reitera que, ao interpretar o âmbito de aplicação do artigo 7.º, alínea f), visa a adoção de uma abordagem equilibrada, que assegure aos responsáveis pelo tratamento a necessária flexibilidade em situações nas quais não se verifique um impacto indevido nas

pessoas em causa, proporcionando, ao mesmo tempo, às pessoas em causa segurança jurídica e garantias suficientes de que esta disposição aberta não será utilizada de forma abusiva.

II.3. Conceitos relacionados

Relação entre o artigo 7.º, alínea f), e os restantes fundamentos para a licitude

O primeiro fundamento para a licitude referido no artigo 7.º é o consentimento, seguindo-se os restantes, incluindo os contratos e as obrigações legais, progressivamente até ao teste da ponderação dos interesses legítimos, que é elencado como o último dos seis fundamentos possíveis. A ordem pela qual os fundamentos jurídicos são elencados no artigo 7.º tem sido por vezes interpretada como uma indicação da importância de cada um dos diferentes fundamentos. No entanto, como já foi realçado no parecer do Grupo de Trabalho sobre o conceito de consentimento²⁰, o texto da diretiva não estabelece uma distinção jurídica entre os seis fundamentos nem aponta para a existência de uma hierarquia entre eles. Não existe qualquer indicação de que o artigo 7.º, alínea f), deva ser aplicado apenas em casos excecionais e o texto também não aponta no sentido de que a ordem específica pela qual os seis fundamentos jurídicos são elencados tenha qualquer efeito jurídico relevante. Simultaneamente, o significado exato do artigo 7.º, alínea f), e a sua relação com os restantes fundamentos para a licitude são há muito tempo pouco claros.

Neste enquadramento, e dadas as diversidades históricas e culturais e a linguagem aberta da diretiva, desenvolveram-se várias abordagens: alguns Estados-Membros revelaram uma tendência para considerar o artigo 7.º, alínea f), um fundamento não preferencial, que se destina a colmatar lacunas apenas nalguns casos excecionais, quando nenhum dos restantes cinco fundamentos seja ou possa ser aplicável²¹. Outros Estados-Membros, pelo contrário, consideram-no apenas uma de seis opções, que não é nem mais nem menos importante do que as outras opções e que pode ser aplicada em inúmeras e variadas situações, desde que estejam reunidas as condições necessárias.

²⁰ Ver a nota 2 supra.

²¹ Deve também observar-se que, no seu projeto de relatório, a Comissão LIBE propôs, na alteração n.º 100, que se separasse o artigo 7.º, alínea f), dos restantes fundamentos jurídicos e propôs igualmente o estabelecimento de requisitos suplementares para os casos em que este fundamento jurídico seja invocado, incluindo mais transparência e maior responsabilidade, como se verá mais à frente.

Tendo em conta estas diferenças, e à luz do acórdão ASNEF e FECEMD, é importante clarificar a relação entre o fundamento relativo aos «interesses legítimos» e os restantes fundamentos de licitude – por exemplo, relativamente ao consentimento, aos contratos, às missões de interesse público – e também relativamente ao direito de oposição da pessoa em causa. Tal pode ajudar a definir melhor o papel e a função do fundamento relativo aos interesses legítimos e, assim, contribuir para aumentar a segurança jurídica.

Deve igualmente observar-se que o fundamento relativo aos interesses legítimos, tal como os restantes fundamentos, com exceção do consentimento, exige a realização de um teste da «necessidade». Tal limita rigorosamente o contexto em que cada fundamento é aplicável. O Tribunal de Justiça da União Europeia considerou que a «necessidade» é um conceito autónomo de direito comunitário²². O Tribunal Europeu dos Direitos do Homem forneceu igualmente orientações úteis²³.

Além disso, o facto de ter um fundamento jurídico adequado não exige o responsável pelo tratamento dos dados das suas obrigações decorrentes do artigo 6.º no que respeita à lealdade, à licitude, à necessidade e à proporcionalidade, bem como à qualidade dos dados. Por exemplo, mesmo que o tratamento de dados pessoais se baseie no fundamento relativo aos interesses legítimos, ou na execução de um contrato, tal não permite uma recolha de dados excessiva em relação à finalidade estabelecida.

Os interesses legítimos e os restantes fundamentos previstos no artigo 7.º são fundamentos alternativos, pelo que é suficiente que um deles seja aplicável. No entanto, são cumulativos não apenas com os requisitos previstos no artigo 6.º mas igualmente com todos os outros princípios e requisitos em matéria de proteção de dados que possam ser aplicáveis.

Outros testes da ponderação

²² Acórdão do Tribunal de Justiça da União Europeia de 16 de dezembro de 2008, Heinz Huber/Alemanha, no processo C-524/06, n.º 52: «Por conseguinte, face ao objetivo de assegurar um nível de proteção equivalente em todos os Estados-Membros, o conceito de necessidade, tal como ele resulta do artigo 7.º alínea e), da Diretiva 95/46, que se destina precisamente a delimitar uma das hipóteses em que o tratamento de dados pessoais é lícito, não pode ter um conteúdo variável consoante o Estado-Membro. Logo, trata-se de um conceito autónomo de direito comunitário que deve receber uma interpretação suscetível de cumprir plenamente o objetivo dessa diretiva, definido no seu artigo 1.º, n.º 1».

²³ Acórdão do Tribunal Europeu dos Direitos do Homem de 25 de março de 1983, no processo Silver e o. c. Reino Unido, § 97, a propósito da expressão «necessário numa sociedade democrática»: «o adjetivo ‘necessário’ não é sinónimo de ‘indispensável’ nem possui a flexibilidade de termos como ‘admissível’, ‘normal’, ‘útil’, ‘razoável’ ou ‘desejável’ (...)».

O teste da ponderação do artigo 7.º, alínea f), não é o único previsto na diretiva. Por exemplo, o artigo 9.º requer a ponderação entre o direito à proteção de dados pessoais e a liberdade de expressão. Este artigo permite aos Estados-Membros estabelecer as isenções e derrogações necessárias para o tratamento de dados pessoais «efetuado para fins exclusivamente jornalísticos ou de expressão artística ou literária» na medida em que aquelas sejam «necessárias para conciliar o direito à vida privada com as normas que regem a liberdade de expressão».

Além disso, muitas outras disposições da diretiva exigem igualmente uma análise casuística, uma ponderação entre os interesses e os direitos em jogo e uma avaliação multifatorial flexível. Estas incluem as disposições relativas à necessidade, à proporcionalidade e à limitação da finalidade, as exceções previstas no artigo 13.º e a investigação científica, para mencionar apenas algumas.

De facto, a diretiva parece ter sido concebida para deixar uma margem de interpretação e de ponderação de interesses. Obviamente pretendeu-se, pelo menos em parte, deixar uma margem maior aos Estados-Membros na transposição para o direito nacional. Acresce, no entanto, que a necessidade de alguma flexibilidade resulta igualmente da própria natureza do direito à proteção de dados pessoais e do direito ao respeito pela vida privada. De facto, estes dois direitos, tal como quase todos (mas não todos) os outros direitos fundamentais, são considerados direitos humanos relativos ou qualificados²⁴. Estes tipos de direitos devem ser sempre interpretados no seu contexto. Sob reserva de garantias adequadas, podem ser ponderados em relação aos direitos de terceiros. Nalgumas situações – e também sob reserva de garantias adequadas – podem ser igualmente restringidos por motivos de interesse público.

II.4. Contexto e consequências estratégicas

²⁴ Existem apenas alguns direitos humanos que não podem ser ponderados em relação aos direitos de terceiros ou aos interesses da comunidade em geral. São conhecidos como direitos absolutos. Estes direitos nunca podem ser limitados ou objeto de restrições, sejam quais forem as circunstâncias – mesmo em situações de guerra ou de emergência. Um exemplo é o direito de não ser submetido a tortura nem a tratamentos desumanos ou degradantes. Em caso algum é permitido submeter alguém a tortura ou a tratamentos desumanos ou degradantes, independentemente das circunstâncias. São exemplos de direitos humanos não absolutos o direito ao respeito pela vida privada e familiar, o direito à liberdade de expressão e o direito à liberdade de pensamento, de consciência e de religião.

Garantir a legitimidade mas também a flexibilidade: meios de especificação do artigo 7.º, alínea f)

O texto atual do artigo 7.º, alínea f), da diretiva é aberto. Tal significa que este pode ser invocado numa grande variedade de situações, desde que os seus requisitos, incluindo o teste da ponderação, sejam cumpridos. No entanto, esta flexibilidade pode igualmente ter implicações negativas. Para evitar que conduza a uma aplicação incoerente a nível nacional, ou à falta de segurança jurídica, a emissão de orientações suplementares pode desempenhar um papel importante.

Na proposta de regulamento, a Comissão prevê a emissão de tais orientações sob a forma de atos delegados. Entre as restantes opções está a inclusão de esclarecimentos e de disposições pormenorizadas no texto da própria proposta de regulamento²⁵ e/ou a atribuição ao Comité Europeu para a proteção de dados (a seguir designado por «CEPD») da missão de fornecer orientações suplementares neste domínio.

Cada uma destas opções, por sua vez, tem vantagens e desvantagens. Se a avaliação for efetuada caso a caso, sem quaisquer orientações suplementares, existe o risco de aplicação incoerente e de falta de previsibilidade, como aconteceu no passado.

Por outro lado, o fornecimento, no texto da própria proposta de regulamento, de listas pormenorizadas e exaustivas de situações nas quais os interesses legítimos do responsável pelo tratamento, por norma, prevalecem sobre os direitos fundamentais da pessoa em causa, ou vice-versa, pode induzir em erro, ser desnecessariamente prescritivo ou ambos.

Contudo, estas abordagens podem servir de inspiração para uma solução equilibrada, contribuindo para um maior grau de pormenor da própria proposta de regulamento, e para a emissão de orientações suplementares sob a forma de atos delegados ou pelo CEPD²⁶.

²⁵ Ver a secção II.1, Síntese histórica, sob a epígrafe «Proposta de regulamento sobre a proteção de dados», páginas 8 e 9.

²⁶ Quanto aos atos delegados e à orientação por parte do CEPD, no Parecer 8/2012 que presta um contributo suplementar para o debate sobre a reforma em matéria de proteção de dados, adotado em 5.10.2012 (WP199), o Grupo de Trabalho manifesta uma clara preferência pela segunda (págs. 13 e 14 da versão portuguesa).

A análise constante do capítulo III visa lançar as bases que permitam encontrar uma abordagem que não seja nem tão genérica que se revele desprovida de significado nem tão específica que se revele excessivamente rígida.

III. Análise das disposições

III.1. Síntese do artigo 7.º

O artigo 7.º exige que tratamento de dados pessoais só possa ser efetuado se pelo menos um dos seis fundamentos jurídicos elencados nesse artigo for aplicável. Antes de analisar cada um desses fundamentos, a presente secção III.1 apresenta uma síntese do artigo 7.º e da sua relação com o artigo 8.º, relativo a certas categorias específicas de dados.

III.1.1. Consentimento ou «necessário para [...]»

É possível estabelecer uma distinção entre um caso em que os dados pessoais são tratados com base no consentimento inequívoco da pessoa em causa (artigo 7.º, alínea a)) e os restantes cinco casos (artigo 7.º, alíneas b) a f)). Estes cinco casos - resumidamente – descrevem cenários nos quais o tratamento pode ser necessário num contexto específico, tal como a execução de um contrato com a pessoa em causa, o cumprimento de uma obrigação legal imposta ao responsável pelo tratamento, etc.

No primeiro caso, nos termos do artigo 7.º, alínea a), são as próprias pessoas em causa que autorizam o tratamento dos seus dados pessoais. Cabe-lhes decidir se permitem que os seus dados sejam tratados. Simultaneamente, o consentimento não elimina a necessidade de respeitar os princípios previstos no artigo 6.º ²⁷. Além disso, para ser legítimo, o consentimento tem ainda de satisfazer determinadas condições essenciais, tal como explicado no Parecer 15/2011 do Grupo de Trabalho²⁸. Uma vez que o tratamento dos dados **do** utilizador depende, em última análise, da vontade deste, a tónica é colocada na validade e no alcance do consentimento da pessoa em causa.

²⁷ Acórdão do Supremo Tribunal dos Países Baixos de 9 de setembro de 2011, no processo ECLI:NL:HR:2011:BQ8097, §3.3, alínea e), quanto ao princípio da proporcionalidade. Ver igualmente a página 8 (da versão portuguesa) do Parecer 15/2011 do Grupo de Trabalho, já referido na nota 2: «... a obtenção de consentimento não exonera o responsável pelo tratamento das obrigações estabelecidas no artigo 6.º relativas à lealdade, necessidade e proporcionalidade, assim como à qualidade dos dados. Por exemplo, mesmo que o tratamento de dados seja baseado no consentimento da pessoa em causa, este consentimento não legitimaria uma recolha de dados excessiva em relação ao fim em causa».

²⁸ Ver as páginas 12 a 28 (da versão portuguesa) do Parecer 15/2011, já referido na nota 2.

Por outras palavras, o primeiro fundamento, previsto no artigo 7.º, alínea a), centra-se na autodeterminação da pessoa em causa como fundamento para o tratamento legítimo. Em contrapartida, todos os outros fundamentos permitem o tratamento – sob reserva de garantias e medidas – em situações nas quais, independentemente do consentimento, o tratamento de dados num determinado contexto seja adequado e necessário para prosseguir um interesse legítimo específico.

Cada uma das alíneas b), c), d) e e) especifica um critério que legitima o tratamento:

- b) A execução de um contrato com a pessoa em causa;
- c) O cumprimento de uma obrigação legal imposta ao responsável pelo tratamento;
- d) A proteção de interesses vitais da pessoa em causa;
- e) A execução de uma missão de interesse público.

A alínea f) é menos específica e refere-se, de forma mais genérica, a (qualquer tipo de) interesse legítimo prosseguido pelo responsável pelo tratamento (em qualquer contexto). No entanto, esta disposição geral está expressamente subordinada a um teste da ponderação complementar, que visa proteger os interesses e os direitos das pessoas em causa, como se verá mais adiante, na secção III.2.

A avaliação do cumprimento dos critérios estabelecidos no artigo 7.º, alíneas a) a f), é, em todos os casos, inicialmente efetuada pelo responsável pelo tratamento dos dados, nos termos da lei aplicável e das orientações sobre a forma como a lei deve ser aplicada. Num segundo momento, a legitimidade do tratamento pode ser objeto de nova avaliação, e pode ser potencialmente contestada pelas pessoas em causa, por outras partes interessadas e pelas autoridades responsáveis pela proteção de dados, e, em última instância, pode ser objeto de decisão pelos tribunais.

Para completar esta breve síntese, há que referir que, como se abordará na secção III.3.6, pelo menos nos casos referidos nas alíneas e) e f), a pessoa em causa pode exercer o direito de

oposição nos termos do artigo 14.^{o29}. Tal desencadeará uma nova avaliação dos interesses em jogo ou, no caso do marketing direto (artigo 14.^o, alínea b)), exigirá que o responsável pelo tratamento ponha termo ao tratamento dos dados pessoais sem mais avaliações.

III.1.2. Relação com o artigo 8.^o

O artigo 8.^o da diretiva regula o tratamento de certas categorias específicas de dados pessoais. Aplica-se expressamente a dados «que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como [ao] tratamento de dados relativos à saúde e à vida sexual» (artigo 8.^o, n.^o 1), e a dados «relativos a infrações [ou] condenações penais» (artigo 8.^o, n.^o 5).

O tratamento de tais dados é, em princípio, proibido, salvo algumas exceções. O artigo 8.^o, n.^o 2, alíneas a) a e), prevê várias exceções a essa proibição. O artigo 8.^o, n.^{os} 3 e 4, prevê mais algumas exceções. Algumas destas disposições são semelhantes – mas não idênticas – às disposições estabelecidas no artigo 7.^o, alíneas a) a f).

As condições específicas previstas no artigo 8.^o, bem como o facto de alguns fundamentos elencados no artigo 7.^o se assemelharem às condições estabelecidas no artigo 8.^o, suscitam a questão da relação entre as duas disposições.

Se o artigo 8.^o tiver sido concebido como uma *lex specialis*, há que analisar se exclui a aplicação do artigo 7.^o no seu todo. Se assim for, tal significa que certas categorias específicas de dados pessoais podem ser objeto de tratamento sem cumprir o disposto no artigo 7.^o, desde que uma das exceções previstas no artigo 8.^o seja aplicável. No entanto, é igualmente possível que a relação seja mais complexa e que os artigos 7.^o e 8.^o sejam aplicáveis cumulativamente³⁰.

²⁹ De acordo com o artigo 14.^o, alínea a), este direito aplica-se «salvo disposição em contrário do direito nacional». Por exemplo, na Suécia, o direito nacional não permite a oposição ao tratamento quando este se baseie no artigo 7.^o, alínea e).

³⁰ Uma vez que o artigo 8.^o constitui uma *proibição com exceções*, essas exceções podem ser consideradas requisitos que apenas limitam o alcance da proibição mas não conferem, por si sós, uma base jurídica suficiente para o tratamento. De acordo com este entendimento, a aplicação das exceções previstas no artigo 8.^o não exclui a aplicação dos requisitos estabelecidos no artigo 7.^o e, quando necessário, ambos devem ser aplicados cumulativamente.

De qualquer forma, é evidente que o objetivo, em termos de política, é conferir proteção complementar para certas categorias específicas de dados. Consequentemente, o resultado final da análise deve ser igualmente evidente: a aplicação do artigo 8.º, de forma isolada ou cumulativamente com o artigo 7.º, visa conferir um nível mais elevado de proteção a certas categorias específicas de dados.

Na prática, embora, nalguns casos, o artigo 8.º apresente requisitos mais rigorosos – tal como o consentimento «explícito» previsto no artigo 8.º, n.º 2, alínea a), face ao «consentimento inequívoco» previsto no artigo 7.º - o mesmo não se aplica a todas as disposições. Algumas exceções previstas no artigo 8.º não se afiguram equivalentes ou mais rigorosas do que os fundamentos elencados no artigo 7.º. Não é correto concluir, por exemplo, que o facto de alguém ter manifestamente tornado públicas certas categorias específicas de dados nos termos do artigo 8.º, n.º 2, alínea e), é – sempre e por si só – condição suficiente para permitir qualquer tipo de tratamento de dados, sem uma avaliação do equilíbrio entre os interesses e os direitos em jogo, tal como exigido no artigo 7.º, alínea f)³¹.

Nalgumas situações, o facto de o responsável pelo tratamento dos dados ser um partido político suspende igualmente a proibição do tratamento de certas categorias específicas de dados nos termos do artigo 8.º, n.º 2, alínea d). No entanto, tal não significa que qualquer tratamento abrangido pelo âmbito de aplicação desta disposição seja necessariamente lícito. Tal deve ser avaliado separadamente e o responsável pelo tratamento pode ter de provar, por exemplo, que o tratamento dos dados é necessário para a execução de um contrato (artigo 7.º, alínea b)), ou que o seu interesse legítimo, nos termos do artigo 7.º, alínea f), prevalece. Neste último caso, é necessário realizar o teste da ponderação previsto no artigo 7.º, alínea f), após verificar que o responsável pelo tratamento dos dados cumpre os requisitos estabelecidos no artigo 8.º.

De igual forma, o mero facto de «o tratamento dos dados [ser] necessário para efeitos de medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamentos médicos ou gestão de serviços da saúde» e de o tratamento desses dados estar sujeito a uma obrigação de

³¹ Além disso, o artigo 8.º, n.º 2, alínea e), não deve ser interpretado *a contrario* no sentido de que, quando os dados tornados públicos pela pessoa em causa não sejam sensíveis, podem ser tratados sem que sejam impostas mais condições. Os dados disponíveis ao público continuam a ser dados pessoais sujeitos a requisitos de proteção de dados, incluindo o cumprimento do disposto no artigo 7.º, independentemente de se tratar ou não de dados sensíveis.

segredo – tal como referido no artigo 8.º, n.º 3 – implica que tal tratamento de dados sensíveis está *isento da proibição* prevista no artigo 8.º, n.º 1. No entanto, tal não é necessariamente suficiente para garantir também a licitude nos termos do artigo 7.º, e exigirá um fundamento jurídico, como, por exemplo, um contrato com o doente nos termos do artigo 7.º, alínea b), uma obrigação legal nos termos do artigo 7.º, alínea c), a execução de uma missão de interesse público nos termos do artigo 7.º, alínea e), ou uma avaliação nos termos do artigo 7.º, alínea f).

Em conclusão, o Grupo de Trabalho considera que há que analisar caso a caso se o artigo 8.º, por si só, impõe condições mais rigorosas e suficientes³² ou se é necessária a aplicação cumulativa dos artigos 7.º e 8.º para garantir a proteção total das pessoas em causa. Em caso algum pode o resultado dessa análise conduzir a uma proteção menor para certas categorias específicas de dados³³.

Tal significa igualmente que um responsável pelo tratamento de certas categorias específicas de dados nunca pode invocar *exclusivamente* um fundamento jurídico nos termos do artigo 7.º para legitimar uma atividade de tratamento de dados. Quando aplicável, o artigo 7.º, não *prevalecerá* mas será sempre aplicado *cumulativamente* com o artigo 8.º para assegurar que todas as garantias e medidas relevantes sejam respeitadas. Tal será ainda mais relevante no caso de os Estados-Membros decidirem acrescentar outras derrogações às constantes do artigo 8.º, tal como previsto no artigo 8.º, n.º 4.

III.2. Artigo 7.º, alíneas a) a e)

A secção III.2 apresenta uma breve síntese de cada um dos fundamentos jurídicos previstos no artigo 7.º, alíneas a) a e), da diretiva e, mais adiante, na secção III.3, o parecer centra-se no artigo 7.º, alínea f). Esta análise irá igualmente realçar algumas das interfaces mais frequentes entre estes fundamentos jurídicos, por exemplo, que associam «contrato», «obrigação legal» e «interesse legítimo», dependendo do contexto específico e das circunstâncias do caso.

³² Ver a análise efetuada no Parecer AMA do Grupo de Trabalho, n.º 3.3, que tem em conta quer o artigo 7.º quer o artigo 8.º da diretiva: Segundo parecer 4/2009 sobre a Norma Internacional relativa à proteção da privacidade e dos dados pessoais da Agência Mundial Antidopagem (AMA), sobre as disposições pertinentes do Código AMA e sobre outros aspetos relacionados com a privacidade no contexto da luta contra a dopagem no desporto por parte da AMA e de outras organizações antidopagem (nacionais), adotado em 06.04.2009 (WP162).

³³ Escusado será dizer que também em caso de aplicação do artigo 8.º deve ser assegurado o respeito pelas outras disposições da diretiva, incluindo o artigo 6.º.

III.2.1. Consentimento

O consentimento como fundamento jurídico foi analisado no Parecer 15/2011 do Grupo de Trabalho sobre a definição de consentimento. As principais conclusões desse parecer são que o consentimento é um de entre vários fundamentos jurídicos para o tratamento de dados pessoais, e não o fundamento principal; desempenha um papel importante, mas não exclui a possibilidade, dependendo do contexto, de outros fundamentos jurídicos serem porventura mais apropriados, tanto do ponto de vista do responsável pelo tratamento como da pessoa em causa; se for utilizado corretamente, o consentimento consubstancia uma ferramenta que confere à pessoa em causa controlo sobre o tratamento dos seus dados; se for utilizado incorretamente, o controlo da pessoa em causa torna-se ilusório e o consentimento constitui uma base inadequada para o tratamento de dados.

Entre as suas recomendações, o Grupo de Trabalho reiterou a necessidade de clarificar o significado de «consentimento inequívoco»: «A clarificação deveria procurar sublinhar que o requisito do consentimento inequívoco obriga ao uso de mecanismos que não deixem qualquer dúvida de que a pessoa em causa teve a intenção de dar o seu consentimento. Simultaneamente deve ser clarificado que a utilização de configurações pré-definidas, que têm de ser alteradas pela pessoa em causa para rejeitar o tratamento (consentimento baseado no silêncio) não conduz a um consentimento inequívoco. Isto é especialmente verdade num ambiente em linha»³⁴. Recomendou igualmente a obrigatoriedade de os responsáveis pelo tratamento dos dados instituírem mecanismos que permitam fazer prova do consentimento (no âmbito de uma obrigação genérica de responsabilidade) e solicitou ao legislador a previsão de uma exigência expressa relativa à qualidade e acessibilidade da informação que forma a base para o consentimento.

III.2.2. Contrato

O artigo 7.º, alínea b), proporciona um fundamento jurídico se «[o] tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa». Tal abrange dois cenários diferentes.

³⁴ Ver a página 40 (da versão portuguesa) do Parecer 15/2011 do Grupo de Trabalho sobre a definição de consentimento.

- i) Em primeiro lugar, a disposição abrange as situações nas quais o tratamento seja necessário para a execução de um contrato no qual a pessoa em causa é parte. Tal pode incluir, por exemplo, o tratamento dos dados relativos ao endereço da pessoa em causa para que os bens adquiridos em linha possam ser entregues ou o tratamento dos dados relativos ao cartão de crédito para que o pagamento seja efetuado. No contexto laboral, este fundamento pode permitir, por exemplo, o tratamento das informações relativas ao salário e dos dados relativos à conta bancária para que os salários possam ser pagos.

A disposição deve ser interpretada de forma estrita e não abrange as situações nas quais o tratamento não seja verdadeiramente *necessário* para a execução de um contrato, mas sim imposto unilateralmente à pessoa em causa pelo responsável pelo tratamento. Também o facto de determinado tratamento de dados ser abrangido por um contrato não significa automaticamente que o tratamento é necessário para a execução desse contrato. Por exemplo, o artigo 7.º, alínea b), não constitui um fundamento jurídico adequado para construir um perfil dos gostos e do estilo de vida do utilizador com base na sequência de cliques num sítio Web e nos bens adquiridos. Isto porque o responsável pelo tratamento dos dados não foi contratado para elaborar um perfil mas sim para entregar determinados bens e serviços, por exemplo. Mesmo que essas atividades de tratamento estejam especificamente referidas no texto em caracteres reduzidos do contrato, este facto, por si só, não as torna «necessárias» para a execução do contrato.

Neste contexto, existe uma ligação clara entre a avaliação da necessidade e a conformidade com o princípio da limitação da finalidade. É importante determinar a razão de ser exata do contrato, ou seja, o seu conteúdo e o seu objetivo fundamental, uma vez que será tida em conta na apreciação da necessidade do tratamento dos dados para a execução do contrato.

Nalgumas situações ambíguas, a determinação da necessidade do tratamento para a execução do contrato pode ser discutível ou exigir um apuramento mais específico dos factos. Por exemplo, a criação, numa empresa, de uma base de dados interna dos contactos dos trabalhadores que contenha o nome, o endereço profissional, o número

de telefone e o endereço de correio eletrónico de todos os trabalhadores, de forma a possibilitar que os trabalhadores contactem os colegas, pode, em determinadas situações, ser considerada necessária para a execução de um contrato nos termos do artigo 7.º, alínea b), mas pode ser igualmente lícita nos termos do artigo 7.º, alínea f), se ficar demonstrado que o interesse do responsável pelo tratamento prevalece e se forem tomadas todas as medidas adequadas, incluindo, por exemplo, a necessária consulta dos representantes dos trabalhadores.

Outros casos como, por exemplo, a monitorização eletrónica da utilização da Internet, do correio eletrónico ou do telefone pelos trabalhadores, ou a videovigilância dos trabalhadores, constituem mais claramente um tipo de tratamento suscetível de ultrapassar o que é necessário para a execução de um contrato de trabalho, embora também nestes casos tal possa depender da natureza das funções laborais. A prevenção da fraude – que pode incluir, entre outros, a monitorização e a elaboração de perfis de clientes – é outra área característica, na qual existe a probabilidade de se considerar que o tratamento ultrapassa o que é necessário para a execução de um contrato. Contudo, tal tratamento pode, ainda assim, ser legítimo com base noutro fundamento previsto no artigo 7.º, por exemplo, o consentimento, sempre que adequado, uma obrigação legal ou o interesse legítimo do responsável pelo tratamento (artigo 7.º, alíneas a), c) ou f))³⁵. Neste último caso, o tratamento deve ficar sujeito a garantias e medidas complementares para proteger adequadamente os interesses ou os direitos e liberdades das pessoas em causa.

O artigo 7.º, alínea b), é aplicável apenas ao que for necessário para a *execução* de um contrato. Não é aplicável a nenhuma ação subsequente desencadeada por incumprimento nem a nenhum outro incidente na execução de um contrato. Desde que o tratamento abarque a execução normal de um contrato, pode ser abrangido pelo âmbito de aplicação do artigo 7.º, alínea b). Se, na execução de um contrato, ocorrer

³⁵ Outro exemplo de múltiplos fundamentos jurídicos consta do Parecer 15/2011 do Grupo de Trabalho sobre a definição de consentimento (referido na nota 2). Na aquisição de um automóvel, o responsável pelo tratamento dos dados pode proceder ao tratamento de dados pessoais com diferentes finalidades e com base em diversos fundamentos:

- dados necessários para comprar o automóvel: artigo 7.º, alínea b),
- para tratar dos documentos do automóvel: artigo 7.º, alínea c),
- para serviços de gestão de clientes (por exemplo, para que o automóvel seja assistido noutras filiais na UE): artigo 7.º, alínea f),
- para transferir os dados a terceiros para as suas próprias atividades de comercialização: artigo 7.º, alínea a).

um incidente que origine um conflito, o tratamento de dados pode tomar um rumo diferente. O tratamento de informações básicas relativas à pessoa em causa, tais como o nome, o endereço e a referência a obrigações contratuais ainda em vigor, que possibilitem o envio de avisos oficiais, deve continuar a ser considerado abrangido pelo tratamento de dados necessário para a execução de um contrato. Quanto ao tratamento de dados mais elaborado, que pode ou não envolver terceiros, como a cobrança de dívidas externa ou a propositura de uma ação contra um cliente que não tenha pago um serviço, pode argumentar-se que tal tratamento já não se enquadra na execução «normal» do contrato, pelo que não é abrangido pelo âmbito de aplicação do artigo 7.º, alínea b). No entanto, este facto, por si só, não torna o tratamento ilegítimo: o responsável pelo tratamento tem um interesse legítimo em utilizar os meios judiciais necessários para assegurar que os seus direitos contratuais sejam respeitados. Outros fundamentos jurídicos, como, por exemplo, o artigo 7.º, alínea f), podem ser invocados, sob reserva de garantias e medidas adequadas e do respeito pelo teste da ponderação³⁶.

- ii) Em segundo lugar, o artigo 7.º, alínea b), abrange igualmente o tratamento que *preceda* a celebração de um contrato. Tal abrange as relações pré-contratuais, desde que a negociação ocorra a pedido da pessoa em causa, e não por iniciativa do responsável pelo tratamento ou de terceiros. Por exemplo, se uma pessoa pedir a um retalhista que lhe envie uma oferta relativa a um produto, o tratamento necessário para esse fim, como, por exemplo, a conservação dos dados relativos ao endereço e das informações sobre o que foi pedido, durante um período limitado, será adequado à luz deste fundamento jurídico. De igual modo, se uma pessoa solicitar a uma seguradora uma proposta de seguro automóvel, a seguradora pode tratar os dados necessários, por exemplo, relativos à origem e à idade do automóvel, e outros dados relevantes e proporcionados, de forma a preparar a proposta.

No entanto, a verificação pormenorizada de antecedentes, por exemplo, o tratamento de dados relativos a exames médicos antes de uma seguradora disponibilizar um seguro de saúde ou um seguro de vida a um requerente, não é considerada uma medida necessária, tomada a pedido da pessoa em causa. A verificação de referências de

³⁶ No que respeita a certas categorias específicas de dados, pode ser necessário ter igualmente em conta o artigo 8.º, n.º 1, alínea e) - «necessário à declaração, ao exercício ou à defesa de um direito num processo judicial».

crédito antes da concessão de um empréstimo também não é efetuada a *pedido* da pessoa em causa nos termos do artigo 7.º, alínea b), mas sim nos termos do artigo 7.º, alínea f), ou nos termos do artigo 7.º, alínea c), em cumprimento de uma obrigação legal, por parte dos bancos, de consultar uma lista oficial de devedores registados.

O marketing direto por iniciativa do retalhista/responsável pelo tratamento também não será possível com base neste fundamento. Nalguns casos, o artigo 7.º, alínea f), pode proporcionar um fundamento jurídico adequado, em vez do artigo 7.º, alínea b), sob reserva de garantias e medidas adequadas e do respeito pelo teste da ponderação. Noutros casos, incluindo os que impliquem a criação de perfis muito completos, o intercâmbio de dados, o marketing direto em linha ou a publicidade comportamental, deve ter-se em conta o consentimento nos termos do artigo 7.º, alínea a), como decorre da análise *infra*³⁷.

III.2.3. Obrigação legal

O artigo 7.º, alínea c), proporciona um fundamento jurídico se «[o] tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito». Tal pode ser o caso, por exemplo, quando os empregadores tenham de fornecer à segurança social ou às autoridades fiscais dados relativos aos salários dos seus trabalhadores, ou quando instituições financeiras sejam obrigadas a denunciar determinadas transações suspeitas às autoridades competentes nos termos das normas em matéria de luta contra o branqueamento de capitais. Pode igualmente tratar-se de uma obrigação à qual uma autoridade pública esteja sujeita, uma vez que nada limita a aplicação do artigo 7.º, alínea c), ao setor privado ou ao setor público. Tal aplica-se, por exemplo, à recolha de dados por uma autarquia local para o tratamento de multas de estacionamento em locais proibidos.

O artigo 7.º, alínea c), apresenta semelhanças com o artigo 7.º, alínea e), uma vez que uma missão de interesse público se baseia muitas vezes, ou tem origem, numa disposição legal. No entanto, o âmbito de aplicação do artigo 7.º, alínea c), está rigorosamente delimitado.

³⁷ Ver a secção III.3.6, alínea b), sob a epígrafe «*Ilustração: evolução na abordagem ao marketing direto*» nas páginas 45-46.

Para o artigo 7.º, alínea c), ser aplicável, a obrigação deve ser imposta por lei (e não, por exemplo, por acordo contratual). A lei deve preencher todas as condições pertinentes para que a obrigação seja válida e vinculativa, e deve igualmente respeitar a legislação em matéria de proteção de dados, incluindo o requisito da necessidade, da proporcionalidade³⁸ e da limitação da finalidade.

É igualmente importante realçar que o artigo 7.º, alínea c), remete para a legislação da União Europeia ou de um Estado-Membro. As obrigações decorrentes da legislação de países terceiros (tais como, por exemplo, a obrigação de instituir sistemas de denúncia de infrações nos termos da Lei Sarbanes–Oxley, de 2002, nos Estados- Unidos) não são abrangidas por este fundamento. Para ser válida, uma obrigação legal de um país terceiro necessita de ser oficialmente reconhecida e integrada na ordem jurídica do Estado-Membro em causa, por exemplo, através de um acordo internacional³⁹. Por outro lado, a necessidade de cumprir uma obrigação estrangeira pode representar um interesse legítimo do responsável pelo tratamento, mas apenas sob reserva da aplicação do teste da ponderação previsto no artigo 7.º, alínea f), e desde que sejam instituídas garantias adequadas, tais como as aprovadas pela autoridade responsável pela proteção de dados competente.

O cumprimento ou não da obrigação não pode ficar ao critério do responsável pelo tratamento. Por conseguinte, os compromissos voluntários unilaterais e as parcerias público-privadas que envolvam o tratamento de dados para além do que é exigido legalmente não são abrangidos pelo âmbito de aplicação do artigo 7.º, alínea c). Por exemplo, se um fornecedor de serviços de Internet decidir monitorizar os utilizadores desses serviços como forma de combater os descarregamentos ilegais em linha – sem ter a obrigação clara e expressa de o fazer – o artigo 7.º, alínea c), não será um fundamento jurídico adequado para o efeito.

Acresce que a própria obrigação legal deve ser suficientemente clara quanto ao tratamento dos dados pessoais que exige. Por conseguinte, o artigo 7.º, alínea c), é aplicável com base em

³⁸Ver igualmente o Parecer 1/2014 do Grupo de Trabalho sobre a aplicação dos conceitos de necessidade e proporcionalidade e a proteção de dados no setor da aplicação coerciva da lei, adotado em 27.2.2014 (WP211).

³⁹Ver, quanto a esta questão, a secção 4.2.2 do Parecer 10/2006 do Grupo de Trabalho sobre o tratamento de dados pessoais pela Sociedade das Telecomunicações Financeiras Interbancárias no Mundo (Worldwide Interbank Financial Telecommunication - SWIFT), adotado em 20.11.2006 (WP128) e o Parecer 1/2006 do Grupo de Trabalho sobre a aplicação das regras europeias em matéria de proteção de dados aos sistemas internos de denúncia de infrações nos domínios da contabilidade, dos controlos contabilísticos internos, da auditoria, da luta contra a corrupção e do crime bancário e financeiro, adotado em 1.2.2006 (WP117).

disposições legais que refiram expressamente a natureza e o objeto do tratamento. O responsável pelo tratamento não deve dispor de um grau de discricionariedade indevido quanto à forma de cumprir a obrigação legal.

Nalguns casos, a legislação pode estabelecer apenas um objetivo geral, enquanto que as obrigações mais específicas são impostas a outro nível, por exemplo, em normas regulamentares ou através de uma decisão vinculativa de uma autoridade pública num caso concreto. Daí podem resultar obrigações legais nos termos do artigo 7.º, alínea c), desde que a natureza e o objeto do tratamento estejam bem definidos e sob reserva de uma base jurídica adequada.

No entanto, o mesmo não acontece se uma autoridade reguladora apenas fornecer orientações políticas gerais e estabelecer as condições nas quais admite fazer uso das suas competências de execução (por exemplo, orientações regulamentares para instituições financeiras sobre determinadas normas de devida diligência). Nestes casos, as atividades de tratamento devem ser apreciadas nos termos do artigo 7.º, alínea f), e só devem ser consideradas legítimas sob reserva da aplicação do teste da ponderação complementar⁴⁰.

Como observação geral, há que referir que pode parecer que algumas atividades de tratamento se aproximam do âmbito de aplicação do artigo 7.º, alínea c), ou do artigo 7.º, alínea b), mas não cumprem integralmente os critérios de aplicação destes fundamentos. Tal não significa que esse tratamento seja sempre necessariamente ilícito: em certos casos, pode ser legítimo, mas é-o nos termos do artigo 7.º, alínea f), sob reserva da aplicação do teste da ponderação complementar.

⁴⁰As orientações de uma entidade reguladora podem ainda desempenhar um papel importante na apreciação do interesse legítimo do responsável pelo tratamento (ver a secção III.3.4, alínea a), nomeadamente na página 36).

III.2.4. Interesse vital

O artigo 7.º, alínea d), proporciona um fundamento jurídico se «[o] tratamento for necessário para a proteção de interesses vitais da pessoa em causa». Esta redação difere da linguagem utilizada no artigo 8.º, n.º 2, alínea c), que é mais específico e que é aplicável se «[o] tratamento for necessário para proteger interesses vitais da pessoa em causa ou de uma outra pessoa se a pessoa em causa estiver física ou legalmente incapaz de dar o seu consentimento».

Todavia, ambas as disposições parecem indicar que este fundamento jurídico deve ter uma aplicação limitada. Em primeiro lugar, a expressão «interesse vital» parece limitar a aplicação deste fundamento a questões de vida ou morte ou, no mínimo, a ameaças que acarretam um risco de lesão ou de outros danos para a saúde da pessoa em causa (ou, no caso do artigo 8.º, n.º 2, alínea c), de uma outra pessoa).

O considerando 31 confirma que o objetivo deste fundamento jurídico é «proteger um interesse essencial à vida da pessoa em causa». No entanto, a diretiva não esclarece exatamente se a ameaça deve ser imediata. Tal suscita questões relativamente ao alcance da recolha de dados, nomeadamente como medida preventiva ou em larga escala, como, por exemplo, a recolha de dados de passageiros de uma companhia aérea quando tenha sido detetado um risco de doença epidemiológica ou um problema de segurança.

O Grupo de Trabalho considera que esta disposição deve ser interpretada de forma restritiva e coerente com o espírito do artigo 8.º. Embora o artigo 7.º, alínea d), não limite expressamente a utilização deste fundamento a situações nas quais o consentimento não possa ser utilizado como fundamento jurídico pelas razões especificadas no artigo 8.º, n.º 2, alínea c), é razoável presumir que, em situações nas quais exista a possibilidade e a necessidade de obter um consentimento válido, deve, de facto, procurar-se obter o consentimento, sempre que tal seja viável. Tal limita igualmente a aplicação desta disposição a uma análise casuística, não podendo, por norma, ser utilizada para legitimar qualquer recolha ou tratamento massivos de dados pessoais. Caso estes sejam necessários, o artigo 7.º, alíneas c) ou e), constituem fundamentos mais adequados para o tratamento.

III.2.5. Missão pública

O artigo 7.º, alínea e), proporciona um fundamento jurídico se «[o] tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados».

É importante observar que, tal como o artigo 7.º, alínea c), o artigo 7.º, alínea e), refere-se ao interesse público da União Europeia ou de um Estado-Membro. De igual modo, a expressão «autoridade pública» refere-se a uma autoridade reconhecida pela União Europeia ou por um Estado-Membro. Por outras palavras, as missões levadas a cabo no interesse público de um país terceiro ou no exercício de uma autoridade pública legitimada por normas de direito estrangeiro não são abrangidas por esta disposição⁴¹.

O artigo 7.º, alínea e), abrange dois tipos de situações e é relevante tanto para o setor público como para o setor privado. Em primeiro lugar, abrange as situações nas quais o próprio responsável pelo tratamento tenha sido investido de autoridade pública ou de uma missão de interesse público (mas não necessariamente também de uma obrigação legal de tratar dados) e o tratamento seja necessário para o exercício dessa autoridade ou a execução dessa missão. Por exemplo, uma autoridade tributária pode recolher e tratar os dados relativos à declaração fiscal de uma pessoa para determinar e verificar o valor do imposto a pagar. Uma associação profissional, como uma ordem dos advogados ou uma ordem dos médicos, investida de autoridade pública para tal, pode levar a cabo procedimentos disciplinares contra alguns dos seus membros. Outro exemplo possível é o de um órgão de poder local, como uma autoridade municipal, que tenha por missão administrar uma biblioteca, uma escola ou uma piscina local.

Em segundo lugar, o artigo 7.º, alínea e), abrange igualmente as situações nas quais o responsável pelo tratamento não tenha sido investido de autoridade pública, mas lhe seja solicitada a comunicação de dados por um terceiro investido de tal autoridade. Por exemplo, um funcionário de um órgão público competente para investigar crimes pode solicitar ao responsável pelo tratamento que coopere numa investigação em curso, em vez de lhe ordenar

⁴¹ Ver a secção 2.4 do Documento de trabalho sobre uma interpretação comum do n.º 1 do artigo 26.º da Diretiva 95/46/CE de 24 de outubro de 1995, adotado pelo Grupo de Trabalho em 25 de novembro de 2005 (WP114), no que respeita a uma interpretação semelhante do conceito de «proteção de um interesse público importante», referido no artigo 26.º, n.º 1, alínea d).

que satisfaça um pedido específico de cooperação. Além disso, o artigo 7.º, alínea e), pode abranger as situações nas quais o responsável pelo tratamento comunique, de forma proactiva, dados a um terceiro investido de tal autoridade pública. Tal pode acontecer, por exemplo, no caso de um responsável pelo tratamento se aperceber de que foi cometido um crime e facultar essa informação às autoridades competentes por iniciativa própria.

Ao contrário do que se verificava no caso do artigo 7.º, alínea c), não existe qualquer exigência de que o responsável pelo tratamento atue por força de uma obrigação legal. Utilizando o exemplo anterior, um responsável pelo tratamento que acidentalmente se aperceba de que foi cometido um roubo ou uma fraude pode não estar legalmente obrigado a reportar esse facto à polícia mas, no entanto, nos casos que o justifiquem, pode fazê-lo voluntariamente com base no artigo 7.º, alínea e).

Contudo, o tratamento deve ser «necessário para a execução de uma missão de interesse público». Em alternativa, o responsável pelo tratamento ou o terceiro a quem o responsável pelo tratamento comunica os dados deve estar investido de autoridade pública e o tratamento de dados deve ser necessário para o exercício dessa autoridade⁴². É igualmente importante realçar que, por norma, essa autoridade pública ou missão pública, é atribuída por ato legislativo ou outro tipo de regulamentação legal. Se o tratamento implicar uma violação da privacidade, ou se tal for de outro modo exigido pelo direito nacional para garantir a proteção das pessoas em causa, a base jurídica deve estabelecer, de forma suficientemente específica e precisa, o tipo de tratamento de dados que pode ser autorizado.

Estas situações estão a tornar-se cada vez mais comuns, também fora dos limites do setor público, tendo em conta a tendência para concessionar serviços públicos a entidades do setor privado. Tal pode acontecer, por exemplo, no contexto das atividades de tratamento de dados nos setores dos transportes e da saúde (por exemplo, estudos epidemiológicos, investigação). Este fundamento pode ser igualmente invocado num contexto de aplicação da lei, como já foi indicado nos exemplos anteriores. No entanto, a questão de saber em que medida uma empresa privada pode ser autorizada a cooperar com as autoridades responsáveis pela aplicação da lei, por exemplo na luta contra a fraude ou os conteúdos ilegais na Internet, exige

⁴²Por outras palavras, nestes casos, a relevância pública das funções e a correspondente responsabilidade continuarão a existir, ainda que a execução da missão tenha sido delegada noutras entidades, incluindo entidades privadas.

uma análise não apenas nos termos do artigo 7.º mas igualmente nos termos do artigo 6.º, tendo em conta os requisitos da limitação da finalidade, da licitude e da lealdade⁴³.

O artigo 7.º, alínea e), tem potencialmente um âmbito de aplicação muito amplo, que requer uma interpretação estrita e a uma identificação clara, caso a caso, do interesse público em jogo e da autoridade pública que justifica o tratamento. Este âmbito de aplicação amplo justifica igualmente que, tal como acontece relativamente ao artigo 7.º, alínea f), o artigo 14.º preveja um direito de oposição quando o tratamento se baseie no artigo 7.º, alínea e)⁴⁴. Por conseguinte, em ambos os casos, podem ser aplicadas garantias e medidas complementares semelhantes⁴⁵.

Nesse sentido, o artigo 7.º, alínea e), tem semelhanças com o artigo 7.º, alínea f), e, nalguns contextos, em especial no que respeita às autoridades públicas, o artigo 7.º, alínea e), pode substituir o artigo 7.º, alínea f).

Na apreciação do âmbito de aplicação destas disposições aos órgãos do setor público, em especial à luz das alterações propostas ao quadro jurídico em matéria de proteção de dados, é útil observar que do texto atual do Regulamento 45/2001⁴⁶, que contém as normas em matéria de proteção de dados aplicáveis às instituições e aos órgãos da União Europeia, não consta nenhuma disposição comparável com o artigo 7.º, alínea f).

No entanto, o considerando 27 do referido regulamento dispõe que «o tratamento de dados pessoais para o desempenho de funções *de interesse público* pelas instituições e órgãos comunitários inclui o tratamento de dados pessoais indispensáveis à gestão e ao funcionamento dessas instituições e órgãos». Por conseguinte, esta disposição permite o tratamento de dados com base num fundamento de «missão pública», em sentido lato, numa grande variedade de casos que de outro modo poderiam ser abrangidos por uma disposição

⁴³Ver, nesse sentido, o parecer do Grupo de Trabalho sobre a SWIFT (já referido na nota 39), o Parecer 4/2003 do Grupo de Trabalho sobre o nível de proteção conferido pelos EUA à transferência de dados dos passageiros, adotado em 13.6.2003 (WP78) e o Documento de trabalho sobre questões de proteção de dados relacionadas com os direitos de propriedade intelectual, adotado em 18.1.2005 (WP104).

⁴⁴Tal como já foi referido, nalguns Estados-Membros (por exemplo, na Suécia) não existe esta possibilidade de apresentar oposição no que respeita ao tratamento de dados baseado no artigo 7.º, alínea e).

⁴⁵Como se verá adiante, o projeto de relatório da Comissão LIBE propôs um aumento das garantias – em especial, maior transparência – quando o artigo 7.º, alínea f), seja aplicável.

⁴⁶Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho de 18 de dezembro de 2000 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).

semelhante ao artigo 7.º, alínea f). A videovigilância de instalações para fins de segurança, a monitorização do tráfego de correio eletrónico ou as avaliações do pessoal são apenas alguns exemplos do que se pode enquadrar nesta disposição relativa ao «desempenho de funções de interesse público», interpretada em sentido lato.

Em relação ao futuro, é igualmente importante ter em conta que a proposta de regulamento prevê expressamente, no artigo 6.º, n.º 1, alínea f), que o fundamento relativo ao interesse legítimo «não se aplica ao tratamento de dados efetuado por autoridades públicas no exercício das suas funções». Se esta disposição for adotada e vier a ser interpretada em sentido lato, de forma a excluir totalmente a utilização, pelas autoridades públicas, do interesse legítimo como fundamento jurídico, torna-se necessário interpretar os fundamentos relativos ao «interesse público» e à «autoridade pública» previstos no artigo 7.º, alínea e), de forma a permitir às autoridades públicas alguma flexibilidade, pelo menos para garantir a sua gestão e o seu funcionamento adequados, tal como o Regulamento 45/2001 é atualmente interpretado.

Em alternativa, a referida última frase do artigo 6.º, n.º 1, alínea f), da proposta de regulamento pode ser interpretada de forma a não excluir totalmente a utilização, pelas autoridades públicas, do interesse legítimo como fundamento jurídico. Neste caso, a expressão «tratamento de dados efetuado por autoridades públicas no exercício das suas funções», constante do proposto artigo 6.º, n.º 1, alínea f), deve ser interpretada em sentido estrito. Esta interpretação em sentido estrito significa que o tratamento necessário para a gestão e o funcionamento adequados dessas autoridades públicas não é abrangido pelo âmbito do «tratamento de dados efetuado por autoridades públicas no exercício das suas funções». Em consequência, o tratamento necessário para a gestão e o funcionamento adequados dessas autoridades públicas pode ainda ser possível com base no fundamento relativo ao interesse legítimo.

III.3. Artigo 7.º, alínea f): interesses legítimos

O artigo 7.º, alínea f),⁴⁷ requer a realização de um teste da ponderação: os interesses legítimos do responsável pelo tratamento (ou de terceiros) devem ser ponderados em relação aos

⁴⁷Para consultar o texto completo do artigo 7.º, alínea f), ver a página 4 supra.

interesses ou aos direitos e liberdades fundamentais da pessoa em causa. O resultado do teste da ponderação determina, em grande medida, se o artigo 7.º, alínea f), pode ser invocado como fundamento jurídico para o tratamento.

Vale a pena referir, desde já, que não se trata de um teste da ponderação simples, que consiste apenas em ponderar dois «valores» facilmente quantificáveis e facilmente comparáveis em relação um ao outro. Pelo contrário, como adiante se descreverá mais pormenorizadamente, aplicar o teste da ponderação pode exigir uma avaliação complexa que tenha em conta vários fatores. Para ajudar a estruturar e a simplificar a avaliação, dividimos o processo em várias fases, de forma a assegurar que o teste da ponderação possa ser realizado de forma eficaz.

Em primeiro lugar, a secção III.3.1 analisa um dos lados a ponderar: o que constitui «interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados». Na secção III.3.2, analisamos o outro lado a ponderar: o que constitui «interesses ou [...] direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do n.º 1 do artigo 1.º».

Nas secções III.3.3 e III.3.4, são fornecidas orientações sobre como realizar o teste da ponderação. A secção III.3.3 apresenta uma introdução geral, recorrendo a três cenários diferentes. Após esta introdução, a secção III.3.4 sublinha os aspetos mais importantes que devem ser tidos em conta na realização do teste da ponderação, incluindo as garantias e as medidas previstas pelo responsável pelo tratamento dos dados.

Por último, nas secções III.3.5 e III.3.6, analisaremos igualmente alguns mecanismos em especial, tais como a responsabilidade, a transparência e o direito de oposição, que podem ajudar a garantir – e a reforçar – um equilíbrio adequado entre os vários interesses em jogo.

III.3.1. Interesses legítimos do responsável pelo tratamento (ou de terceiros)

Conceito de «interesse»

O conceito de «interesse» está estreitamente relacionado com o conceito de «finalidade» referido no artigo 6.º da diretiva, embora se trate de conceitos distintos. Em matéria de

proteção de dados, a «finalidade» é a razão específica pela qual os dados são tratados: o objetivo ou a intenção do tratamento de dados. Por outro lado, um interesse é o objetivo mais abrangente que o responsável pelo tratamento pode ter no tratamento, ou o benefício que o responsável pelo tratamento retira – ou que a sociedade pode retirar – do tratamento.

Por exemplo, uma empresa pode ter um *interesse* em garantir a saúde e a segurança do seu pessoal que trabalha na sua unidade de produção de energia nuclear. Neste sentido, a empresa pode ter como *finalidade* a implementação de procedimentos específicos de controlo de acessos que justifique o tratamento de determinados dados pessoais definidos como forma de garantir a saúde e a segurança do pessoal.

Um interesse deve ser definido de forma suficientemente clara para permitir a realização do teste da ponderação em relação aos interesses e aos direitos fundamentais da pessoa em causa. Além disso, o interesse em jogo deve ser igualmente «do responsável pelo tratamento». Tal exige que se trate de um interesse real e atual, algo que corresponda a atividades atuais ou a benefícios esperados num futuro muito próximo. Por outras palavras, os interesses que sejam demasiado vagos ou especulativos não serão suficientes.

A natureza do interesse pode variar. Alguns interesses podem ser preponderantes e benéficos para a sociedade em geral, tal como o interesse da imprensa em publicar informações sobre corrupção governamental ou o interesse em desenvolver investigações científicas (sob reserva de garantias adequadas). Outros interesses podem ser menos prementes para a sociedade em geral ou, pelo menos, o impacto da sua prossecução na sociedade pode ser mais variável ou controverso. Tal pode ser o caso, por exemplo, do interesse económico de uma empresa em ter a maior quantidade possível de informação sobre os seus potenciais clientes para poder direcionar melhor a publicidade relativa aos seus produtos ou serviços.

O que torna um interesse «legítimo» ou «ilegítimo»?

O objetivo desta questão é identificar o limiar daquilo que constitui um interesse legítimo. Se o interesse do responsável pelo tratamento dos dados for ilegítimo, o teste da ponderação não terá lugar, uma vez que o limiar inicial para a utilização do artigo 7.º, alínea f), não será atingido.

Na opinião do Grupo de Trabalho, o conceito de interesse legítimo pode incluir um vasto leque de interesses, sejam eles triviais ou muito preponderantes, simples ou mais controversos. Por conseguinte, só num segundo momento, quando se trate de ponderar esses interesses em relação aos interesses e aos direitos fundamentais da pessoa em causa, deve ser adotada uma abordagem mais restrita e uma análise mais substancial.

Segue-se uma lista não exaustiva de alguns contextos mais comuns nos quais a questão do interesse legítimo na aceção do artigo 7.º, alínea f), pode ser suscitada. Esta lista é aqui apresentada sem prejuízo da questão de saber se os interesses do responsável pelo tratamento acabarão por prevalecer sobre os interesses e os direitos da pessoa em causa quando seja realizado o teste da ponderação.

- Exercício do direito à liberdade de expressão ou de informação, nomeadamente nos meios de comunicação social e nas artes.
- Marketing direto convencional e outras formas de marketing ou de publicidade.
- Mensagens não comerciais não solicitadas, nomeadamente relativas a campanhas políticas ou a atividades de angariação de fundos para fins de beneficência.
- Execução de créditos, incluindo cobrança de dívidas através de processos não judiciais.
- Prevenção da fraude, utilização abusiva de serviços ou branqueamento de capitais.
- Monitorização da atividade dos trabalhadores para fins de segurança ou de gestão.
- Sistemas de denúncia.
- Segurança física, tecnologias de informação e segurança das redes.
- Tratamento para fins históricos, científicos ou estatísticos.
- Tratamento para fins de investigação (nomeadamente pesquisas de mercado)

Por conseguinte, um interesse pode ser considerado legítimo desde que o responsável pelo tratamento possa prosseguir esse interesse em conformidade com a legislação em matéria de proteção de dados e a demais legislação aplicável. Por outras palavras, um interesse legítimo deve ser «admissível nos termos da lei»⁴⁸.

⁴⁸As observações acerca da natureza da «legitimidade» constantes da secção III.1.3 do Parecer 3/2013 do Grupo de Trabalho sobre a limitação da finalidade (já referido na nota 9) aplicam-se, *mutatis mutandis*, igualmente aqui. Tal como consta das páginas 19 e 20 desse parecer, o conceito de «lei» é aqui utilizado no sentido mais lato. Tal inclui a demais legislação aplicável, designadamente em matéria de trabalho, de contratos ou de defesa

Assim, para efeitos da aplicação do artigo 7.º, alínea f), um «interesse legítimo» deve:

- ser lícito (ou seja, deve respeitar o direito da UE e o direito nacional aplicáveis),
- ser definido de forma suficientemente clara para permitir a realização do teste da ponderação em relação aos interesses e aos direitos fundamentais da pessoa em causa (ou seja, deve ser suficientemente específico),
- representar um interesse real e atual (ou seja, não deve ser especulativo).

O facto de o responsável pelo tratamento ter tal interesse legítimo no tratamento de determinados dados não significa necessariamente que possa invocar o artigo 7.º, alínea f), como fundamento jurídico para o tratamento. A legitimidade do interesse do responsável pelo tratamento dos dados é apenas um ponto de partida, um dos elementos que necessitam de ser analisados nos termos do artigo 7.º, alínea f). A questão de saber se o artigo 7.º, alínea f), pode ser invocado dependerá do resultado do teste da ponderação subsequente.

A título ilustrativo: os responsáveis pelo tratamento podem ter um interesse legítimo em conhecer as preferências dos respetivos clientes para poderem personalizar melhor as suas ofertas e, em última análise, disponibilizar produtos e serviços que satisfaçam melhor as necessidades e os desejos dos clientes. Nesta perspetiva, o artigo 7.º, alínea f), pode ser um fundamento jurídico adequado para ser utilizado no que respeita a algumas atividades de marketing, em linha ou sem ser em linha, desde que sejam instituídas garantias adequadas (incluindo, entre outros, um mecanismo viável que permita exercer o direito de oposição nos termos do artigo 14.º, alínea b), como se verá na secção III.3.6, *Direito de oposição e outros*).

No entanto, tal não significa que os responsáveis pelo tratamento possam invocar o artigo 7.º, alínea f), para monitorizar indevidamente as atividades, em linha ou sem ser em linha, dos

dos consumidores. Além disso, o conceito de lei «inclui todas as formas de direito escrito ou consuetudinário, legislação primária ou derivada, decretos municipais, precedentes judiciais, princípios constitucionais, direitos fundamentais, outros princípios jurídicos, bem como jurisprudência, na medida em que essa ‘lei’ seja interpretada e tida em conta pelos tribunais competentes. Nos limites da lei, para determinar se uma certa finalidade é legítima, poderão ser tidos em conta outros elementos, tais como costumes, códigos de conduta, códigos deontológicos, contratos, bem como o contexto geral e os factos do processo. Tal incluirá natureza da relação subjacente entre o responsável pelo tratamento e as pessoas em causa, seja ela comercial ou outra». Além disso, o que pode ser considerado um interesse legítimo «pode também sofrer alterações ao longo do tempo, em consequência de desenvolvimentos científicos e tecnológicos e de mudanças na sociedade e nas atitudes culturais».

respetivos clientes, combinar grandes volumes de dados respeitantes aos clientes, provenientes de diferentes fontes e recolhidos inicialmente noutros contextos e para outros fins, e criar – e, por exemplo, por intermédio de corretores de dados, também comercializar – perfis complexos das personalidades e das preferências dos clientes sem que estes tenham conhecimento, disponham de um mecanismo viável que lhes permita exercer o direito de oposição, sem falar do seu consentimento informado. Tal atividade de elaboração de perfis é suscetível de representar uma intromissão significativa na vida privada do cliente, e quando assim seja, os interesses e os direitos da pessoa em causa prevalecem sobre o interesse do responsável pelo tratamento⁴⁹.

Outro exemplo: no seu Parecer sobre a SWIFT⁵⁰, o Grupo de Trabalho, embora tenha reconhecido que a empresa tinha um interesse legítimo em cumprir as intimações previstas na legislação dos EUA, para evitar o risco de ser sancionada pelas autoridades dos EUA, concluiu que o artigo 7.º, alínea f), não podia ser invocado. O Grupo de Trabalho considerou, em especial, que, tendo em conta as consequências muito importantes para as pessoas do tratamento de dados efetuado de forma «oculta, sistemática, maciça e a longo prazo», «os interesses das muitas pessoas em causa em termos de direitos e liberdades fundamentais prevalecem em relação ao interesse da SWIFT em não ser sancionada pelos EUA por eventual incumprimento das intimações».

Como se verá adiante, se o interesse prosseguido pelo responsável pelo tratamento não for preponderante, os interesses e os direitos da pessoa em causa são mais suscetíveis de prevalecer sobre os interesses legítimos – mas menos significativos - do responsável pelo tratamento. Ao mesmo tempo, tal não significa que os interesses menos preponderantes do responsável pelo tratamento não possam, por vezes, prevalecer sobre os interesses e os direitos das pessoas em causa: é o que acontece, por norma, quando o impacto do tratamento nas pessoas em causa é também menos significativo.

Interesse legítimo no setor público

⁴⁹ A questão das tecnologias de rastreamento e o papel do consentimento nos termos do artigo 5.º, n.º 3, da «privacidade e comunicações eletrónicas» serão analisados separadamente. Ver a secção III.3.6, alínea b), sob a epígrafe «*Ilustração: evolução na abordagem ao marketing direto*».

⁵⁰ Ver a secção 4.2.3 do parecer já referido na nota 39. Neste caso, o interesse legítimo do responsável pelo tratamento estava igualmente associado ao interesse público de um país terceiro, o qual não era abrangido pelo âmbito de aplicação da Diretiva 95/46/CE.

O texto atual da diretiva não exclui especificamente a utilização, pelos responsáveis pelo tratamento que sejam autoridades públicas, do artigo 7.º, alínea f), como fundamento para o tratamento⁵¹.

No entanto, a proposta de regulamento⁵² exclui esta possibilidade no que respeita ao «tratamento de dados efetuado por autoridades públicas no exercício das suas funções».

A alteração legislativa proposta realça a importância do princípio geral de que, por norma, as autoridades públicas devem proceder ao tratamento de dados no exercício das suas funções apenas se estiverem devida e legalmente autorizadas a fazê-lo. A observância deste princípio é especialmente importante – e claramente exigida pela jurisprudência do Tribunal Europeu dos Direitos do Homem – nos casos em que a privacidade das pessoas em causa esteja em jogo e em que as atividades da autoridade pública afetem essa privacidade.

Consequentemente, quando o tratamento pelas autoridades públicas afete a privacidade das pessoas em causa é exigida - também nos termos da atual diretiva - uma autorização legal suficientemente *pormenorizada e específica*. Pode tratar-se de uma obrigação legal específica de tratar dados, que respeite o disposto no artigo 7.º, alínea c), ou de uma autorização específica (mas não necessariamente uma obrigação) para tratar dados, que cumpra os requisitos previstos no artigo 7.º, alínea e) ou alínea f)⁵³.

Interesses legítimos de terceiros

O texto atual da diretiva não se refere apenas à prossecução dos «interesses legítimos do responsável pelo tratamento» mas permite igualmente que o artigo 7.º, alínea f), seja utilizado para prosseguir interesses legítimos «do terceiro ou terceiros a quem os dados sejam

⁵¹ Originalmente, o âmbito de aplicação da primeira proposta de diretiva da Comissão abrangia separadamente o tratamento de dados no setor privado e as atividades de tratamento do setor público. Esta distinção formal entre as normas aplicáveis ao setor público e ao setor privado desapareceu na proposta alterada. Tal pode ter conduzido igualmente a diferenças na interpretação e na aplicação pelos vários Estados-Membros.

⁵² Ver o artigo 6.º, n.º 1, alínea f), da proposta de regulamento.

⁵³ A este respeito, ver igualmente a secção III.2.5 supra, relativa às funções públicas (páginas 21 a 23), bem como as considerações infra, sob a epígrafe *Interesses legítimos de terceiros* (nas páginas 27 e 28). Ver igualmente as reflexões sobre os limites à «aplicação privada» da lei, na página 35, sob a epígrafe «Interesses públicos/interesses da comunidade em geral». Em todas estas situações, é especialmente importante assegurar que os limites previstos no artigo 7.º, alínea f), e no artigo 7.º, alínea e), sejam plenamente respeitados.

comunicados»⁵⁴. Os exemplos que se seguem ilustram alguns contextos nos quais esta disposição pode ser aplicada.

Publicação de dados para fins de transparência e de responsabilidade. Um contexto importante no qual o artigo 7.º, alínea f), pode ser relevante é o da publicação de dados para fins de transparência e de responsabilidade (por exemplo, os salários dos quadros superiores de uma sociedade). Neste caso, pode considerar-se que a divulgação pública é efetuada, acima de tudo, não no interesse do responsável pelo tratamento que publica os dados mas sim no interesse de outros interessados, tais como os trabalhadores, os jornalistas ou o público em geral, a quem os dados são comunicados.

Do ponto de vista da proteção de dados e da privacidade, e para garantir a segurança jurídica, é aconselhável, em geral, que os dados pessoais sejam divulgados publicamente com base numa lei que o permita e – se necessário – que especifique, de forma clara, quais os dados a publicar, a finalidade da publicação e as garantias eventualmente necessárias⁵⁵. Tal significa igualmente que pode ser preferível utilizar como base jurídica o artigo 7.º, alínea c), em vez do artigo 7.º, alínea f), quando sejam divulgados dados pessoais para fins de transparência e de responsabilidade⁵⁶.

No entanto, na falta de uma obrigação ou permissão legal específica para publicar dados, deve ser possível, ainda assim, comunicar dados pessoais às partes interessadas pertinentes. Nos casos adequados, deve ser igualmente possível publicar dados pessoais para fins de transparência e de responsabilidade.

⁵⁴A proposta de regulamento visa limitar a utilização deste fundamento à prossecução dos «interesses legítimos do responsável pelo tratamento». Não resulta claro do texto, por si só, se a redação proposta constitui apenas uma simplificação do texto ou se tem como objetivo excluir as situações em que um responsável pelo tratamento possa comunicar dados no interesse legítimo de terceiros. Contudo, este texto não é definitivo. O interesse de terceiros foi reintroduzido, por exemplo, no relatório final da Comissão LIBE por ocasião da votação das alterações acordadas pela Comissão LIBE do Parlamento Europeu em 21 de outubro de 2013. Ver a alteração n.º 100, relativa ao artigo 6.º. A reintrodução do interesse de terceiros na proposta é apoiada pelo Grupo de Trabalho, uma vez que a sua utilização pode continuar a ser adequada nalgumas situações, nomeadamente nas descritas mais adiante.

⁵⁵Esta recomendação de boas-práticas não deve pôr em causa as normas jurídicas nacionais sobre transparência e acesso público a documentos.

⁵⁶ De facto, nalguns Estados-Membros devem ser cumpridas diferentes normas no que respeita ao tratamento de dados por entidades públicas e privadas. Por exemplo, de acordo com o Código de Proteção de Dados italiano, a disseminação de dados pessoais por um organismo público apenas é permitido se estiver previsto numa lei ou num regulamento (secção 19.3).

Em ambos os casos – ou seja, independentemente de os dados pessoais serem ou não comunicados com base numa lei que o permita – a comunicação depende diretamente do resultado do teste da ponderação previsto no artigo 7.º, alínea f), e da aplicação de garantias e medidas adequadas⁵⁷.

Além disso, pode ser desejável utilizar dados pessoais já divulgados para obter uma maior transparência (por exemplo, uma nova publicação dos dados pela imprensa, ou uma maior disseminação do conjunto de dados inicialmente publicado, de forma mais inovadora e acessível, por uma ONG). A questão de saber se essa nova publicação ou reutilização é possível depende igualmente do resultado do teste da ponderação, que deve ter em conta, entre outros, a natureza da informação e o efeito da nova publicação ou reutilização sobre as pessoas⁵⁸.

Investigação histórica ou outros tipos de investigação científica. Outro contexto importante no qual a comunicação de dados no interesse legítimo de terceiros pode ser relevante é o da investigação histórica ou outros tipos de investigação científica, em especial quando seja necessário o acesso a determinadas bases de dados. A diretiva prevê o reconhecimento específico dessas atividades, sob reserva de garantias e medidas adequadas⁵⁹, mas há que não esquecer que o fundamento legítimo para essas atividades será frequentemente a utilização ponderada do artigo 7.º, alínea f)⁶⁰.

⁵⁷ Tal como explicado no Parecer 6/2013 do Grupo de Trabalho sobre os dados abertos (ver a página 9 da versão portuguesa desse parecer, referido na nota 88 *infra*), «a legislação nacional tem de cumprir o artigo 8.º da Convenção Europeia dos Direitos do Homem («CEDH») e os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia («Carta da UE»). Por conseguinte, tal como sustentou o Tribunal de Justiça da União Europeia nos acórdãos *Österreichischer Rundfunk* e *Schecke*, é necessário determinar se a divulgação é necessária e proporcional ao objetivo legítimo prosseguido pela lei». Ver o acórdão do TJUE de 20 de maio de 2003, *Rundfunk*, nos processos apensos C-465/00, C-138/01 e C-139/01, e o acórdão do TJUE de 9 de novembro de 2010, *Volker und Markus Schecke*, nos processos apensos C-92/09 e C-93/09.

⁵⁸ A limitação da finalidade é igualmente um aspeto importante a ter em conta neste contexto. Na página 21 (da versão portuguesa) do Parecer 6/2013 do Grupo de Trabalho sobre os dados abertos (referido na nota 88 *infra*), o GT29 recomenda «que qualquer legislação que implique o acesso público a dados especifique claramente os fins para que poderão ser divulgados dados pessoais. Se estes fins não forem especificados, ou se o forem em termos vagos e gerais, a previsibilidade e a segurança jurídica ficam comprometidas. Em especial, perante um pedido de reutilização, será muito difícil para o organismo do setor público e para os potenciais utilizadores em causa determinar quais eram as finalidades iniciais pretendidas com a publicação e, subsequentemente, que outras finalidades seriam compatíveis com essas finalidades iniciais. Tal como já mencionado, mesmo que os dados pessoais tenham sido publicados na Internet, não se deve presumir que podem ser objeto de um tratamento posterior para qualquer fim possível».

⁵⁹ Ver, por exemplo, o artigo 6.º, n.º 1, alíneas b) e e).

⁶⁰ Tal como explicado no Parecer 3/2013 do Grupo de Trabalho sobre a limitação da finalidade (já referido na nota 9), a utilização posterior dos dados para fins secundários deve ser submetida a um duplo teste. Em primeiro

Interesse público geral ou interesse de terceiros. Por último, o interesse legítimo de terceiros pode ser igualmente relevante de outra forma. É o caso quando um responsável pelo tratamento - por vezes encorajado pelas autoridades públicas – prossiga um interesse que corresponde a um interesse público geral ou a um interesse de terceiros. Tal pode incluir as situações em que um responsável pelo tratamento vai além das suas obrigações legais específicas estabelecidas em leis ou regulamentos para apoiar entidades responsáveis pela aplicação da lei ou privadas nos seus esforços para combater atividades ilícitas, tais como o branqueamento de capitais, o tráfico de crianças, ou a partilha ilícita de ficheiros em linha. No entanto, nestas situações é especialmente importante assegurar que os limites previstos no artigo 7.º, alínea f), sejam plenamente respeitados⁶¹.

O tratamento deve ser necessário para a(s) finalidade(s) pretendidas

Por último, o tratamento de dados pessoais deve ser igualmente «necessário para prosseguir interesses legítimos» do responsável pelo tratamento ou – em caso de comunicação de dados - de terceiros. Esta condição complementa o requisito da necessidade previsto no artigo 6.º e exige que exista uma ligação entre o tratamento e os interesses prosseguidos. Este requisito da «necessidade» aplica-se em todas as situações referidas no artigo 7.º, alíneas b) a f), mas é especialmente relevante no caso da alínea f), para assegurar que o tratamento de dados baseado em interesses legítimos não conduza a uma interpretação demasiado lata da necessidade do tratamento de dados. Tal como nos outros casos, tal significa que deve verificar-se se existem outros meios menos invasivos para alcançar a mesma finalidade.

III.3.2. Interesses ou direitos da pessoa em causa

«Interests or rights» (em vez de «interests for rights»)

No artigo 7.º, alínea f), da diretiva, na versão em língua inglesa, pode ler-se: «the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)».

lugar, deve assegurar-se que os dados sejam utilizados para fins compatíveis. Em segundo lugar, deve garantir-se a existência de uma base jurídica adequada, nos termos do artigo 7.º, para o tratamento.

⁶¹ Ver, a este respeito, por exemplo, o Documento de trabalho sobre questões de proteção de dados relacionadas com os direitos de propriedade intelectual, adotado em 18.1.2005 (WP104).

No entanto, ao comparar as diferentes versões linguísticas da diretiva, o Grupo de Trabalho observou que a expressão «interests for» foi traduzida por «interesses ou» noutras línguas chave que foram utilizadas quando o texto foi negociado⁶².

Após uma análise mais aprofundada, conclui-se que a redação da versão inglesa da diretiva resulta apenas de um erro tipográfico: escreveu-se «for», em vez de «or»⁶³. Assim, a redação correta é «interests or fundamental rights and freedoms».

Os termos «interesses» e «direitos» devem ser interpretados em sentido lato

O facto de esta disposição referir «os interesses ou os direitos e liberdades fundamentais» tem um impacto direto no seu âmbito de aplicação. Confere mais proteção à pessoa em causa, designadamente exigindo que os seus «interesses», e não apenas os seus direitos e liberdades fundamentais, sejam tidos em conta. No entanto, não há razão para partir do princípio de que a restrição prevista no artigo 7.º, alínea f), aos direitos fundamentais «protegidos ao abrigo do n.º 1 do artigo 1.º» - e, por conseguinte, a referência explícita ao objeto da diretiva⁶⁴ - não se aplica também ao termo «interesses». A mensagem clara é, todavia, que todos os interesses relevantes da pessoa em causa devem ser tidos em conta.

Esta interpretação do texto faz sentido não apenas gramaticalmente mas também tendo em conta a interpretação lata do conceito de «interesses legítimos» do responsável pelo tratamento. Se o responsável pelo tratamento – ou, em caso de comunicação de dados, um terceiro – pode prosseguir quaisquer interesses desde que estes não sejam ilegítimos, a pessoa

⁶² Por exemplo, «l'intérêt ou les droits et libertés fondamentaux de la personne concernée», em francês, «l'interesse o i diritti e le libertà fondamentali della persona interessata», em italiano, e «das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person», em alemão.

⁶³ O Grupo de Trabalho observa que a versão inglesa gramaticalmente correta seria «interests in», em vez de «interests for», se esse fosse o significado pretendido. Além disso, a expressão «interests for» ou «interests in» parece ser, à primeira vista, redundante, uma vez que a referência aos «direitos e liberdades fundamentais» seria, em princípio, suficiente, se esse fosse o significado pretendido. A interpretação no sentido de que se tratou de um erro tipográfico é igualmente confirmada pelo facto de, na Posição Comum (CE) n.º 1/95 adotada pelo Conselho em 20 de fevereiro de 1995, poder ler-se igualmente, na versão inglesa, «interests or fundamental rights and freedoms». Por último, o Grupo de Trabalho observa igualmente que a Comissão pretendeu corrigir esse erro tipográfico na proposta de regulamento: no artigo 6.º, n.º 1, alínea f), pode ler-se, na versão inglesa, «the interests or fundamental rights and freedoms of the data subject which require protection of personal data», e não «interests for [...]».

⁶⁴ Ver o artigo 1.º, n.º 1: «Os Estados-membros assegurarão, em conformidade com a presente diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais».

em causa deve ter igualmente direito a que todos os seus tipos de interesses sejam tidos em conta e ponderados em relação aos do responsável pelo tratamento, desde que sejam relevantes no âmbito de aplicação da diretiva.

Numa época em que existe um crescente desequilíbrio no «capacidade de informação», em que quer governos quer organizações empresariais vêm acumulando volumes sem precedentes de dados sobre as pessoas e têm cada vez mais condições para elaborar perfis pormenorizados que permitirão prever os seus comportamentos (reforçando o desequilíbrio de informação e reduzindo a sua autonomia), é mais importante do que nunca assegurar que o interesse das pessoas em preservar a sua privacidade e a sua autonomia seja protegido.

Por último, é importante observar que, ao contrário do que acontece relativamente aos interesses do responsável pelo tratamento, a referência aos «interesses» das pessoas em causa não é seguida pelo adjetivo «legítimos». Tal implica o reconhecimento de um âmbito de aplicação mais amplo para a proteção dos interesses e dos direitos das pessoas. Mesmo as pessoas que estejam envolvidas em atividades ilegais não devem estar sujeitas a uma ingerência desproporcionada nos seus direitos e interesses⁶⁵. Por exemplo, os interesses de uma pessoa suspeita de ter praticado um furto num supermercado podem, ainda assim, prevalecer sobre a publicação da sua fotografia e da sua morada particular nas paredes do supermercado e/ou na Internet pelo proprietário da loja.

III.3.3. Introdução à aplicação do teste da ponderação

É útil imaginar um espectro no qual estejam representados tanto os interesses legítimos do responsável pelo tratamento como o impacto nos interesses e nos direitos da pessoa em causa. Os interesses legítimos podem ir desde os insignificantes, passando pelos relativamente importantes, até aos preponderantes. Do mesmo modo, o impacto nos interesses e nos direitos das pessoas em causa pode ser mais ou menos significativo e pode ir desde o trivial até ao muito grave.

Em geral, os interesses legítimos do responsável pelo tratamento, quando sejam pouco relevantes e não muito preponderantes, só prevalecem sobre os interesses e os direitos das

⁶⁵ É claro que uma das consequências da criminalidade pode ser a recolha e possível publicação de dados pessoais sobre criminosos e suspeitos. No entanto, tal deve estar sujeito a condições e garantias rigorosas.

pessoas em causa nos casos em que o impacto nesses direitos e interesses seja ainda mais trivial. Por outro lado, os interesses legítimos importantes e preponderantes podem, nalguns casos e sob reserva de garantias e medidas, justificar mesmo uma intromissão significativa na vida privada ou outro impacto significativo nos interesses ou nos direitos das pessoas em causa⁶⁶.

Neste aspeto, é importante salientar o papel especial que as garantias podem desempenhar⁶⁷ na redução do impacto indevido nas pessoas em causa, alterando assim o equilíbrio de direitos e interesses de modo a que os interesses legítimos do responsável pelo tratamento não sejam sacrificados. É claro que a utilização de garantias, só por si, não é suficiente para justificar qualquer tipo de tratamento em todos os contextos. Além disso, as garantias em causa devem ser adequadas e suficientes e devem reduzir os impactos nas pessoas em causa de forma inquestionável e significativa.

Cenários introdutórios

Antes de prosseguir com o fornecimento de orientações sobre como realizar o teste da ponderação, os três cenários introdutórios que se seguem podem ajudar a ilustrar como pode ser feita a ponderação dos interesses e dos direitos na vida real. Os três exemplos baseiam-se num cenário simples e inofensivo que principia com uma oferta especial de comida italiana «pronta a levar». Os exemplos vão introduzindo gradualmente novos elementos que mostram como o equilíbrio é alterado à medida que o impacto na pessoa em causa aumenta.

⁶⁶ Ver, a título de ilustração, a argumentação do Grupo de Trabalho em vários pareceres e documentos de trabalho:

- Parecer 4/2006 sobre o aviso de proposta de regulamentação do Departamento de Saúde e Serviços Humanos dos Estados Unidos relativa ao controlo das doenças transmissíveis e à recolha de informação sobre passageiros, de 20 de novembro de 2005 (Proposta relativa ao controlo das doenças transmissíveis n.º 42, CFR, partes 70 e 71), adotado em 14.6.2006 (WP121), no qual estão em causa ameaças graves específicas à saúde pública.

- Parecer 1/2006 sobre sistemas de denúncia (já referido na nota 39), no qual a gravidade de uma infração alegada é um dos elementos do teste da ponderação.

- Documento de trabalho sobre a vigilância das comunicações eletrónicas no local de trabalho, adotado em 29.5.2002 (WP55), no qual o direito do empregador de administrar eficientemente a sua empresa é ponderado em relação à dignidade humana do trabalhador, bem como ao direito à confidencialidade da correspondência.

⁶⁷As garantias podem incluir, entre outros, a limitação rigorosa do volume de dados recolhidos, a eliminação de dados imediatamente após utilização, medidas técnicas e organizativas para garantir a separação funcional, utilização adequada de técnicas de anonimização, agregação de dados e tecnologias para reforçar a proteção da privacidade, bem como uma maior transparência e responsabilidade e a possibilidade de optar por não permitir o tratamento. Sobre esta matéria, ver ainda a secção III.3.4, alínea d) e seguintes.

Cenário 1: oferta especial de uma cadeia de pizarias

Cláudia encomenda uma pizza através de uma aplicação móvel que tem no seu smartphone mas, no sítio Web, não optou por não receber publicidade. Os dados relativos à sua morada e ao seu cartão de crédito são conservados para efeitos da entrega. Alguns dias mais tarde, Cláudia recebe na caixa de correio do seu domicílio cupões de desconto relativos a produtos semelhantes, provenientes da referida cadeia de pizarias.

Breve análise: a cadeia de pizarias tem um interesse legítimo, mas não especialmente preponderante, em tentar vender mais produtos aos seus clientes. Por outro lado, não parece existir qualquer intromissão significativa na vida privada de Cláudia ou qualquer outro impacto indevido nos seus interesses ou nos seus direitos. Os dados e o contexto são relativamente inofensivos (consumo de pizza). A cadeia de pizarias estabeleceu algumas garantias: apenas é utilizada informação relativamente limitada (informações de contacto) e os cupões são enviados através do correio tradicional. Além disso, no sítio Web é dada a possibilidade de optar facilmente por não receber publicidade.

Em conclusão, e tendo em conta igualmente as garantias e as medidas adotadas (incluindo uma ferramenta que permite optar facilmente por não receber publicidade), não se afigura que os interesses e os direitos da pessoa em causa prevaleçam sobre os interesses legítimos da cadeia de pizarias em realizar este tratamento mínimo de dados.

Cenário 2: publicidade dirigida relativa à mesma oferta especial

O contexto é o mesmo mas, desta vez, a cadeia de pizarias conserva não apenas os dados relativos à morada e ao cartão de crédito de Cláudia mas igualmente o seu histórico de encomendas recentes (dos últimos três anos). Além disso, o histórico de compras é combinado com dados do supermercado onde Cláudia faz as suas compras em linha, que pertence à mesma empresa que gere a cadeia de pizarias. A cadeia de pizarias envia a Cláudia ofertas especiais e publicidade dirigida com base no histórico de encomendas realizadas nos dois serviços. Cláudia recebe a publicidade e as ofertas especiais quer em linha quer sem ser em linha, enviadas por correio normal ou correio eletrónico, ou colocadas no sítio Web da empresa, bem como nos sítios Web de vários parceiros selecionados (quando acede a esses sítios Web no seu computador ou através do seu telemóvel). O seu histórico de navegação (sequência de cliques) é também rastreado. Os dados relativos à sua localização são igualmente rastreados através do seu telemóvel. É utilizado um software que analisa os dados e permite prever as suas preferências e os momentos e os locais em que estará mais disponível para efetuar uma compra mais avultada, disposta a pagar um preço mais elevado, suscetível de ser influenciada por um determinado desconto ou mais ansiosa por saborear a sua sobremesa ou refeição pronta favorita⁶⁸. Cláudia é constantemente incomodada por anúncios persistentes que aparecem no seu telemóvel quando está a ver o horário do autocarro à ida para casa, com publicidade às ofertas mais recentes de comida pronta a levar às quais Cláudia tem tentado resistir. Cláudia não conseguiu encontrar informação acessível ou uma forma simples de desligar esses anúncios, embora a empresa alegue que está em funcionamento, em todo o setor, um sistema que permite que as pessoas optem por não receber publicidade. Cláudia constatou igualmente com surpresa que, quando foi viver para um bairro menos abastado, deixou de receber as suas ofertas especiais. Em consequência, os seus gastos mensais com alimentação aumentaram cerca de 10%. Uma amiga com mais conhecimentos sobre tecnologias mostrou-lhe um blogue em linha no qual se especulava que o supermercado cobrava mais pelas encomendas provenientes de «bairros maus», com fundamento em informações estatísticas que apontavam para um maior risco de fraude na utilização de cartões de crédito nesses casos. A empresa não comentou e alegou que a sua política de descontos e o algoritmo que utiliza para estabelecer os preços são assuntos privados e não podem ser revelados.

Breve análise: a natureza dos dados e o contexto mantêm-se relativamente inofensivos. No entanto, o alcance da recolha de dados e as técnicas utilizadas para influenciar Cláudia (incluindo várias técnicas de rastreamento, que preveem os momentos e os locais em que Cláudia está mais ansiosa por saborear determinados alimentos e o facto de, nesses momentos, Cláudia estar mais vulnerável para ceder à tentação) são fatores a ter em conta na avaliação do impacto do tratamento de dados. A falta de transparência sobre a lógica do tratamento de dados pela empresa, que pode ter conduzido a uma discriminação de preços *de facto* baseada na localização a partir da qual a encomenda é efetuada e o potencial impacto financeiro significativo nos clientes acabam por alterar o equilíbrio, mesmo no contexto relativamente inocente da comida pronta a levar e das compras de mercearia. Em vez da mera possibilidade de optar por não permitir este tipo de elaboração de perfis e de publicidade dirigida, é necessário um consentimento informado, nos termos do artigo 7.º, alínea a), mas também nos termos do artigo 5.º, n.º 3, da diretiva «privacidade e comunicações eletrónicas». Consequentemente, o artigo 7.º, alínea f), não deve ser invocado como fundamento jurídico para o tratamento.

⁶⁸ Ver, por exemplo, <http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review->

Cenário 3: utilização das encomendas de comida para adaptar os prémios dos seguros de saúde

Os hábitos de consumo de pizza de Cláudia, incluindo as horas e o tipo de comida encomendada, são vendidos pela cadeia a uma companhia de seguros, que os utiliza para adaptar os seus prémios dos seguros de saúde.

Breve análise: a companhia de seguros de saúde pode ter um interesse legítimo – na medida em que os regulamentos aplicáveis o permitam – em avaliar os riscos para a saúde dos seus clientes e cobrar prémios diferenciados de acordo com os diferentes riscos. No entanto, a forma como os dados são recolhidos e o alcance da própria recolha de dados são excessivos. Seria improvável que qualquer pessoa razoável na situação de Cláudia previsse que a informação acerca do seu consumo de pizza seria utilizada para calcular os prémios do seu seguro de saúde.

Para além da natureza excessiva da elaboração de perfis e das possíveis ilações incorretas (a pizza podia ser encomendada para outra pessoa), a inferência de dados sensíveis (dados relativos à saúde) a partir de dados aparentemente inócuos (encomendas de comida pronta a levar) contribui para alterar o equilíbrio a favor dos interesses e dos direitos da pessoa em causa. Por último, o tratamento dos dados tem igualmente um impacto financeiro significativo na vida de Cláudia.

Em conclusão, neste caso específico, os interesses e os direitos da pessoa em causa prevalecem sobre os interesses legítimos da companhia de seguros de saúde. Consequentemente, o artigo 7.º, alínea f), não deve ser invocado como fundamento jurídico para o tratamento. É igualmente questionável se o artigo 7.º, alínea a), pode ser utilizado como fundamento jurídico, tendo em conta o alcance excessivo da recolha de dados e possivelmente também devido a outras restrições específicas nos termos do direito nacional.

boards: «Investigações recentes indicam que a força de vontade é um recurso limitado que pode esgotar-se e renovar-se ao longo do tempo.[10] Imaginem que as preocupações com a obesidade levam uma consumidora a procurar resistir à sua ‘comida de plástico’ favorita. Acontece que há momentos e locais em que ela não consegue resistir. Os grandes volumes de dados podem ajudar os publicitários a compreender exatamente como e quando podem abordar esta consumidora em situação mais vulnerável – especialmente num mundo em que estamos constantemente à frente do ecrã e em que até os nossos aparelhos conseguem fazer uma campanha de vendas».

Os cenários apresentados e a possível introdução de variações com outros elementos sublinham a necessidade de limitar o número de fatores-chave que podem ajudar a focalizar a avaliação, bem como a necessidade de adotar uma abordagem pragmática que permita utilizar presunções práticas («princípios por aproximação») baseadas, antes de mais, no que qualquer pessoa razoável consideraria aceitável nas mesmas circunstâncias («expectativas razoáveis») e baseadas nas consequências da atividade de tratamento de dados para as pessoas em causa («impacto»).

III.3.4. Fatores-chave a ter em conta na aplicação do teste da ponderação

Os Estados-Membros desenvolveram alguns fatores úteis a ter em conta na realização do teste da ponderação. Esses fatores são discutidos na presente secção, sob as quatro epígrafes principais seguintes: a) avaliação do interesse legítimo do responsável pelo tratamento, b) impacto nas pessoas em causa, c) equilíbrio provisório e d) garantias complementares aplicadas pelo responsável pelo tratamento para evitar qualquer impacto indevido nas pessoas em causa.⁶⁹

Para realizar o teste da ponderação é importante ter em conta, antes de mais, a natureza e a origem dos interesses legítimos, por um lado, e o impacto nas pessoas em causa, por outro. Esta avaliação já deve ter em conta as medidas que o responsável pelo tratamento tenciona adotar para cumprir o disposto na diretiva (por exemplo, garantir a limitação da finalidade e a proporcionalidade nos termos do artigo 6.º ou fornecer informações às pessoas em causa nos termos dos artigos 10.º e 11.º).

Após analisar e ponderar cada um dos lados em relação ao outro é possível estabelecer um «equilíbrio» provisório. Caso o resultado da avaliação ainda suscite dúvidas, o passo seguinte será verificar se a aplicação de garantias complementares, que proporcionem mais proteção à pessoa em causa, pode alterar o equilíbrio de modo a legitimar o tratamento.

a) Avaliação do interesse legítimo do responsável pelo tratamento

⁶⁹ Devido à sua importância, algumas questões específicas relacionadas com as garantias serão discutidas de forma mais aprofundada, sob outras epígrafes, nas secções III.3.5 e III.3.6.

Tendo em conta que o conceito de interesses legítimos é bastante abrangente, tal como explicado na secção III.3.1 supra, a sua natureza desempenha um papel crucial quando se trata de ponderar esses interesses em relação aos direitos e aos interesses das pessoas em causa. Embora seja impossível fazer juízos de valor relativamente a todos os eventuais interesses legítimos, é possível fornecer algumas orientações. Como já foi referido, esses interesses podem ir desde os triviais até aos preponderantes, e ser simples ou mais controversos.

i) Exercício de um direito fundamental

Entre os direitos e as liberdades fundamentais consagrados na Carta dos Direitos Fundamentais da União Europeia (a seguir designada por «Carta»)⁷⁰ e na Convenção Europeia dos Direitos do Homem (a seguir designada por «CEDH»), há vários que podem entrar em conflito com o direito ao respeito pela vida privada e o direito à proteção de dados pessoais, tais como a liberdade de expressão e de informação⁷¹, a liberdade das artes e das ciências⁷², o direito de acesso aos documentos⁷³, bem como, por exemplo, o direito à liberdade e à segurança⁷⁴, a liberdade de pensamento, de consciência e de religião⁷⁵, a liberdade de empresa⁷⁶, o direito de propriedade⁷⁷, o direito à ação e a um tribunal imparcial⁷⁸ ou a presunção de inocência e os direitos de defesa⁷⁹.

Para que o interesse legítimo do responsável pelo tratamento prevaleça, o tratamento de dados deve ser «necessário» e «proporcionado», de forma a possibilitar o exercício do direito fundamental em causa.

A título ilustrativo, dependendo das circunstâncias específicas do caso, pode muito bem ser necessário e proporcionado um jornal publicar determinados pormenores comprometedores

⁷⁰ As disposições da Carta têm por destinatários as instituições e órgãos da UE, na observância do princípio da subsidiariedade, bem como as autoridades nacionais, apenas quando apliquem o direito da União.

⁷¹ Artigo 11.º da Carta e artigo 10.º da CEDH.

⁷² Artigo 13.º da Carta e artigos 9.º e 10.º da CEDH.

⁷³ Artigo 42.º da Carta. «Qualquer cidadão da União, bem como qualquer pessoa singular ou coletiva com residência ou sede social num Estado-Membro, tem direito de acesso aos documentos do Parlamento Europeu, do Conselho e da Comissão». Existem direitos de acesso semelhantes em vários Estados-Membros no que respeita a documentos que estão na posse de organismos públicos nesses Estados-Membros.

⁷⁴ Artigo 6.º da Carta e artigo 5.º da CEDH.

⁷⁵ Artigo 10.º da Carta e artigo 9.º da CEDH.

⁷⁶ Artigo 16.º da Carta.

⁷⁷ Artigo 17.º da Carta e artigo 1.º do Protocolo adicional à CEDH.

⁷⁸ Artigo 47.º da Carta e artigo 6.º da CEDH.

⁷⁹ Artigo 48.º da Carta e artigos 6.º e 13.º da CEDH.

sobre os hábitos de consumo de um alto funcionário governamental envolvido num alegado escândalo de corrupção. Por outro lado, os órgãos de comunicação social não devem ter uma permissão generalizada para publicar todos e quaisquer pormenores irrelevantes sobre a vida privada de figuras públicas. Estes e outros casos semelhantes levantam geralmente questões complexas de avaliação, pelo que, para ajudar a orientar a avaliação, a legislação específica, a jurisprudência, as diretrizes, bem como os códigos de conduta e outras normas mais ou menos formais, podem desempenhar um papel importante.⁸⁰

Se necessário, também neste contexto, as garantias complementares podem desempenhar um papel importante e ajudar a determinar de que forma se pode alcançar o - por vezes frágil - equilíbrio.

ii) Interesses públicos/interesses da comunidade em geral

Nalguns casos, o responsável pelo tratamento pode desejar invocar o interesse público ou o interesse da comunidade em geral (quer tal esteja previsto na legislação ou regulamentação nacional quer não). Por exemplo, uma organização de beneficência pode tratar dados pessoais para efeitos de investigação médica, ou uma organização sem fins lucrativos pode fazê-lo com o objetivo de alertar para a corrupção governamental.

Pode dar-se igualmente o caso de o interesse comercial privado de uma empresa coincidir, em certa medida, com o interesse público. Tal pode acontecer, por exemplo, no que respeita ao combate à fraude financeira ou a outra utilização fraudulenta de serviços⁸¹. Um prestador de serviços pode ter um interesse comercial legítimo em assegurar que os seus clientes não utilizem o serviço de forma abusiva (ou não consigam obter serviços sem pagar) e, ao mesmo tempo, os clientes da empresa, os contribuintes e o público em geral têm igualmente um

⁸⁰ No que respeita aos critérios a aplicar nos casos relacionados com a liberdade de expressão, a jurisprudência do Tribunal Europeu dos Direitos do Homem fornece igualmente orientações úteis. Ver, por exemplo, o acórdão do TEDH de 7 de fevereiro de 2012, no processo von Hannover c. Alemanha (N.º 2), em especial §§ 95 a 126. Há que tomar em consideração igualmente que o artigo 9.º da diretiva (sob a epígrafe *Tratamento de dados pessoais e liberdade de expressão*) dispõe que os Estados-Membros «estabelecerão isenções ou derrogações [a determinadas disposições da diretiva] para o tratamento de dados pessoais efetuado para fins exclusivamente jornalísticos ou de expressão artística ou literária», desde que aquelas sejam «necessárias para conciliar o direito à vida privada com as normas que regem a liberdade de expressão».

⁸¹ Ver, por exemplo, o «Exemplo 21: recolha de dados de contadores inteligentes para detetar a utilização fraudulenta de energia», na página 67 do Parecer 3/2013 do Grupo de Trabalho sobre a limitação da finalidade (já referido na nota 9).

interesse legítimo em assegurar que as atividades fraudulentas, quando ocorram, sejam desencorajadas e detetadas.

Em regra, o facto de um responsável pelo tratamento atuar não apenas no seu próprio interesse legítimo (por exemplo, comercial) mas igualmente no interesse da comunidade em geral pode dar mais «valor» a esse interesse. Quanto mais preponderante for o interesse público ou o interesse da comunidade em geral, e quanto mais o facto de o responsável pelo tratamento poder atuar e tratar os dados na prossecução desse interesse for claramente reconhecido e esperado pela comunidade e pelas pessoas em causa, mais valor esse interesse legítimo tem na ponderação.

Por outro lado, a «aplicação privada» da lei não deve ser utilizada para legitimar práticas intrusivas suscetíveis, quando sejam levadas a cabo por uma organização governamental, de ser proibidas nos termos da jurisprudência do Tribunal Europeu dos Direitos do Homem, com fundamento no facto de as atividades da autoridade pública constituírem uma ingerência na vida privada que não cumpre o critério rigoroso estabelecido no artigo 8.º, n.º 2, da CEDH.

iii) Outros interesses legítimos

Nalguns casos, como já foi referido na secção III.2, o interesse legítimo surge num contexto que pode assemelhar-se a um dos contextos nos quais alguns dos outros fundamentos jurídicos, em especial, os fundamentos jurídicos previstos no artigo 7.º, alínea, b) (contrato), alínea c) (obrigação legal) ou alínea e) (missão pública), são aplicáveis. Por exemplo, uma atividade de tratamento de dados pode não ser estritamente necessária mas ser, ainda assim, relevante para a execução de um contrato, ou uma lei pode apenas permitir, mas não exigir, o tratamento de determinados dados. Como vimos, pode nem sempre ser fácil traçar uma linha divisória clara entre os diferentes fundamentos, o que torna ainda mais importante a inclusão do teste da ponderação previsto no artigo 7.º, alínea f), na análise.

Também neste caso, bem como em todos os outros casos possíveis que não foram referidos até agora, quanto mais preponderante for o interesse do responsável pelo tratamento, e quanto mais o facto de o responsável pelo tratamento poder atuar e tratar dados na prossecução desse interesse for claramente reconhecido e esperado na comunidade em geral, mais valor esse

interesse legítimo tem na ponderação⁸². Esta conclusão conduz-nos ao ponto seguinte, mais geral.

iv) Reconhecimento jurídico e cultural/social da legitimidade dos interesses

Em todos os contextos acima referidos é, sem dúvida, igualmente relevante saber se o direito da UE ou o direito do Estado-Membro permite especificamente (mesmo que não o exija) que os responsáveis pelo tratamento efetuem diligências na prossecução do interesse público ou privado em causa. É ainda relevante saber se existem quaisquer orientações validamente adotadas e não vinculativas, emitidas pelos organismos competentes, por exemplo, por entidades reguladoras, que incentivem os responsáveis pelo tratamento a tratar os dados na prossecução do interesse em causa.

A conformidade com quaisquer orientações não vinculativas fornecidas pelas autoridades responsáveis pela proteção de dados ou por outros organismos relevantes no que respeita às modalidades do tratamento de dados é suscetível de contribuir também para uma avaliação favorável do equilíbrio. As expectativas culturais e sociais, ainda que não se reflitam diretamente em instrumentos legislativos ou regulamentares, podem igualmente desempenhar um papel importante e podem ajudar a alterar o equilíbrio em qualquer dos sentidos.

Quanto mais o facto de os responsáveis pelo tratamento poderem atuar e tratar dados na prossecução de um interesse em particular for expressamente reconhecido na legislação, noutros instrumentos regulamentares – quer vinculem o responsável pelo tratamento quer não – ou até na cultura de uma dada comunidade em geral, sem qualquer base jurídica específica, mais valor esse interesse legítimo tem na ponderação⁸³.

⁸² É evidente que a avaliação deve incluir também uma reflexão sobre o eventual prejuízo sofrido pelo responsável pelo tratamento, por terceiros ou pela comunidade em geral se o tratamento de dados não for efetuado.

⁸³ Contudo, esse interesse não pode ser utilizado para legitimar práticas intrusivas que, de outro modo, não cumpram o critério estabelecido no artigo 8.º, n.º 2, da CEDH.

b) Impacto nas pessoas em causa

Olhando para o outro lado a ponderar, o impacto do tratamento nos interesses ou nos direitos e liberdades fundamentais da pessoa em causa é um critério essencial. A primeira subsecção infra aborda, em termos gerais, a forma como deve ser avaliado o impacto na pessoa em causa.

Nesse sentido, vários elementos podem ser úteis e são analisados nas subsecções seguintes, nomeadamente a natureza dos dados pessoais, a forma como a informação é tratada, as expectativas razoáveis das pessoas em causa e o estatuto do responsável pelo tratamento e da pessoa em causa. Abordaremos igualmente, de forma sucinta, questões relacionadas com potenciais fontes de risco que possam provocar um impacto nas pessoas em causa, a gravidade de quaisquer impactos nas pessoas em causa e a probabilidade de esses impactos se concretizarem.

i) Avaliação de impacto

Na avaliação do impacto⁸⁴ do tratamento, deve ter-se em conta quer as consequências positivas quer as negativas. Estas podem incluir potenciais decisões ou ações futuras por parte de terceiros, situações nas quais o tratamento possa conduzir à exclusão ou à discriminação de pessoas e à difamação ou, de forma mais abrangente, situações nas quais exista o risco de prejudicar a reputação, o poder de negociação ou a autonomia da pessoa em causa.

Para além dos efeitos adversos que podem ser especificamente previstos, há que ter em conta igualmente os impactos emocionais mais abrangentes, tais como a irritação, o medo e a angústia que podem ser provocados pelo facto de a pessoa em causa perder o controlo sobre informações pessoais ou aperceber-se de que estas foram ou podem ser utilizadas de forma abusiva ou indevida – por exemplo, através da sua publicação na Internet. Deve ter-se também devidamente em conta o efeito inibidor no comportamento protegido, tal como a liberdade de investigação ou de expressão, que pode ser provocado pelo controlo/rastreamento contínuo.

O Grupo de Trabalho salienta que é essencial compreender que o conceito de «impacto» relevante é muito mais abrangente do que o de dano ou prejuízo sofrido por determinada ou determinadas pessoas em causa. O termo «impacto» tal como é utilizado no presente parecer abrange quaisquer consequências possíveis (potenciais ou reais) do tratamento de dados. Por uma questão de clareza, salientamos igualmente que este conceito não está relacionado com o conceito de violação de dados e é muito mais abrangente do que os impactos provocados por uma violação de dados. Pelo contrário, o conceito de impacto tal como é utilizado no presente parecer engloba as várias formas como uma pessoa pode ser afetada – positiva ou negativamente – pelo tratamento dos seus dados pessoais⁸⁵.

⁸⁴ Esta avaliação de impacto deve ser entendida no contexto do artigo 7.º, alínea f). Por outras palavras, não nos referimos a uma «análise de risco» ou a uma «avaliação de impacto sobre a proteção de dados» na aceção da proposta de regulamento (artigos 33.º e 34.º) e respetivas alterações propostas pela Comissão LIBE. A questão de saber que metodologia deve ser seguida numa «análise de risco» ou numa «avaliação de impacto sobre a proteção de dados» ultrapassa o âmbito do presente parecer. Por outro lado, há que ter em atenção que – de uma forma ou de outra – a análise do impacto nos termos do artigo 7.º, alínea f), pode ser uma parte importante de qualquer «análise de risco» ou «avaliação de impacto sobre a proteção de dados» e pode também ajudar a identificar as situações nas quais a autoridade responsável pela proteção de dados deve ser consultada.

⁸⁵ O risco de prejuízo financeiro, por exemplo, se uma violação de dados provocar uma fuga de informações financeiras que deveriam estar num ambiente seguro, acabando por conduzir a uma usurpação de identidade ou a outros tipos de fraude, ou o risco de lesão corporal, dor, sofrimento e perda de qualidade de vida que possam, em última análise, ter sido provocados, por exemplo, por alterações não autorizadas a relatórios médicos, e pelo

É igualmente importante compreender que, na maior parte dos casos, várias ocorrências relacionadas ou não entre si podem, cumulativamente, provocar um impacto final negativo na pessoa em causa e pode ser difícil identificar a atividade de tratamento, e o respetivo responsável, que desempenhou um papel essencial nesse impacto negativo.

Tendo em conta que, neste contexto, é muitas vezes difícil às pessoas em causa propor uma ação para obter uma indemnização por um dano ou prejuízo sofrido, mesmo que o próprio efeito seja muito real, é ainda mais importante colocar a ênfase na prevenção e assegurar que as atividades de tratamento de dados apenas possam ser realizadas se não comportarem nenhum risco, ou se comportarem um risco muito baixo, de impacto negativo indevido nos interesses ou nos direitos e liberdades fundamentais das pessoas em causa.

Na avaliação de impacto, a terminologia e a metodologia tradicionais de avaliação dos riscos podem, em certa medida, ser úteis, pelo que alguns elementos desta metodologia serão destacados, de forma sucinta, mais adiante. Contudo, uma metodologia global para a avaliação de impacto – no contexto do artigo 7.º, alínea f), ou num contexto mais abrangente – ultrapassaria o âmbito do presente parecer.

Neste contexto, como em qualquer outro, é importante identificar as fontes dos potenciais impactos nas pessoas em causa.

A probabilidade de um risco poder realizar-se é um dos elementos a ter em conta. Por exemplo, o acesso à Internet, o intercâmbio de dados com sítios Web fora da UE, as interligações com outros sistemas e um elevado grau de heterogeneidade e de variabilidade do sistema podem constituir vulnerabilidades que os piratas informáticos podem explorar. Esta fonte de riscos acarreta uma probabilidade relativamente grande de o risco de utilização indevida de dados se realizar. Em contrapartida, um sistema homogéneo e estável que não tenha interligações nem esteja ligado à Internet acarreta uma probabilidade muito menor de os dados serem indevidamente utilizados.

consequente tratamento desadequado do doente, deve ser sempre tido devidamente em conta, embora não esteja, de forma nenhuma, limitado às situações previstas no âmbito de aplicação do artigo 7.º, alínea f). Ao mesmo tempo, estes riscos não são os únicos a ter em conta na avaliação de impacto nos termos do artigo 7.º, alínea f).

Outro elemento da avaliação dos riscos é a gravidade das consequências da realização de um risco. Essa gravidade pode ir desde níveis baixos (por exemplo, a necessidade incómoda de voltar a inserir informações de contacto pessoais que o responsável pelo tratamento tenha perdido) até níveis muito altos (por exemplo, a perda de vidas quando as referências da localização de pessoas que estão sob proteção vão parar às mãos de criminosos ou quando o fornecimento de energia seja interrompido à distância, através de contadores inteligentes, em situações meteorológicas extremas ou em situações graves de saúde das pessoas).

Estes dois elementos-chave – a probabilidade de o risco se realizar, por um lado, e a gravidade das consequências, por outro lado – contribuem para a avaliação global do potencial impacto.

Por último, na aplicação da metodologia, deve recordar-se que a avaliação de impacto nos termos do artigo 7.º, alínea f), não pode conduzir a um exercício mecânico e puramente quantitativo. Nos cenários tradicionais de avaliação dos riscos, a «gravidade» pode ter em conta o número de pessoas potencialmente afetadas. No entanto, deve ter-se em atenção que o tratamento de dados pessoais que tenha um impacto numa minoria de pessoas em causa – ou mesmo numa única pessoa – exige, ainda assim, uma análise muito cuidada, especialmente se o impacto em cada uma dessas pessoas for potencialmente significativo.

ii) Natureza dos dados

Em primeiro lugar, é importante verificar se o processo envolve dados sensíveis, quer porque pertençam às categorias específicas de dados previstas no artigo 8.º da diretiva quer por outras razões, como no caso de dados biométricos, dados genéticos, dados de comunicações, dados de localização e outros tipos de informações pessoais que exijam proteção especial⁸⁶.

A título ilustrativo, na opinião do Grupo de Trabalho, regra geral, a utilização de dados biométricos por exigências gerais de segurança de bens ou de pessoas é considerada um interesse legítimo sobre o qual prevalecem os interesses ou os direitos e liberdades fundamentais da pessoa em causa. Por outro lado, dados biométricos como a impressão digital

⁸⁶ Os dados biométricos e os dados genéticos são considerados categorias específicas de dados na proposta da Comissão de um regulamento sobre a proteção de dados, lida em conjugação com as alterações propostas pela Comissão LIBE. Ver a alteração n.º 103 ao artigo 9.º no relatório final da Comissão LIBE. Quanto à relação entre os artigos 7.º e 8.º da Diretiva 95/46/CE, ver a secção II.1.2 supra, nas páginas 14 e 15.

e/ou o reconhecimento da íris podem ser utilizados para garantir a segurança de um local de alto risco, como um laboratório que esteja a investigar vírus perigosos, desde que o responsável pelo tratamento tenha apresentado provas concretas da existência de um risco considerável⁸⁷.

Em geral, quanto mais sensível for a informação envolvida, mais consequências podem existir para a pessoa em causa. Contudo, tal não significa que dados que, por si sós, pareçam inócuos possam ser tratados livremente com base no artigo 7.º, alínea f). De facto, mesmo esses dados, dependendo da forma como são tratados, podem ter um impacto significativo nas pessoas, como se verá na subsecção iii) infra.

A este respeito, pode ser relevante saber se os dados já foram tornados públicos pela pessoa em causa ou por terceiros. Neste aspeto, é importante, antes de mais, salientar que os dados pessoais, mesmo que tenham sido tornados públicos, continuam a ser considerados dados pessoais, pelo que o seu tratamento continua a exigir garantias adequadas⁸⁸. Não existe uma permissão generalizada para reutilizar e continuar a tratar dados pessoais tornados públicos nos termos do artigo 7.º, alínea f).

Dito isto, o facto de os dados pessoais terem sido tornados públicos pode ser considerado um fator a ter em conta na avaliação, em especial se a publicação tiver tido efetuada na expectativa razoável de os dados virem a ser utilizados posteriormente para determinados fins (por exemplo, para fins de investigação ou para fins relacionados com a transparência e a responsabilidade).

iii) Forma como os dados são tratados

A avaliação de impacto, em sentido lato, pode implicar que se verifique se os dados são divulgados publicamente ou de outro modo colocados à disposição de um grande número de

⁸⁷ Ver o Parecer 3/2012 do Grupo de Trabalho do artigo 29 sobre a evolução das tecnologias biométricas (WP193). Novamente a título ilustrativo, no seu Parecer 4/2009 sobre a Agência Mundial Antidopagem (já referido na nota 32), o Grupo de Trabalho salientou que o artigo 7.º, alínea f), não constituía um fundamento válido para o tratamento de dados médicos e de dados relativos a infrações no contexto de investigações antidopagem, dada a «gravidade das intrusões na privacidade». O tratamento de dados deve estar previsto na lei e cumprir os requisitos estabelecidos no artigo 8.º, n.ºs 4 ou 5, da diretiva.

⁸⁸ Ver o Parecer 3/2013 do Grupo de Trabalho sobre a limitação da finalidade (já referido na nota 9) e o Parecer 6/2013 do Grupo de Trabalho sobre os dados abertos e a reutilização de informação do setor público («ISP»), adotado em 5.6.2013 (WP207).

pessoas, ou se grandes volumes de dados pessoais são tratados ou combinados com outros dados (por exemplo, no caso da elaboração de perfis, para fins comerciais, de aplicação da lei ou outros). Dados aparentemente inócuos, quando sejam tratados em grande escala e combinados com outros dados, podem dar azo a inferências sobre dados mais sensíveis, como se viu no cenário 3 supra, que ilustrava a relação entre os padrões de consumo de pizza e os prémios de seguros de saúde.

Para além de poder conduzir ao tratamento de dados mais sensíveis, tal análise pode igualmente dar azo a previsões inquietantes, inesperadas e por vezes também incorretas, por exemplo, a respeito do comportamento ou da personalidade das pessoas em causa. Dependendo da natureza e do impacto dessas previsões, tal pode ser altamente intrusivo na privacidade das pessoas⁸⁹.

Num parecer anterior, o Grupo de Trabalho realçou igualmente os riscos inerentes a determinadas soluções de segurança (nomeadamente no que respeita a firewalls, antivírus ou anti-spam), uma vez que podem conduzir à realização de inspeções profundas de grande escala, o que pode influenciar significativamente a avaliação do equilíbrio de direitos⁹⁰.

Em geral, quanto mais negativo ou incerto for o impacto do tratamento, mais improvável é que o tratamento venha a ser considerado, em termos gerais, legítimo. A existência de métodos alternativos para alcançar os objetivos prosseguidos pelo responsável pelo tratamento, com um impacto menos negativo na pessoa em causa, deverá ser seguramente um fator relevante a ter em conta neste contexto. Se necessário, as avaliações de impacto na privacidade e na proteção de dados podem ser utilizadas para determinar se essa possibilidade existe.

iv) Expectativas razoáveis da pessoa em causa

A este respeito, as expectativas razoáveis da pessoa em causa quanto à utilização e à comunicação dos dados são também muito relevantes. Como foi igualmente salientado em

⁸⁹ Ver a secção III.2.5 e o anexo 2 (quanto aos grandes volumes de dados e aos dados abertos) do parecer sobre a limitação da finalidade (já referido na nota 9).

⁹⁰ Ver a secção 3.1 do Parecer 1/2009 do Grupo de Trabalho sobre as propostas de alteração da Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (diretiva da privacidade eletrónica) (WP159).

relação à análise do princípio da limitação da finalidade⁹¹, é «importante verificar se o estatuto do responsável pelo tratamento dos dados⁹², a natureza da relação ou do serviço prestado⁹³ ou as obrigações jurídicas ou contratuais aplicáveis (ou outras promessas feitas no momento da recolha) podem gerar expectativas razoáveis de uma maior confidencialidade e de limitações mais rigorosas na utilização posterior dos dados. Em geral, quanto mais específico e restritivo for o contexto da recolha, maior é a probabilidade de existirem mais limitações na utilização. Também neste caso, é necessário ter em conta o contexto factual, e não tomar por base apenas a informação escrita em caracteres reduzidos.»

v) Estatuto do responsável pelo tratamento dos dados e da pessoa em causa

O estatuto da pessoa em causa e do responsável pelo tratamento dos dados é igualmente relevante na avaliação do impacto do tratamento. A posição do responsável pelo tratamento dos dados pode ser mais ou menos dominante em relação à pessoa em causa consoante se trate de uma pessoa singular ou de uma pequena organização, uma grande empresa multinacional ou um organismo do setor público, e consoante as circunstâncias específicas do caso. Uma grande empresa multinacional pode, por exemplo, ter mais recursos e poder de negociação do que a pessoa singular em causa, pelo que pode estar em melhores condições de impor à pessoa em causa o que acredita ser o seu «interesse legítimo». Tal pode acontecer sobretudo se a empresa tiver uma posição dominante no mercado. Se estas situações não forem controladas, podem ser prejudiciais para as pessoas singulares em causa. Assim como a legislação em matéria de defesa do consumidor e de concorrência ajuda a assegurar que esse poder não seja utilizado de forma abusiva, a legislação em matéria de proteção de dados também pode desempenhar um papel importante, assegurando que os direitos e os interesses das pessoas em causa não sejam indevidamente lesados.

Por outro lado, o estatuto da pessoa em causa é igualmente relevante. Embora o teste da ponderação deva, em princípio, ser realizado tendo como referência uma pessoa comum, as situações específicas devem ser objeto de uma abordagem mais casuística: por exemplo, será

⁹¹ Ver as páginas 24 e 25 do Parecer 3/2013 do Grupo de Trabalho sobre a limitação da finalidade (já referido na nota 9).

⁹² «por exemplo, se se trata de um advogado ou de um médico».

⁹³ «por exemplo, serviços de computação em nuvem para a gestão de documentos pessoais, serviços de correio eletrónico, agendas, leitores de livros digitais com capacidade para anotações, e várias aplicações *Lifelog* que possam conter informações muito pessoais.»

relevante verificar se a pessoa em causa é uma criança⁹⁴ ou se de outro modo pertence a um segmento mais vulnerável da população que requeira proteção especial, como, por exemplo, os doentes mentais, os requerentes de asilo ou os idosos. A questão de saber se a pessoa em causa é um trabalhador, um estudante ou um doente, ou se de outro modo existe algum tipo de desequilíbrio na relação entre a posição da pessoa em causa e do responsável pelo tratamento, deve ser seguramente também relevante. É importante avaliar o efeito do tratamento efetivo nestas pessoas.

Por último, é importante salientar que nem todos os impactos negativos nas pessoas em causa têm o mesmo «valor» na ponderação. A finalidade do exercício de ponderação previsto no artigo 7.º, alínea f), não é evitar qualquer efeito negativo na pessoa em causa. A sua finalidade é antes evitar um impacto desproporcionado. Esta diferença é essencial. Por exemplo, a publicação de um artigo de jornal elaborado com base numa investigação aprofundada e de forma cuidadosa sobre um caso de alegada corrupção governamental pode prejudicar a reputação dos funcionários governamentais envolvidos e pode ter consequências significativas, nomeadamente a perda de reputação, a perda de eleições ou a prisão, mas pode ainda assim encontrar fundamento no artigo 7.º, alínea f)⁹⁵.

c) Equilíbrio provisório

Na ponderação dos interesses e dos direitos em jogo, tal como acima descrito, as medidas tomadas pelo responsável pelo tratamento para cumprir as suas obrigações gerais nos termos da diretiva, nomeadamente em matéria de proporcionalidade e de transparência, contribuirão substancialmente para assegurar que o responsável pelo tratamento dos dados preencha os requisitos estabelecidos no artigo 7.º, alínea f). O cumprimento integral deve implicar que o impacto nas pessoas seja reduzido, que seja *menos provável* que os interesses ou os direitos e liberdades fundamentais das pessoas em causa sejam afetados e que, por isso, seja *mais provável* que o responsável pelo tratamento dos dados possa invocar o artigo 7.º, alínea f). Tal

⁹⁴ Ver o Parecer 2/2009 do Grupo de Trabalho sobre a proteção dos dados pessoais das crianças (Orientações gerais e a situação especial das escolas), adotado em 11.2.2009 (WP160). Este parecer realça a vulnerabilidade específica da criança e, quando a criança esteja a ser representada, a necessidade de ter em conta o interesse superior da criança e não o do seu representante.

⁹⁵ Como já foi explicado, quaisquer derrogações relevantes necessárias para o tratamento para fins jornalísticos nos termos do artigo 9.º da diretiva devem ser igualmente tidas em conta.

deve incentivar os responsáveis pelo tratamento a cumprir melhor todas as disposições horizontais da diretiva⁹⁶.

Contudo, tal não significa que o cumprimento desses requisitos horizontais seja, enquanto tal, sempre suficiente para garantir uma base jurídica assente no artigo 7.º, alínea f). De facto, se assim fosse, o artigo 7.º, alínea f), seria supérfluo ou tornar-se-ia uma brecha que desproveria de sentido todo o artigo 7.º, que preconiza uma base jurídica específica adequada para o tratamento de dados.

Por esta razão, é importante realizar uma nova avaliação no exercício de ponderação nos casos em que - com base na análise preliminar - não seja clara a forma como o equilíbrio deve ser obtido. O responsável pelo tratamento pode considerar a possibilidade de introduzir medidas complementares, que vão além do cumprimento das disposições horizontais da diretiva, para ajudar a reduzir o impacto indevido do tratamento nas pessoas em causa.

As medidas complementares podem incluir, por exemplo, a disponibilização de um mecanismo viável e acessível para assegurar que as pessoas em causa possam optar, de forma incondicional, por não permitir o tratamento. Estas medidas complementares podem, nalguns casos (mas não em todos), ajudar a alterar o equilíbrio e ajudar a assegurar que o tratamento possa basear-se no artigo 7.º, alínea f), protegendo, ao mesmo, tempo, os direitos e os interesses das pessoas em causa.

(d) Garantias complementares aplicadas pelo responsável pelo tratamento

Como já foi explicado, a forma como o responsável pelo tratamento aplica medidas adequadas pode, nalgumas situações, ajudar a «alterar o equilíbrio». Se o resultado é ou não aceitável dependerá da avaliação no seu todo. Quanto mais significativo for o impacto na pessoa em causa, mais atenção deve ser dada às garantias relevantes.

São exemplos de medidas relevantes, entre outras, a limitação rigorosa do volume de dados recolhidos e a eliminação imediata de dados após utilização. Embora algumas dessas medidas

⁹⁶ Quanto ao papel importante do «respeito pelas disposições horizontais», ver igualmente a página 54 do Parecer 3/2013 do Grupo de Trabalho sobre a limitação da finalidade, já referido na nota 9.

possam já ser obrigatórias nos termos da diretiva, são muitas vezes moduláveis e deixam margem para que os responsáveis pelo tratamento assegurem uma melhor proteção das pessoas em causa. Por exemplo, o responsável pelo tratamento pode recolher menos dados ou fornecer informações complementares em relação ao que está especificamente previsto nos artigos 10.º e 11.º da diretiva.

Noutros casos, as garantias não são *expressamente* exigidas nos termos da Diretiva, mas podem bem vir a sê-lo nos termos da proposta de regulamento, ou são exigidas apenas em situações específicas, por exemplo:

- medidas técnicas e organizativas para assegurar que os dados não possam ser utilizados para tomar decisões ou outras medidas em relação às pessoas («separação funcional», como é frequentemente o caso no âmbito de uma investigação),
- utilização ampla de técnicas de anonimização,
- agregação de dados,
- tecnologias para reforçar a proteção da privacidade, privacidade desde a conceção, avaliações de impacto na privacidade e na proteção de dados,
- maior transparência,
- direito generalizado e incondicional de optar por não permitir o tratamento,
- portabilidade dos dados e medidas afins para capacitar as pessoas em causa.

O Grupo de Trabalho observa que, no que se refere a algumas questões-chave, nomeadamente à separação funcional e às técnicas de anonimização, já foram fornecidas algumas orientações nas partes relevantes dos seus pareceres sobre limitação da finalidade, dados abertos e técnicas de anonimização⁹⁷.

No que respeita à utilização de pseudónimos e à criptografia, o Grupo de Trabalho gostaria de salientar que o facto de os dados não serem diretamente identificáveis não afeta, por si só, a

⁹⁷ Ver as secções III.2.3 e III.2.5 e o anexo 2 do Parecer 3/2013 do Grupo de Trabalho sobre a limitação da finalidade, já referido na nota 9, quanto ao tratamento posterior para fins históricos, estatísticos e científicos e quanto aos grandes volumes de dados e aos dados abertos; ver igualmente as partes relevantes do Parecer 6/2013 do Grupo de Trabalho sobre os dados abertos (já referido na nota 88) e o Parecer 5/2014 do Grupo de Trabalho sobre técnicas de anonimização.

apreciação da legitimidade do tratamento: não deve considerar-se que esse facto torna legítimo um tratamento ilegítimo⁹⁸.

Ao mesmo tempo, a utilização de pseudónimos e a criptografia, tal como quaisquer outras medidas técnicas e organizativas introduzidas para proteger informações pessoais, desempenharão um papel importante no que respeita à avaliação do potencial impacto do tratamento na pessoa em causa, pelo que, nalguns casos, podem contribuir para alterar o equilíbrio a favor do responsável pelo tratamento. A utilização de formas de tratamento de dados pessoais que comportem menos riscos (por exemplo, dados pessoais que sejam encriptados enquanto estão armazenados ou em trânsito, ou dados pessoais que sejam menos direta e rapidamente identificáveis) significa geralmente que a probabilidade de os interesses e os direitos e liberdades fundamentais da pessoa em causa serem afetados é menor.

Em relação a estas garantias – e à avaliação global do equilíbrio – o Grupo de Trabalho gostaria de salientar três questões específicas que muitas vezes desempenham um papel essencial no contexto do artigo 7.º, alínea f):

- a relação entre o teste da ponderação, a transparência e o princípio da responsabilidade,
- o direito da pessoa em causa de se opor ao tratamento e, para além da oposição, a possibilidade de optar por não permitir o tratamento sem que seja necessária qualquer justificação, e
- a capacitação das pessoas em causa: a portabilidade dos dados e a existência de mecanismos viáveis que permitam à pessoa em causa aceder, alterar, eliminar, transferir ou de outro modo proceder (ou autorizar que terceiros procedam) ao tratamento posterior dos seus próprios dados.

Dada a sua importância, estes temas serão discutidos sob epígrafes distintas.

⁹⁸ Ver, quanto a este ponto, as alterações aprovadas pela Comissão LIBE no respetivo relatório final, em especial a alteração n.º 15 relativa ao considerando 38, que relaciona a utilização de pseudónimos com as expectativas legítimas da pessoa em causa.

III.3.5. Responsabilidade e transparência

Em primeiro lugar, antes de ter lugar uma operação de tratamento de dados com base no artigo 7.º, alínea f), o responsável pelo tratamento tem a responsabilidade de verificar se tem um interesse legítimo, se o tratamento é necessário para prosseguir esse interesse legítimo e se, no caso específico, os interesses e os direitos das pessoas em causa prevalecem sobre esse interesse.

Nesse sentido, o artigo 7.º, alínea f), baseia-se no princípio da responsabilidade. O responsável pelo tratamento deve levar previamente a cabo um teste cuidadoso e eficaz, com base nos factos específicos do caso e não de forma abstrata, tendo em conta igualmente as expectativas razoáveis das pessoas em causa. A título de boa prática, sempre que adequado, a realização desse teste deve ser documentada de forma suficientemente pormenorizada e transparente para que a aplicação completa e correta do teste possa ser verificada - quando necessário - pelas partes interessadas, nomeadamente as pessoas em causa e as autoridades responsáveis pela proteção de dados, e, em última análise, pelos tribunais.

O responsável pelo tratamento começará por definir o interesse legítimo e realizar o teste da ponderação, mas não se trata necessariamente da avaliação final e definitiva: se, na realidade, o interesse prosseguido não for o que foi especificado pelo responsável pelo tratamento ou se o responsável pelo tratamento não tiver definido o interesse de forma suficientemente pormenorizada, o equilíbrio deve ser reavaliado com base no interesse efetivo, a determinar por uma autoridade responsável pela proteção de dados ou por um tribunal⁹⁹. Como acontece relativamente a outros aspetos essenciais da proteção de dados, tais como a identificação do responsável pelo tratamento de dados ou a especificação da finalidade¹⁰⁰, o importante é a realidade que está por trás de qualquer afirmação feita pelo responsável pelo tratamento.

O conceito de responsabilidade está estreitamente ligado ao conceito de transparência. Para possibilitar que as pessoas em causa exerçam os seus direitos e permitir um escrutínio público mais alargado pelas partes interessadas, o Grupo de Trabalho recomenda que os responsáveis pelo tratamento expliquem às pessoas em causa, de forma clara e acessível, as razões pelas quais consideram que sobre os seus interesses não prevalecem os interesses ou os direitos e

⁹⁹ Por exemplo, no seguimento de uma queixa ou do exercício do direito de oposição nos termos do artigo 14.º.

¹⁰⁰ Ver os pareceres referidos na nota 9.

liberdades fundamentais das pessoas em causa, e lhes expliquem igualmente que garantias acionaram para proteger os dados pessoais, incluindo, sempre que adequado, o direito de optar por não permitir o tratamento¹⁰¹.

A este respeito, o Grupo de Trabalho salienta que a legislação em matéria de defesa do consumidor, em especial as leis que defendem os consumidores contra práticas comerciais desleais, é igualmente muito relevante neste contexto.

Se o responsável pelo tratamento esconder informações importantes a respeito de uma inesperada utilização posterior dos dados, camufladas em cláusulas jurídicas escritas em caracteres reduzidos num contrato, tal pode violar as normas de defesa do consumidor relativas às cláusulas contratuais abusivas (nomeadamente a proibição de «cláusulas-surpresa») e também não preencherá os requisitos previstos no artigo 7.º, alínea a), para um consentimento válido e informado, nem os requisitos previstos no artigo 7.º, alínea f), em termos de expectativas razoáveis da pessoa em causa e de equilíbrio de interesses global aceitável. Obviamente, levanta também questões de conformidade com o artigo 6.º no que se refere à necessidade de um tratamento leal e lícito dos dados pessoais.

Por exemplo, em muitos casos, os utilizadores de serviços em linha «gratuitos», tais como motores de busca, correio eletrónico, redes sociais, armazenamento de ficheiros ou outras aplicações em linha ou móveis, não estão plenamente conscientes da medida em que a sua atividade é registada e analisada a fim de criar valor para o prestador do serviço, pelo que não estão preocupados com os riscos envolvidos.

Para capacitar as pessoas em causa nessas situações, uma das primeiras condições prévias necessárias¹⁰² – mas de modo nenhum suficiente em si mesma – é tornar claro que os serviços não são gratuitos e que, pelo contrário, os consumidores pagam utilizando os seus dados

¹⁰¹ Tal como explicado na página 46 do Parecer 3/2013 do Grupo de Trabalho sobre a limitação da finalidade (já referido na nota 9), no caso da elaboração de perfis e da automatização das decisões, «para assegurar a transparência, as pessoas em causa/os consumidores devem ter acesso aos seus ‘perfis’, bem como à lógica da tomada de decisão (algoritmo) que conduziu ao desenvolvimento do perfil. Por outras palavras: as organizações devem divulgar os respetivos critérios de decisão. Trata-se de uma garantia crucial e ainda mais importante no mundo dos grandes volumes de dados». A questão de saber se uma organização oferece ou não essa transparência é um fator muito relevante a ter em conta igualmente no exercício de ponderação.

¹⁰² Quanto a outras garantias possíveis no que respeita às situações, cada vez mais comuns, em que os consumidores pagam com os seus dados pessoais, ver a secção III.3.6, em especial as páginas 47 e 48, sobre «*Alternativas aos serviços em linha ‘gratuitos’ respeitadoras da proteção de dados*» e sobre «*Portabilidade dos dados, o programa ‘Midata’ e questões afins*».

pessoais. As condições e as garantias das quais depende a utilização dos dados devem também ser claramente explicitadas em cada caso, de forma a garantir a validade do consentimento previsto no artigo 7.º, alínea a), ou um equilíbrio favorável nos termos do artigo 7.º, alínea f).

III.3.6. Direito de oposição e outros

a) Direito de oposição nos termos do artigo 14.º da diretiva

O artigo 7.º, alíneas e) e f), é especial no sentido em que, embora assente sobretudo numa avaliação objetiva dos interesses e dos direitos envolvidos, permite igualmente que a pessoa em causa exerça a sua autodeterminação através de um direito de oposição¹⁰³: pelo menos no caso destes dois fundamentos, o artigo 14.º, alínea a), da diretiva dispõe que («salvo disposição em contrário do direito nacional») a pessoa em causa pode opor-se «em qualquer altura, por razões preponderantes e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objeto de tratamento». Acrescenta que, em caso de oposição justificada, deve ser posto termo ao tratamento dos seus dados.

Assim, em princípio, nos termos da legislação atual, a pessoa em causa terá de demonstrar que possui «interesses preponderantes e legítimos» para impedir o tratamento dos seus dados pessoais (artigo 14.º, alínea a)), exceto no contexto de atividades de marketing direto, no qual não é necessário que a oposição seja justificada (artigo 14.º, alínea b)).

Não deve considerar-se que tal contradiz o teste da ponderação previsto no artigo 7.º, alínea f), que é realizado *a priori*: antes complementa essa ponderação, no sentido em que, sempre que o tratamento seja autorizado na sequência de uma avaliação razoável e objetiva dos diferentes direitos e interesses em jogo, a pessoa em causa tem ainda uma possibilidade *complementar* de se opor por motivos relacionados com a sua situação específica. Tal deverá então conduzir a uma nova avaliação, tendo em conta os argumentos específicos apresentados

¹⁰³ Este direito de oposição não deve ser confundido com o consentimento baseado no artigo 7.º, alínea a), que dispõe que o responsável pelo tratamento não pode tratar os dados antes de obter esse consentimento. No âmbito do artigo 7.º, alínea f), o responsável pelo tratamento pode tratar os dados, sob reserva de determinadas condições e garantias, desde que a pessoa em causa não se tenha oposto. Neste sentido, o direito de oposição pode ser considerado sobretudo uma forma específica de optar por não permitir o tratamento. Para mais pormenores, ver o Parecer 15/2011 do Grupo de Trabalho sobre a definição de consentimento (referido na nota 2).

pela pessoa em causa. Esta nova avaliação é, em princípio, novamente objeto de verificação por uma autoridade responsável pela proteção de dados ou pelos tribunais.

b) Para além da oposição: o papel da opção de não permitir o tratamento enquanto garantia complementar

O Grupo de Trabalho salienta que, embora o direito de oposição previsto no artigo 14.º, alínea a), tenha de ser justificado pela pessoa em causa, nada impede que o responsável pelo tratamento lhe dê uma possibilidade de optar por não permitir o tratamento, que seja mais abrangente e que não exija qualquer demonstração complementar dos interesses legítimos (preponderantes ou outros) por parte da pessoa em causa. Não é necessário que este direito incondicional se baseie na situação específica das pessoas em causa.

De facto, especialmente em caso de dúvida, quando o equilíbrio seja difícil de alcançar, um mecanismo bem concebido e viável de exclusão do tratamento, mesmo que não proporcione necessariamente às pessoas em causa todos os elementos que satisfazem as condições para um consentimento válido nos termos do artigo 7.º, alínea a), pode desempenhar um papel importante na salvaguarda dos direitos e dos interesses das pessoas em causa.

Para tal, é necessário uma abordagem diferenciada, que estabeleça uma distinção entre os casos em que é exigido o consentimento prévio previsto no artigo 7.º, alínea a), e os casos em que uma possibilidade viável de optar por não permitir o tratamento (conjuntamente com outras medidas complementares possíveis) pode contribuir para proteger as pessoas em causa nos termos do artigo 7.º, alínea f).

Quanto maior for o âmbito de aplicação do mecanismo de exclusão do tratamento e quanto mais fácil for utilizá-lo, mais este contribuirá para alterar o equilíbrio no sentido de que o tratamento encontre uma base jurídica no artigo 7.º, alínea f).

Ilustração: evolução na abordagem ao marketing direto

Para ilustrar como é estabelecida uma distinção entre os casos em que é exigido o consentimento previsto no artigo 7.º, alínea a), e os casos em que a opção de não permitir o tratamento pode ser utilizada como garantia nos termos do artigo 7.º, alínea f), é útil recorrer

ao exemplo do marketing direto, relativamente ao qual existe, desde o início, uma disposição específica de exclusão de tratamento no artigo 14.º, alínea b), da diretiva. A fim de acompanhar os novos desenvolvimentos tecnológicos, esta disposição foi posteriormente complementada por disposições específicas na diretiva «privacidade e comunicações eletrónicas»¹⁰⁴.

Nos termos do artigo 13.º da diretiva «privacidade e comunicações eletrónicas», no que respeita a determinados tipos – mais intrusivos – de atividades de marketing direto (tais como o marketing através de correio eletrónico e aparelhos de chamadas automáticas), o consentimento é a regra. A título excecional, nas relações com os clientes existentes, quando um responsável pelo tratamento publicite os seus próprios produtos ou serviços «análogos», é suficiente que seja dada aos clientes a possibilidade (incondicional) de optar por não permitir o tratamento sem necessidade de justificação.

As tecnologias evoluíram, o que tornou necessário encontrar soluções semelhantes e relativamente simples, seguindo a mesma lógica, para as novas práticas de marketing.

Em primeiro lugar, a forma como o material publicitário é divulgado evoluiu: já não se trata apenas de mensagens que chegam às caixas de correio eletrónico, mas também de mensagens publicitárias direcionadas para padrões de comportamento que surgem nos smartphones e nos ecrãs de computador. Num futuro próximo, a publicidade pode ser igualmente incorporada em objetos inteligentes interligados na Internet das coisas.

Em segundo lugar, as mensagens publicitárias são cada vez mais especificamente direcionadas: já não se baseiam em simples perfis dos clientes, antes as informações sobre as atividades dos consumidores são cada vez mais rastreadas e conservadas, em linha e sem ser em linha, e analisadas através de métodos automáticos mais sofisticados¹⁰⁵.

Em consequência destes desenvolvimentos, o objeto do exercício de ponderação alterou-se: já não se trata do direito à liberdade de expressão para fins comerciais, mas sobretudo do interesse económico das organizações empresariais em conhecer os seus clientes através do

¹⁰⁴ Quanto ao artigo 13.º da diretiva «privacidade e comunicações eletrónicas», ver igualmente a secção III.2.4 do Parecer 3/2013 do Grupo de Trabalho sobre a limitação da finalidade (já referido na nota 9).

¹⁰⁵ Ver a secção III.2.5 e o anexo 2 (quanto aos grandes volumes de dados e à abertura de dados) do parecer do Grupo de Trabalho sobre a limitação da finalidade (já referido na nota 9).

rastreio e da monitorização das informações sobre as suas atividades em linha e sem ser em linha, o qual deve ser ponderado em relação aos direitos (fundamentais) ao respeito pela vida privada e à proteção de dados pessoais dessas pessoas e ao seu interesse em não serem indevidamente monitorizadas.

Esta mudança nos modelos comerciais predominantes e a valorização dos dados pessoais como um trunfo para as organizações empresariais explica a recente exigência de consentimento neste contexto, nos termos do artigo 5.º, n.º 3, e do artigo 13.º da diretiva «privacidade e comunicações eletrónicas».

Por conseguinte, existem diferentes normas específicas aplicáveis consoante o tipo de marketing, nomeadamente:

- o direito incondicional de oposição ao marketing direto (concebido para o contexto tradicional do correio postal e para a publicitação de produtos análogos) nos termos do artigo 14.º, alínea b), da diretiva; nesse caso, o artigo 7.º, alínea f), pode constituir o fundamento jurídico,
- a exigência de consentimento nos termos do artigo 13.º da diretiva «privacidade e comunicações eletrónicas» no que respeita à utilização de sistemas de chamada automatizados, fax, mensagens de texto e correio eletrónico para fins de marketing (sob reserva de exceções)¹⁰⁶, e aplicação *de facto* do artigo 7.º, alínea a), da diretiva relativa à proteção de dados.
- a exigência de consentimento nos termos do artigo 5.º, n.º 3, da **diretiva** «privacidade e comunicações eletrónicas» (e do artigo 7.º, alínea a), da diretiva relativa à proteção de dados) no que respeita à publicidade comportamental, baseada em técnicas de rastreamento, tais como cookies que armazenam informações no terminal do utilizador¹⁰⁷.

Embora os fundamentos jurídicos aplicáveis sejam claros no que se refere aos artigos 5.º, n.º 3, e 13.º da diretiva «privacidade e comunicações eletrónicas», nem todos os tipos de marketing são abrangidos e é desejável que existam orientações sobre quais as situações que

¹⁰⁶ Ver igualmente o artigo 13.º, n.º 3, da diretiva «privacidade e comunicações eletrónicas», que permite aos Estados-Membros escolher entre o consentimento prévio ou a opção de não permitir o tratamento no que respeita ao marketing direto através de outros meios.

¹⁰⁷ Quanto à aplicação desta disposição, ver o Parecer 2/2010 do Grupo de Trabalho sobre publicidade comportamental em linha (WP171).

exigem o consentimento previsto no artigo 7.º, alínea a), e quais as situações em que é alcançado um equilíbrio nos termos do artigo 7.º, alínea f), incluindo a possibilidade de optar por não permitir o tratamento.

A este respeito, é útil recordar o parecer do Grupo de Trabalho sobre a limitação da finalidade, que refere expressamente que, «quando uma organização pretenda especificamente analisar ou prever as preferências, o comportamento e as atitudes pessoais dos clientes individuais, que posteriormente servirão de inspiração para ‘medidas ou decisões’ tomadas em relação a esses clientes [...], o consentimento prévio, livre, específico, informado e inequívoco é quase sempre exigido, caso contrário a utilização posterior dos dados não pode ser considerada compatível. É importante que esse consentimento seja exigido, por exemplo, para o rastreamento e a elaboração de perfis para fins de marketing direto, publicidade comportamental, corretagem de dados, publicidade baseada na localização ou pesquisa de mercado digital baseada no rastreamento»¹⁰⁸.

Alternativas aos serviços em linha «gratuitos» respeitadoras da proteção de dados

Num contexto em que os clientes que aderem a serviços em linha «gratuitos» na realidade «pagam» esses serviços ao permitir a utilização dos seus dados pessoais, se o responsável pelo tratamento disponibilizar também uma versão alternativa dos seus serviços, na qual os «dados pessoais» não sejam utilizados para fins de marketing, tal contribui também para uma avaliação favorável do equilíbrio – ou para a conclusão de que o cliente teve realmente liberdade de escolha e, por conseguinte, foi dado consentimento válido nos termos do artigo 7.º, alínea a).

Quando tais serviços alternativos não estejam disponíveis, é mais difícil argumentar que foi dado consentimento válido (e livre) nos termos do artigo 7.º, alínea a), pelo simples facto de os serviços gratuitos terem sido utilizados ou que o equilíbrio previsto no artigo 7.º, alínea f), deve ser favorável ao responsável pelo tratamento.

As considerações precedentes sublinham o papel importante que as garantias complementares, nomeadamente a disponibilização de um mecanismo viável de exclusão do

¹⁰⁸ Ver o anexo II (quanto aos grandes volumes de dados e aos dados abertos) do parecer (já referido na nota 9), página 45.

tratamento, podem desempenhar na alteração do equilíbrio provisório. Ao mesmo tempo, mostram igualmente que, nalguns casos, o artigo 7.º, alínea f), não pode ser invocado como fundamento para o tratamento e os responsáveis pelo tratamento devem obter um consentimento válido nos termos do artigo 7.º, alínea a), - ou satisfazer outras condições estabelecidas na diretiva – para que o tratamento possa ser realizado.

Portabilidade dos dados, o programa «Midata» e questões afins

Entre as garantias complementares que podem ajudar a alterar o equilíbrio, há que dar especial atenção à portabilidade dos dados e medidas afins, que podem ser cada vez mais relevantes num ambiente em linha. O Grupo de Trabalho recorda o seu parecer sobre a limitação da finalidade, no qual salientou que «em muitas situações, a aplicação de garantias, tais como permitir que as pessoas em causa/os clientes tenham acesso direto aos seus dados em formato portátil, acessível e de leitura ótica, pode ajudar a capacitá-las e a compensar o desequilíbrio económico existente entre as grandes empresas, por um lado, e as pessoas em causa/os consumidores, por outro. Permite igualmente às pessoas «partilhar da riqueza» gerada pelos grandes volumes de dados e incentiva os produtores a disponibilizar mais funcionalidades e aplicações aos seus utilizadores¹⁰⁹.

A existência de mecanismos viáveis que permitam às pessoas em causa aceder, alterar, eliminar, transferir ou de outro modo proceder (ou autorizar que terceiros procedam) ao tratamento posterior dos seus próprios dados capacitará as pessoas em causa e permitir-lhes-á retirar mais benefícios dos serviços digitais. Além disso, pode promover um ambiente de mercado mais concorrencial ao permitir que os clientes mudem mais facilmente de prestador (por exemplo, no contexto das operações bancárias em linha ou, no caso de fornecedores de energia, no contexto das redes inteligentes). Por último, pode igualmente contribuir para o desenvolvimento, por terceiros que tenham possibilidade de aceder aos dados dos clientes a pedido e com base no consentimento destes, de serviços complementares de valor

¹⁰⁹ «Ver iniciativas como o programa ‘Midata’, no Reino Unido, que se baseiam no princípio fundamental de que os dados devem ser devolvidos aos consumidores. O Midata é um programa voluntário que, com o tempo, deverá facilitar cada vez mais o acesso dos consumidores aos respetivos dados pessoais em formato portátil e eletrónico. A ideia-chave é a de que os consumidores devem beneficiar também dos grandes volumes de dados através do acesso às informações que lhes dizem respeito, de forma a poderem fazer melhores escolhas. Ver igualmente as iniciativas ‘Green button’, que permitem aos consumidores aceder às informações sobre o seu próprio consumo de energia». Para mais informações sobre as iniciativas existentes no Reino Unido e em França, ver <http://www.midadoslab.org.uk/> e <http://mesinfos.fing.org/>.

acrescentado. Por conseguinte, nesta perspetiva, a portabilidade dos dados é vantajosa não apenas para a proteção de dados mas igualmente para a concorrência e para a defesa dos consumidores¹¹⁰.

IV. Observações finais

No presente parecer, o Grupo de Trabalho analisou os critérios estabelecidos no artigo 7.º da diretiva, que legitimam o tratamento de dados. Para além de orientações sobre a interpretação e a aplicação práticas do artigo 7.º, alínea f), no atual quadro jurídico, o presente parecer pretende formular recomendações que auxiliem os decisores políticos na ponderação das mudanças a efetuar ao atual quadro jurídico em matéria de proteção de dados. Antes da apresentação dessas recomendações, segue-se um resumo das principais conclusões relativas à interpretação do artigo 7.º.

IV.1. Conclusões

Síntese do artigo 7.º

O artigo 7.º exige que tratamento de dados pessoais só possa ser efetuado se pelo menos um dos seis fundamentos jurídicos elencados nesse artigo for aplicável.

O primeiro fundamento, no artigo 7.º, alínea a), centra-se no consentimento da pessoa em causa como fundamento para o tratamento legítimo. Os restantes fundamentos, pelo contrário, permitem o tratamento – sob reserva de garantias – em situações nas quais, independentemente do consentimento, seja adequado e necessário tratar os dados num determinado contexto para prosseguir um interesse legítimo específico.

Cada uma das alíneas b), c), d) e e) especifica um determinado contexto no qual o tratamento de dados pessoais pode ser considerado legítimo. As condições aplicáveis em cada um desses diferentes contextos exigem especial atenção, uma vez que determinam o alcance dos vários fundamentos para o tratamento legítimo. Mais concretamente, os critérios de que o tratamento

¹¹⁰ Quanto ao direito à portabilidade dos dados, ver o artigo 18.º da proposta de regulamento.

seja «necessário para a execução de um contrato», «necessário para cumprir uma obrigação legal», «necessário para a proteção de interesses vitais da pessoa em causa» e «necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública» contêm diferentes requisitos, os quais foram analisados na secção III.2.

A alínea f) refere-se, de forma mais genérica, a (qualquer tipo de) interesse legítimo prosseguido pelo responsável pelo tratamento (em qualquer contexto). No entanto, esta disposição geral está expressamente subordinada a um teste da ponderação complementar, que exige que os interesses legítimos do responsável pelo tratamento – ou do terceiro ou terceiros a quem os dados sejam comunicados – sejam ponderados em relação aos interesses ou aos direitos fundamentais das pessoas em causa.

Papel do artigo 7.º, alínea f)

O artigo 7.º, alínea f), não deve ser considerado um fundamento jurídico que só pode ser utilizado com parcimónia, como «último recurso» para colmatar lacunas em situações raras e imprevistas - ou como última possibilidade quando nenhum outro fundamento seja aplicável. De igual modo, não deve ser considerado uma opção preferencial nem a sua utilização deve ser indevidamente alargada por ser considerada menos restritiva do que os restantes fundamentos. Pelo contrário, trata-se de um meio tão válido como qualquer um dos outros fundamentos que legitimam o tratamento de dados pessoais.

A utilização correta do artigo 7.º, alínea f), nas condições certas e sob reserva de garantias adequadas, pode ajudar a evitar a utilização abusiva, e a invocação excessiva, de outros fundamentos jurídicos. Uma avaliação adequada do equilíbrio nos termos do artigo 7.º, alínea f), muitas vezes com a possibilidade de optar por não permitir o tratamento, pode, nalguns casos, ser uma alternativa válida à utilização incorreta, por exemplo, do fundamento do «consentimento» ou da necessidade «para a execução de um contrato». Neste sentido, o artigo 7.º, alínea f), apresenta garantias complementares em comparação com os restantes fundamentos predeterminados. Por conseguinte, não deve ser considerado o «elo mais fraco» ou uma porta aberta para legitimar todas as atividades de tratamento de dados que não sejam abrangidas por nenhum dos outros fundamentos jurídicos.

Interesses legítimos do responsável pelo tratamento / interesses ou direitos fundamentais da pessoa em causa

O conceito de «interesse» do responsável pelo tratamento é o interesse mais amplo que este pode ter no tratamento, ou o benefício que retira – ou que a sociedade pode retirar – do tratamento. Pode ser preponderante, simples ou mais controverso. Por conseguinte, as situações visadas pelo artigo 7.º, alínea f), podem ir desde o exercício de direitos fundamentais ou a proteção de interesses pessoais ou sociais importantes até outros contextos menos óbvios ou até problemáticos.

Para ser considerado «legítimo» e para ser relevante nos termos do artigo 7.º, alínea f), o interesse deverá ser lícito, ou seja, deverá respeitar o direito da UE e o direito nacional. Deve também ser definido de forma suficientemente clara e precisa para permitir a realização do teste da ponderação em relação aos interesses e aos direitos fundamentais da pessoa em causa. Deve igualmente consistir num interesse real e atual – ou seja, não deve ser especulativo.

O facto de o responsável pelo tratamento, ou o terceiro a quem se pretende que os dados sejam comunicados, ter tal interesse legítimo não significa necessariamente que possa invocar o artigo 7.º, alínea f), como fundamento jurídico para o tratamento. A questão de saber se o artigo 7.º, alínea f), pode ser invocado dependerá do resultado do teste da ponderação subsequente. O tratamento deve ser igualmente «necessário para prosseguir interesses legítimos» do responsável pelo tratamento ou – em caso de comunicação de dados – de terceiros. Deve dar-se sempre preferência aos meios menos invasivos que sirvam a mesma finalidade.

O conceito de «interesses» das pessoas em causa é definido de forma ainda mais abrangente, uma vez que não exige um elemento de «legitimidade». Se o responsável pelo tratamento dos dados, ou um terceiro, pode prosseguir quaisquer interesses, desde que não sejam ilegítimos, a pessoa em causa, por sua vez, tem direito a que todos os seus tipos de interesses sejam tidos em conta e ponderados em relação aos interesses do responsável pelo tratamento, ou de terceiros, contanto que sejam relevantes no âmbito de aplicação da diretiva.

Aplicação do teste da ponderação

Ao interpretar o âmbito de aplicação do artigo 7.º, alínea f), o Grupo de Trabalho visa a adoção de uma abordagem equilibrada, que assegure aos responsáveis pelo tratamento a necessária flexibilidade em situações nas quais não se verifique um impacto indevido nas pessoas em causa, proporcionando, ao mesmo tempo, às pessoas em causa segurança jurídica e garantias suficientes de que esta disposição aberta não será utilizada de forma abusiva.

Para realizar este teste da ponderação é importante ter em conta, antes de mais, a natureza e a origem dos interesses legítimos, e a questão de saber se o tratamento é necessário para prosseguir esses interesses, por um lado, e o impacto nas pessoas em causa, por outro. Esta avaliação inicial deve ter em conta as medidas que o responsável pelo tratamento tenciona adotar para cumprir o disposto na diretiva, tais como a transparência e a recolha limitada de dados.

Após analisar e ponderar cada um dos lados em relação ao outro é possível estabelecer um «equilíbrio» provisório: pode retirar-se uma conclusão preliminar sobre se os interesses legítimos do responsável pelo tratamento prevalecem sobre os direitos e os interesses das pessoas em causa. Contudo, pode haver casos em que o resultado do teste da ponderação não seja claro e em que haja dúvidas sobre se o interesse legítimo do responsável pelo tratamento (ou de terceiros) prevalece e se o tratamento pode basear-se no artigo 7.º, alínea f).

Por esta razão, é importante realizar uma nova avaliação no exercício de ponderação. Nesta fase, o responsável pelo tratamento pode considerar a possibilidade de introduzir medidas complementares, que vão além do cumprimento das demais disposições horizontais da diretiva, que ajudem a proteger as pessoas em causa. As medidas complementares podem incluir, por exemplo, a disponibilização de um mecanismo viável e acessível para assegurar que as pessoas em causa possam optar, de forma incondicional, por não permitir o tratamento.

Fatores-chave a ter em conta na aplicação do teste da ponderação

Com base nas considerações que precedem, os fatores úteis a ter em conta na realização do teste da ponderação são, entre outros:

- a natureza e a origem do interesse legítimo, nomeadamente:
 - a questão de saber se o tratamento de dados é necessário para o exercício de um direito fundamental, ou
 - se de outro modo é de interesse público ou é reconhecido em termos sociais, culturais ou jurídicos/regulamentares na comunidade em causa;

- o impacto nas pessoas em causa, nomeadamente:
 - a natureza dos dados, como a questão de saber se o tratamento envolve dados que possam ser considerados sensíveis ou que tenham sido obtidos de fontes publicamente disponíveis,
 - a forma como os dados são tratados, incluindo a questão de saber se os dados são divulgados publicamente ou de outro modo colocados à disposição de um grande número de pessoas, ou se grandes volumes de dados pessoais são tratados ou combinados com outros dados (por exemplo, na elaboração de perfis para fins comerciais, de aplicação da lei ou outros),
 - as expectativas razoáveis da pessoa em causa, em especial quanto à utilização e à comunicação dos dados no contexto relevante,
 - o estatuto do responsável pelo tratamento dos dados e da pessoa em causa, incluindo a relação de forças entre a pessoa em causa e o responsável pelo tratamento dos dados, ou a questão de saber se a pessoa em causa é uma criança ou de outro modo pertence a um segmento mais vulnerável da população;

- as garantias complementares para evitar um impacto indevido nas pessoas em causa, nomeadamente:
 - a minimização dos dados (por exemplo, a limitação rigorosa do volume de dados recolhidos e a eliminação imediata de dados após utilização);
 - medidas técnicas e organizativas para assegurar que os dados não possam ser utilizados para tomar decisões ou outras medidas em relação às pessoas («separação funcional»);

- a utilização ampla de técnicas de anonimização, agregação de dados, tecnologias para reforçar a proteção da privacidade, privacidade desde a concepção, avaliações de impacto na privacidade e na proteção de dados;
- maior transparência, direito generalizado e incondicional de optar por não permitir o tratamento, portabilidade dos dados e medidas afins para capacitar as pessoas em causa.

Responsabilidade, transparência, direito de oposição e outros

Relacionadas com estas garantias – e com a avaliação global do equilíbrio - há três questões que frequentemente desempenham um papel crucial no âmbito do artigo 7.º, alínea f), pelo que exigem especial atenção:

- a existência de uma eventual necessidade de medidas complementares para aumentar a transparência e a responsabilidade;
- o direito da pessoa em causa de se opor ao tratamento e, para além dessa oposição, a possibilidade de optar por não permitir o tratamento sem que seja necessária qualquer justificação;
- a capacitação das pessoas em causa: portabilidade dos dados e existência de mecanismos viáveis que permitam à pessoa em causa aceder, alterar, eliminar, transferir ou de outro modo proceder (ou autorizar que terceiros procedam) ao tratamento posterior dos seus próprios dados.

IV. 2. Recomendações

O texto atual do artigo 7.º, alínea f), da diretiva é um texto aberto. Esta redação flexível deixa uma grande margem de interpretação e já algumas vezes conduziu – como a experiência demonstra – à falta de previsibilidade e de segurança jurídica. No entanto, se for utilizado no contexto correto e com a aplicação dos critérios adequados, tal como enunciados no presente parecer, o artigo 7.º, alínea f), tem um papel essencial a desempenhar enquanto fundamento jurídico para o tratamento legítimo de dados.

Por conseguinte, o Grupo de Trabalho apoia a atual abordagem prevista no artigo 6.º da proposta de regulamento, que mantém o equilíbrio de interesses como fundamento jurídico distinto. No entanto, são bem-vindas mais orientações para garantir a aplicação adequada do teste da ponderação.

Âmbito de aplicação e meios de especificação acrescidos

Um requisito essencial é que a disposição se mantenha suficientemente flexível e reflita quer as perspetivas do responsável pelo tratamento de dados e da pessoa em causa quer a natureza dinâmica dos contextos relevantes. Por esta razão, o Grupo de Trabalho considera que é desaconselhável incluir – no texto da proposta de regulamento ou em atos delegados – listas pormenorizadas e exaustivas de situações nas quais o interesse pode ser qualificado *de facto* como legítimo. O Grupo de Trabalho opõe-se igualmente a que se defina os casos em que o interesse ou o direito de uma das partes deve, *enquanto princípio* ou *enquanto pressuposto*, prevalecer sobre o interesse ou o direito da outra parte apenas devido à natureza desse interesse ou desse direito, ou porque tenham sido tomadas determinadas medidas de proteção, como, por exemplo, a mera utilização de pseudónimos. Tal pode não só induzir em erro mas também ser desnecessariamente prescritivo.

Em vez de fazer juízos de valor definitivos quanto ao mérito dos diferentes direitos e interesses, o Grupo de Trabalho reafirma o *papel crucial do teste da ponderação* na avaliação prevista no artigo 7.º, alínea f). É necessário manter a flexibilidade do teste, mas a forma como este é realizado deve ser mais eficaz na prática e permitir um cumprimento mais efetivo. Tal deve traduzir-se numa obrigação *acrescida de responsabilidade* para os responsáveis pelo tratamento dos dados, no âmbito da qual cabe ao responsável pelo tratamento a responsabilidade de *demonstrar* que sobre o seu interesse não prevalecem os interesses e os direitos da pessoa em causa.

Orientações e responsabilidade

Para alcançar este objetivo, o Grupo de Trabalho recomenda que a proposta de regulamento forneça orientações, da seguinte forma:

- 1) Será útil identificar e prever num considerando uma lista não exaustiva dos fatores-chave a ter em conta na aplicação do teste da ponderação, tais como a natureza e a origem do interesse legítimo, o impacto nas pessoas em causa e as garantias complementares que podem ser aplicadas pelo responsável pelo tratamento para evitar qualquer impacto indevido do tratamento nas pessoas em causa. Estas garantias podem incluir, entre outros,
 - a separação funcional dos dados, a utilização adequada de técnicas de anonimização, a criptografia e outras medidas técnicas e organizativas para limitar os potenciais riscos para as pessoas em causa,
 - bem como medidas para garantir às pessoas em causa uma maior transparência e liberdade de escolha, tais como, sempre que adequado, a possibilidade de optar, de forma incondicional, por não permitir o tratamento, sem custos e que possa ser fácil e eficazmente invocada.

- 2) O Grupo de Trabalho é igualmente a favor de que a proposta de regulamento esclareça melhor a forma como o responsável pelo tratamento pode *demonstrar*¹¹¹ a sua responsabilidade acrescida.

A mudança das condições em que as pessoas em causa podem exercer o direito de oposição, tal como previsto no artigo 19.º da proposta de regulamento, é já um importante elemento da responsabilidade. Nos termos da proposta de regulamento, se a pessoa em causa se opuser ao tratamento dos seus dados nos termos do artigo 7.º, alínea f), caberá ao responsável pelo tratamento demonstrar que o seu interesse prevalece. Esta inversão do ónus da prova é firmemente apoiada pelo Grupo de Trabalho, uma vez que contribui para uma obrigação de responsabilidade acrescida.

Se, num determinado caso, o responsável pelo tratamento não conseguir demonstrar à pessoa em causa que o seu interesse prevalece, tal pode ter também consequências mais vastas para todo o tratamento, e não apenas no que respeita à pessoa em causa que exerceu o seu direito de oposição. Consequentemente, o responsável pelo tratamento pode pôr em causa ou decidir reorganizar o tratamento quando tal seja vantajoso não apenas para a

¹¹¹ Essa demonstração deve ser razoável e centrar-se no resultado e não no procedimento administrativo.

pessoa em causa mas também para todas as pessoas que possam estar numa situação semelhante.¹¹²

Este requisito é necessário mas não suficiente. Para garantir a proteção desde o início, e para evitar que a inversão do ónus da prova seja contornada¹¹³, é importante que sejam tomadas medidas *antes* do início do tratamento, e não apenas durante os procedimentos de «oposição» *ex-post*.

Por conseguinte, propõe-se que, na primeira fase de qualquer atividade de tratamento de dados, o responsável pelo tratamento dos dados tome várias medidas. As duas primeiras medidas podem ser elencadas num considerando da proposta de regulamento e a terceira numa disposição específica:

- Realizar uma avaliação¹¹⁴, que deve incluir as diferentes fases da análise desenvolvida no presente parecer e resumida no anexo 1. O responsável pelo tratamento deve

¹¹² Para além da inversão do ónus da prova, o Grupo de Trabalho apoia igualmente o facto de a proposta de regulamento já não exigir que a oposição seja apresentada «por razões preponderantes e legítimas relacionadas com a [...] situação particular [da pessoa em causa]». Pelo contrário, de acordo com a proposta de regulamento, a referência a quaisquer razões legítimas (não necessariamente «preponderantes») relacionadas com a situação particular da pessoa em causa é suficiente. De facto, outra possibilidade, que foi proposta no relatório final da Comissão LIBE, é afastar igualmente o requisito de que a oposição esteja relacionada com a situação particular da pessoa em causa. O Grupo de Trabalho apoia esta abordagem no sentido em que recomenda que as pessoas em causa possam beneficiar de qualquer destas, ou das duas, possibilidades, consoante o caso, ou seja, que possam opor-se ao tratamento com base na sua própria situação particular ou num âmbito mais geral e, neste último caso, sem que lhes seja exigido que apresentem qualquer justificação específica. Neste sentido, ver a alteração n.º 114 ao artigo 19.º, n.º 1, da proposta de regulamento, constante do relatório final da Comissão LIBE.

¹¹³ Por exemplo, os responsáveis pelo tratamento de dados podem sentir-se tentados a evitar demonstrar caso a caso que o seu interesse prevalece, utilizando modelos justificativos tipo, ou de outro modo tornar complicado o exercício do direito de oposição.

¹¹⁴ Como já foi referido na nota 84, esta avaliação não deve ser confundida com uma avaliação abrangente do impacto na privacidade e na proteção de dados. Atualmente, não existem orientações abrangentes sobre avaliações de impacto a nível europeu, embora, nalguns domínios, nomeadamente no que respeita às RFID e aos contadores inteligentes, tenham sido envidados esforços importantes para definir uma metodologia/um quadro (e/ou um modelo) específica(o) para o setor que possa ser aplicada(o) em toda a União Europeia. Ver a «Proposta da indústria relativa a um quadro para as avaliações do impacto das aplicações RFID na proteção da privacidade e dos dados» e o «Modelo de avaliação do impacto dos sistemas de redes inteligentes e dos contadores inteligentes na proteção de dados», preparados pelo Grupo de Peritos 2 da *Task Force* da Comissão Europeia para as redes inteligentes. O Grupo de Trabalho emitiu vários pareceres a respeito destas duas metodologias.

Além disso, tem havido algumas iniciativas com vista à definição de uma metodologia geral para a avaliação do impacto na proteção de dados, da qual os esforços «em domínios específicos» podem beneficiar. Ver, por exemplo, o Projeto PIAF (quadro de avaliação do impacto na privacidade no que respeita aos direitos à proteção de dados e ao respeito pela vida privada): <http://www.piafproject.eu/>.

Além disso, no que respeita a orientações a nível nacional, ver, por exemplo, a metodologia da CNIL, disponível em <http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf>, e o Manual de Avaliação do Impacto na Privacidade, do ICO, disponível em http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

identificar expressamente o(s) interesse(s) prevalecente(s) em jogo e a razão pela qual este(s) prevalece(m) sobre os interesses das pessoas em causa. Esta avaliação prévia não deve ser demasiado morosa e deve ser *modulável*: pode limitar-se aos critérios essenciais se o impacto do tratamento nas pessoas em causa não for *prima facie* significativo mas, por outro lado, deve ser efetuada de forma mais exaustiva se o equilíbrio tiver sido difícil de alcançar e exigir, por exemplo, a adoção de várias garantias complementares. Sempre que adequado – ou seja, quando uma operação de tratamento de dados apresente riscos específicos para os direitos e as liberdades das pessoas em causa – deve ser realizada uma avaliação mais abrangente do impacto na privacidade e na proteção de dados (de acordo com o artigo 33.º da proposta de regulamento), da qual a avaliação prevista no artigo 7.º, alínea f), pode tornar-se uma parte importante.

- Documentar essa avaliação. Da mesma forma que a avaliação é *modulável* quanto ao nível de pormenor em que é necessário realizá-la, também o volume da documentação deve ser *modulável*. Dito isto, em todos os casos, com exceção dos de menor importância, deve estar disponível alguma documentação, independentemente da apreciação do impacto do tratamento na pessoa. É com base nessa documentação que a avaliação do responsável pelo tratamento pode, por sua vez, ser apreciada e eventualmente contestada;
- Garantir a transparência e a visibilidade dessa informação às pessoas em causa e a outras partes interessadas. A transparência deve ser garantida quer em relação às pessoas em causa e às autoridades responsáveis pela proteção de dados quer, quando necessário, ao público em geral. No que respeita às pessoas em causa, o Grupo de Trabalho remete para o projeto de relatório da Comissão LIBE¹¹⁵, que determina que o responsável pelo tratamento deve informar a pessoa em causa das razões pelas quais considera que sobre os seus interesses não prevalecem os interesses ou os direitos e liberdades fundamentais da pessoa em causa. Na opinião do Grupo de Trabalho, essa informação deve ser fornecida às pessoas em causa juntamente com as informações que o responsável pelo tratamento tem de fornecer nos termos dos artigos 10.º e 11.º

¹¹⁵ Projeto de Relatório sobre a Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados), [COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)]

da atual diretiva (artigo 11.º da proposta de regulamento). Tal permitirá que, numa segunda fase, a pessoa em causa eventualmente se oponha ao tratamento e que o responsável pelo tratamento apresente uma justificação complementar, caso a caso, dos interesses prevaletentes. Além disso, mediante requerimento, a documentação na qual o responsável pelo tratamento tenha baseado a sua avaliação deve ser disponibilizada às autoridades responsáveis pela proteção de dados, de forma a permitir a sua eventual verificação e aplicação, se for caso disso.

O Grupo de Trabalho apoia a inclusão expressa destas três medidas na proposta de regulamento, das formas acima enunciadas. Tal constituirá o reconhecimento do papel específico dos fundamentos jurídicos na avaliação da legitimidade e clarificará a importância do teste da ponderação no contexto mais alargado das medidas em matéria de responsabilidade e das avaliações de impacto no novo quadro jurídico proposto.

O Grupo de Trabalho considera que é igualmente aconselhável incumbir o CEPD de fornecer mais orientações, quando necessário, com base neste quadro. Esta abordagem conferirá quer clareza suficiente ao texto quer flexibilidade suficiente à sua implementação.

Anexo 1. Guia rápido para a realização do teste da ponderação previsto no artigo 7.º, alínea f)

Etapa 1: Verificar quais são os fundamentos jurídicos potencialmente aplicáveis nos termos do artigo 7.º, alíneas a) a f)

O tratamento de dados só pode ser concretizado se pelo menos um dos seis fundamentos previstos no artigo 7.º - alíneas a) a f) – for aplicável (podem ser invocados diferentes fundamentos em diferentes fases da mesma atividade de tratamento de dados). Se se afigurar *prima facie* que o artigo 7.º, alínea f), pode ser adequado como fundamento jurídico, deve passar-se à etapa 2.

Indicações breves:

- O artigo 7.º, alínea a), é aplicável apenas se for dado consentimento livre, específico, informado e inequívoco; o facto de uma pessoa não se opor ao tratamento nos termos do artigo 14.º não deve ser confundido com o consentimento previsto no artigo 7.º, alínea a) – no entanto, a existência de um mecanismo acessível que permita que a pessoa se oponha ao tratamento pode ser considerado uma importante garantia nos termos do artigo 7.º, alínea f).
- O artigo 7.º, alínea b), abrange o tratamento que seja necessário para a execução de um contrato; o simples facto de o tratamento de dados estar relacionado com o contrato, ou estar previsto algures nas condições gerais do contrato, não significa necessariamente que este fundamento seja aplicável; sempre que adequado, o artigo 7.º, alínea f), deve ser considerado uma alternativa.
- O artigo 7.º, alínea c), contempla apenas obrigações legais claras e específicas nos termos da legislação da UE ou de um Estado-Membro; no caso de orientações não vinculativas (por exemplo, de entidades reguladoras), ou de uma obrigação legal decorrente de legislação estrangeira, o artigo 7.º, alínea f), deve ser considerado uma alternativa.

Etapa 2: Qualificar um interesse como «legítimo» ou «ilegítimo»

Para ser considerado legítimo, um interesse deve preencher cumulativamente as seguintes condições:

- ser lícito (ou seja, deve respeitar o direito da UE e o direito nacional),

- ser definido de forma suficientemente clara para permitir a realização do teste da ponderação em relação aos interesses e aos direitos fundamentais da pessoa em causa (ou seja, deve ser suficientemente concreto),
- representar um interesse real e atual (ou seja, não deve ser especulativo).

Etapa 3: Determinar se o tratamento é necessário para servir o interesse prosseguido

Para cumprir este requisito, deve verificar-se se existem outros meios menos invasivos para alcançar a finalidade definida para o tratamento e servir o interesse legítimo do responsável pelo tratamento.

Etapa 4: Estabelecer um equilíbrio provisório verificando se os interesses ou os direitos fundamentais das pessoas em causa prevalecem sobre o interesse do responsável pelo tratamento de dados

- Analisar a natureza dos interesses do responsável pelo tratamento (direito fundamental, outro tipo de interesse, interesse público).
- Avaliar o eventual prejuízo sofrido pelo responsável pelo tratamento, por terceiros ou pela comunidade em geral se o tratamento não for efetuado.
- Ter em conta a natureza dos dados (sensíveis em sentido estrito ou lato?).
- Analisar o estatuto da pessoa em causa (menor, trabalhador, etc.) e do responsável pelo tratamento (por exemplo, verificar se uma organização empresarial tem uma posição dominante no mercado).
- Ter em conta a forma de tratamento dos dados (grande escala, prospeção de dados, elaboração de perfis, divulgação a um grande número de pessoas ou publicação).
- Identificar os direitos fundamentais e/ou os interesses da pessoa em causa que podem ser afetados.
- Analisar as expectativas razoáveis das pessoas em causa.
- Avaliar os impactos na pessoa em causa e comparar com o benefício que o responsável pelo tratamento dos dados espera retirar do tratamento.

Indicação breve: analisar o efeito do tratamento efetivo em determinadas pessoas - não considerar que se trata de um exercício abstrato ou hipotético.

Etapa 5: Estabelecer um equilíbrio final tendo em conta as garantias complementares

Identificar e implementar garantias complementares adequadas decorrentes do dever de cuidado e de diligência, tais como:

- a minimização dos dados (por exemplo, a limitação rigorosa do volume de dados recolhidos ou a eliminação imediata de dados após utilização),
- medidas técnicas e organizativas para assegurar que os dados não possam ser utilizados para tomar decisões ou outras medidas em relação às pessoas («separação funcional»),
- a utilização ampla de técnicas de anonimização, agregação de dados, tecnologias para reforçar a proteção da privacidade, privacidade desde a conceção, avaliações de impacto na privacidade e na proteção de dados,
- maior transparência, direito generalizado e incondicional de oposição (optar por não permitir o tratamento), portabilidade dos dados e medidas afins para capacitar as pessoas em causa.

Indicação breve: a utilização de tecnologias para reforçar a proteção da privacidade pode alterar o equilíbrio a favor do responsável pelo tratamento dos dados e proteger igualmente as pessoas.

Etapa 6: Demonstrar o cumprimento e garantir a transparência

- Fazer a planificação das etapas 1 a 5 para justificar o tratamento antes de este ter início.
- Informar as pessoas em causa das razões pelas quais se considera que o equilíbrio é favorável ao responsável pelo tratamento.
- Manter a documentação à disposição das autoridades responsáveis pela proteção de dados.

Indicação breve: esta etapa é modulável. O nível de pormenor da avaliação e a documentação devem ser adaptados à natureza e ao contexto do tratamento. Estas medidas serão mais alargadas quando esteja em causa o tratamento de uma grande quantidade de informação sobre um grande número de pessoas, de uma forma que possa ter um impacto significativo nessas pessoas. Uma avaliação abrangente do impacto na privacidade e na proteção de dados (nos termos do artigo 33 da proposta de regulamento) apenas será necessária quando a operação de tratamento apresente riscos específicos para os direitos e liberdades das pessoas em causa.

Nesses casos, a avaliação nos termos do artigo 7.º, alínea f) pode tornar-se uma parte essencial dessa avaliação de impacto mais ampla.

Etapa 7: E se a pessoa em causa exercer o seu direito de oposição?

- Quando exista apenas como garantia um direito qualificado de optar por não permitir o tratamento (tal é expressamente exigido nos termos do artigo 14.º, alínea a), como garantia mínima): no caso de a pessoa em causa se opor ao tratamento, deve garantir-se a existência de um mecanismo adequado e de fácil utilização que permita reavaliar o equilíbrio no que respeita à pessoa em causa e pôr termo ao tratamento dos respetivos dados se a reavaliação revelar que os seus interesses prevalecem.

- Quando esteja previsto como garantia complementar um direito incondicional de optar por não permitir o tratamento (porque é expressamente exigido nos termos do artigo 14.º, alínea b), ou porque de outro modo se revela uma garantia complementar necessária ou útil): no caso de a pessoa em causa se opor ao tratamento, há que assegurar que essa escolha seja respeitada, sem que seja necessário tomar mais medidas ou proceder a mais avaliações.

Anexo 2. Exemplos práticos para ilustrar a aplicação do teste da ponderação previsto no artigo 7.º, alínea f)

O presente anexo apresenta exemplos de alguns contextos mais comuns nos quais a questão do interesse legítimo na aceção do artigo 7.º, alínea f), pode ser suscitada. Na maior parte dos casos, agrupámos sob a mesma epígrafe dois ou mais exemplos conexos que vale a pena comparar. Muitos dos exemplos baseiam-se em casos reais ou em elementos de casos reais tratados pelas autoridades responsáveis pela proteção de dados dos diferentes Estados-Membros. No entanto, nalguns casos, alterámos os factos, em certa medida, para ajudar a ilustrar melhor a forma como o teste da ponderação deve ser realizado.

Os exemplos são incluídos para ilustrar o *processo de raciocínio* – o método a utilizar na realização do teste da ponderação multifatorial. Por outras palavras, os exemplos *não* se destinam a fornecer uma avaliação *conclusiva* dos casos descritos. Na verdade, em muitos casos, se os factos se alterarem de alguma forma (por exemplo, se o responsável pelo tratamento adotar garantias complementares, tais como uma anonimização mais completa, melhores medidas de segurança, uma maior transparência e uma verdadeira liberdade de escolha para as pessoas em causa), o resultado do teste da ponderação pode ser diferente¹¹⁶.

Tal deve incentivar os responsáveis pelo tratamento a cumprir melhor todas as disposições horizontais da diretiva e proporcionar proteção complementar, sempre que necessário, baseada na privacidade e na proteção de dados desde a conceção. Quanto mais cuidado tiverem os responsáveis pelo tratamento em proteger os dados pessoais em geral, mais provável é que sejam bem sucedidos no teste da ponderação.

Exercício do direito à liberdade de expressão ou de informação¹¹⁷, nomeadamente nos meios de comunicação social e nas artes

¹¹⁶ A aplicação correta do artigo 7.º, alínea f), pode suscitar questões complexas de avaliação, pelo que, para ajudar a orientar a avaliação, a legislação específica, a jurisprudência, as diretrizes, bem como os códigos de conduta e outras normas mais ou menos formais, podem desempenhar um papel importante.

¹¹⁷ Quanto à liberdade de expressão ou de informação, ver a página 34 do parecer. Quaisquer derrogações relevantes nos termos da legislação nacional para o tratamento para fins jornalísticos nos termos do artigo 9.º da diretiva devem ser igualmente tidas em conta na apreciação destes exemplos.

Exemplo 1: ONG publica novamente informações sobre as despesas de deputados

Uma autoridade pública – em cumprimento de uma obrigação legal (artigo 7.º, alínea c)) - publica informações sobre as despesas de deputados; uma ONG especializada em questões de transparência, por sua vez, analisa e publica novamente os dados numa versão anotada, cuidadosa, proporcionada, mas com mais conteúdo informativo, contribuindo para uma maior transparência e responsabilidade.

Partindo do princípio de que a ONG publica e elabora essa versão anotada de forma cuidadosa e proporcionada, adota garantias adequadas e, em geral, respeita os direitos das pessoas em causa, deve poder invocar o artigo 7.º, alínea f), como fundamento jurídico para o tratamento. Fatores como a natureza do interesse legítimo (o direito fundamental à liberdade de expressão ou de informação), o interesse dos cidadãos na transparência e na responsabilidade e o facto de os dados já terem sido publicados e de se tratar de dados pessoais (relativamente menos sensíveis) relacionados com atividades das pessoas em causa que são relevantes para o exercício das suas funções públicas¹¹⁸, militam a favor da legitimidade do tratamento. O facto de a publicação inicial ter sido exigida por lei e de, conseqüentemente, as pessoas em causa deverem estar à espera de que os seus dados fossem divulgados contribui também para uma avaliação favorável. No outro lado a ponderar, o impacto na pessoa em causa pode ser significativo, por exemplo, devido ao escrutínio público, a integridade pessoal de algumas pessoas pode ser questionada, o que pode conduzir nomeadamente à perda de eleições ou, nalguns casos, a uma investigação criminal por atividades fraudulentas. Contudo, os fatores acima referidos, no seu todo, mostram que, na ponderação, os interesses do responsável pelo tratamento (e os interesses dos cidadãos a quem os dados são divulgados) prevalecem sobre os interesses das pessoas em causa.

Exemplo 2: Vereador nomeia a filha para assessora especial

Uma jornalista publica num jornal local em linha um artigo factualmente correto e baseado numa investigação aprofundada sobre um vereador, no qual revela que este só participou

¹¹⁸ Não é de excluir que algumas despesas possam revelar dados mais sensíveis, tais como dados sobre a saúde. Se assim for, estes devem ser desde logo suprimidos do conjunto de dados antes de este ser divulgado. Constitui uma boa prática adotar uma «abordagem proactiva» e dar às pessoas a possibilidade de analisar os respetivos dados antes da sua publicação, bem como informações claras sobre a eventualidade e as modalidades dessa publicação.

numa das últimas onze reuniões da Câmara Municipal e que é pouco provável que venha a ser reeleito devido a um escândalo recente que envolve a nomeação da sua filha de dezassete anos de idade para assessora especial.

Neste caso, a análise é semelhante à do *Exemplo 1*. Tendo em conta os factos, é do interesse legítimo do jornal em questão publicar a informação. Embora tenham sido revelados dados pessoais sobre o vereador, o direito à vida privada do vereador não prevalece sobre o direito fundamental à liberdade de expressão e de publicar a história no jornal. Tal deve-se ao facto de o direito ao respeito pela vida privada das figuras públicas ser relativamente limitado no que respeita às suas atividades públicas, bem como à especial importância da liberdade de expressão – em especial quando a publicação de uma história seja do interesse público.

Exemplo 3: Os principais resultados da pesquisa continuam a mostrar o delito menor

O arquivo em linha de um jornal contém um artigo antigo relativo a uma pessoa que, em tempos, foi uma celebridade local como capitão de uma equipa de futebol amador de uma pequena cidade. A pessoa é identificada pelo seu nome completo e a história relaciona-se com o seu envolvimento num processo-crime por um delito relativamente menor (embriaguez e comportamento desordeiro). Atualmente, o registo criminal da pessoa encontra-se limpo e já não contém a referência ao delito, pelo qual cumpriu pena há vários anos. O que mais preocupa a pessoa em causa é que, ao efetuar uma pesquisa em linha a partir do seu nome nos motores de busca comuns, a ligação para aquela notícia antiga aparece entre os primeiros resultados que lhe dizem respeito. Não obstante o seu pedido, o jornal recusa-se a adotar medidas técnicas que limitem a disponibilidade alargada da referida notícia. Por exemplo, o jornal recusa-se a adotar medidas técnicas e organizativas destinadas – na medida do que a tecnologia permite – a limitar o acesso à informação a partir de motores de busca externos, utilizando o nome da pessoa como critério de pesquisa.

Trata-se de mais um caso que ilustra o potencial conflito entre a liberdade de expressão e o respeito pela vida privada. Mostra igualmente que, nalguns casos, as garantias complementares – tais como assegurar que, pelo menos em caso de oposição justificada nos termos do artigo 14, alínea a), da diretiva, a parte relevante dos arquivos do jornal deixem de poder ser acedidos através de motores de busca externos ou que o formato utilizado para

apresentar a informação não permita a pesquisa a partir do nome – podem desempenhar um papel essencial na procura do equilíbrio adequado entre os dois direitos fundamentais em causa. Tal não impede que quaisquer outras medidas possam ser tomadas por motores de busca ou outros terceiros¹¹⁹.

Marketing direto convencional e outras formas de marketing ou de publicidade

Exemplo 4: Loja de computadores envia publicidade sobre produtos análogos aos seus clientes

Uma loja de computadores obtém, provenientes dos seus clientes, as informações dos respetivos contactos no âmbito da venda de um produto e utiliza essas informações de contacto para publicitar os seus próprios produtos análogos por correspondência. A loja vende igualmente produtos através da Internet e envia mensagens de correio eletrónico promocionais quando chega uma nova linha de produtos para venda. Os clientes são claramente informados sobre a possibilidade de se oporem ao tratamento dos dados, sem custos e de forma fácil, no momento em que os seus dados são recolhidos, e de cada vez que uma mensagem é enviada, caso o cliente não se tenha oposto inicialmente.

A transparência do tratamento, o facto de o cliente poder razoavelmente esperar receber ofertas relativas a produtos análogos enquanto cliente da loja e o facto de ter o direito de se opor ajudam a reforçar a legitimidade do tratamento e a garantir a salvaguarda dos direitos das pessoas. No outro lado a ponderar, não parece existir qualquer impacto desproporcionado no direito ao respeito pela vida privada da pessoa em causa (neste exemplo, partimos do princípio de que a loja de computadores não criou perfis complexos dos seus clientes, por exemplo, utilizando análises pormenorizadas dos dados relativos à sequência de cliques).

Exemplo 5: Farmácia em linha elabora perfis muito completos

Uma farmácia em linha realiza campanhas de marketing com base nos medicamentos e noutros produtos que os clientes compraram, incluindo produtos sujeitos a receita médica. A farmácia analisa essa informação – combinada com informação demográfica acerca dos seus

¹¹⁹ Ver igualmente o processo C-131/12, Google Spain/Agencia Española de Protección de Datos, pendente no Tribunal de Justiça da União Europeia.

clientes – por exemplo, a idade e o género – para construir um perfil de «saúde e bem-estar» de cada cliente. São igualmente recolhidos e utilizados os dados relativos à sequência de cliques, não apenas sobre os produtos que os clientes compraram mas igualmente sobre outros produtos e informações que tenham pesquisado no sítio Web. Os perfis dos clientes incluem informações ou previsões que indicam, por exemplo, que uma determinada cliente está grávida ou que um(a) cliente tem uma determinada doença crónica ou pode estar interessado(a) em adquirir suplementos alimentares, um bronzeador ou outros produtos para cuidar da pele em determinadas alturas do ano. Os analistas da farmácia em linha utilizam essa informação para enviar a determinadas pessoas, através do correio eletrónico, ofertas de medicamentos não sujeitos a receita médica, suplementos para a saúde e outros produtos. Neste caso, a farmácia não pode invocar os seus interesses legítimos quando cria e utiliza os perfis dos seus clientes para fins de marketing. A elaboração de perfis descrita coloca vários problemas. A informação é especialmente sensível e pode ser muito reveladora no que respeita a assuntos que muitas pessoas esperam que permaneçam privados¹²⁰. O grau exaustivo dos perfis e a forma como são elaborados (utilização dos dados relativos à sequência de cliques, algoritmos que permitem fazer previsões) indicam igualmente que o nível de intromissão é muito elevado. No entanto, o consentimento baseado no artigo 7.º, alínea a), e no artigo 8.º, n.º 2, alínea a), (quando estejam em causa dados sensíveis) pode, sempre que adequado, ser considerado uma alternativa.

¹²⁰ Para além de quaisquer restrições impostas pela legislação em matéria de proteção de dados, a publicidade de produtos sujeitos a receita médica é também estritamente regulamentada na UE, e existem ainda algumas restrições relativas à publicidade de substâncias não sujeitas a receita médica. Além disso, os requisitos previstos no artigo 8.º, relativo a certas categorias específicas de dados (tais como dados relativos à saúde), devem ser igualmente tidos em conta.

Mensagens não comerciais não solicitadas, nomeadamente relativas a campanhas políticas ou a atividades de angariação de fundos para fins de beneficência

Exemplo 6: Candidata a eleições locais utiliza, de forma direcionada, cadernos eleitorais

Uma candidata a eleições locais utiliza os cadernos eleitorais¹²¹ para enviar a cada um dos potenciais eleitores do seu círculo eleitoral uma carta de apresentação a promover a sua campanha para as eleições que se avizinham. A candidata utiliza os dados obtidos a partir dos cadernos eleitorais apenas para enviar a carta e não conserva os dados após o termo da campanha.

Tal utilização dos cadernos eleitorais a nível local está dentro das expectativas razoáveis das pessoas quando ocorre no período pré-eleitoral: o interesse do responsável pelo tratamento é claro e legítimo. A utilização limitada e focalizada da informação também contribui para que o equilíbrio seja favorável ao interesse legítimo do responsável pelo tratamento. A legislação nacional pode também prever a utilização dos cadernos eleitorais, numa perspetiva de interesse público, e estabelecer normas específicas, restrições e garantias no que se refere a essa utilização. Se assim for, o cumprimento dessas normas específicas é igualmente exigido para garantir a legitimidade do tratamento.

Exemplo 7: Organismo sem fins lucrativos recolhe informação para se dirigir às pessoas

Uma organização filosófica dedicada ao desenvolvimento humano e social decide organizar atividades de angariação de fundos com base no perfil dos seus membros. Para esse efeito, recolhe dados nas redes sociais, utilizando um software *ad-hoc*, para se dirigir às pessoas que tenham «gostado» da página da organização, que tenham «gostado» ou «partilhado» as mensagens que a organização publicou na sua página, que tenham consultado regularmente alguns tópicos ou que tenham reenviado as mensagens da organização. Depois envia mensagens e boletins informativos aos seus membros, de acordo com os seus perfis. Por exemplo, as pessoas idosas que tenham cães e que tenham «gostado» de artigos sobre abrigos

¹²¹ Parte-se do princípio de que, no Estado-Membro em que este exemplo se aplica, a legislação prevê a existência de cadernos eleitorais.

para animais recebem pedidos de contribuição diferentes das famílias que tenham filhos pequenos; pessoas de grupos étnicos diferentes recebem igualmente mensagens diferentes.

O facto de o tratamento incidir sobre categorias específicas de dados (convicções filosóficas) exige o cumprimento do disposto no artigo 8.º, condição que parece ser satisfeita na medida em que o tratamento é efetuado no âmbito de atividades legítimas da organização. No entanto, neste caso, esta condição não é suficiente: a forma como os dados são utilizados excede as expectativas razoáveis das pessoas. O volume de dados recolhidos e a falta de transparência quanto à recolha e reutilização dos dados com uma finalidade diferente da publicação inicial contribui para a conclusão de que, neste caso, o artigo 7.º, alínea f), não pode ser invocado. Por conseguinte, o tratamento não deve ser autorizado, a não ser que possa ser utilizado outro fundamento, como, por exemplo, o consentimento das pessoas em causa nos termos do artigo 7.º, alínea a).

Execução de créditos, incluindo cobrança de dívidas através de procedimentos não judiciais

Exemplo 8: Litígio relativo à qualidade de um trabalho de remodelação

Um cliente contesta a qualidade de um trabalho de remodelação de uma cozinha e recusa-se a pagar a totalidade do preço. A empresa de construção transfere os dados relevantes e adequados para o seu advogado para que este possa notificar o cliente do pagamento em falta e negociar um acordo com o cliente se este mantiver a recusa em pagar.

Neste caso, as medidas preliminares tomadas pela empresa de construção, utilizando informações básicas sobre a pessoa em causa (por exemplo, o nome, o endereço e a referência do contrato) para enviar uma notificação a essa pessoa (diretamente ou através do seu advogado, como neste caso), podem estar ainda abrangidas pelo tratamento necessário para a execução do contrato (artigo 7.º, alínea b). Contudo, se forem tomadas mais medidas¹²², nomeadamente a intervenção de uma empresa de cobrança de dívidas, estas devem ser apreciadas nos termos do artigo 7.º, alínea f), tendo em conta, entre outros, o seu carácter intrusivo e o impacto na pessoa em causa, como se verá no exemplo que se segue.

¹²² Atualmente, existe um certo desacordo entre os Estados-Membros quanto às medidas que podem ser consideradas necessárias para a execução de um contrato.

Exemplo 9: Cliente desaparece com carro adquirido a crédito

Um cliente não paga as prestações devidas pela aquisição a crédito de um automóvel desportivo caro e, em seguida, «desaparece». O comerciante de automóveis contrata um terceiro, que é «agente de cobranças». O agente de cobranças leva a cabo uma investigação intrusiva «ao estilo policial», utilizando, entre outros, práticas como a videovigilância encoberta e escutas telefónicas.

Embora os interesses do comerciante de automóveis e do agente de cobranças sejam legítimos, o equilíbrio não lhes é favorável devido aos métodos intrusivos utilizados para recolher informações, alguns dos quais são expressamente proibidos por lei (escutas telefónicas). A conclusão seria diferente se, por exemplo, o comerciante de automóveis ou o agente de cobranças apenas tivessem efetuado verificações limitadas para confirmar as informações de contacto da pessoa em causa com o objetivo de propor uma ação judicial contra essa pessoa.

Prevenção da fraude, utilização abusiva de serviços ou branqueamento de capitais

Exemplo 10: Verificação dos dados dos clientes antes da abertura de uma conta bancária

Uma instituição financeira adota procedimentos razoáveis e proporcionados - de acordo com as orientações não vinculativas da autoridade de supervisão financeira competente – para verificar a identidade de qualquer pessoa que pretenda abrir uma conta. Conserva registos da informação utilizada para verificar a identidade da pessoa.

O interesse do responsável pelo tratamento é legítimo e o tratamento de dados envolve apenas informação limitada e necessária (prática habitual neste domínio de atividade, a qual está dentro das expectativas razoáveis das pessoas em causa e é recomendada pelas autoridades competentes). São instituídas garantias adequadas para limitar qualquer impacto desproporcionado e indevido nas pessoas em causa. Por conseguinte, o responsável pelo tratamento pode invocar o artigo 7.º, alínea f). Em alternativa, e na medida em que as ações

levadas a cabo sejam especificamente exigidas pela legislação aplicável, pode aplicar-se o artigo 7.º, alínea c).

Exemplo 11: Intercâmbio de informações para combater o branqueamento de capitais

Uma instituição financeira – após obter o parecer da autoridade responsável pela proteção de dados competente – aplica procedimentos, baseados em critérios específicos e limitados, de intercâmbio de dados relativos a suspeitas de violação das normas em matéria de combate ao branqueamento de capitais com outras empresas do mesmo grupo, respeitando requisitos rigorosos de limitação do acesso, segurança e proibição de qualquer utilização posterior para outros fins.

Por razões semelhantes às referidas supra, e dependendo das circunstâncias do caso, o tratamento de dados pode basear-se no artigo 7.º, alínea f). Em alternativa, e na medida em que as ações levadas a cabo sejam especificamente exigidas pela legislação aplicável, pode aplicar-se o artigo 7.º, alínea c).

Exemplo 12: Lista negra de toxicodependentes agressivos

Um grupo de hospitais criou uma lista negra conjunta de pessoas «agressivas» que procuram drogas, com o objetivo de impedi-las de entrar em todas as instalações médicas dos hospitais participantes.

Ainda que o interesse dos responsáveis pelo tratamento em manter instalações seguras e protegidas seja legítimo, deve ser ponderado em relação ao direito fundamental ao respeito pela vida privada e a outras preocupações preponderantes, tais como a necessidade de não impedir o acesso das pessoas em causa aos tratamentos de saúde. O facto de o tratamento incidir sobre dados sensíveis (por exemplo, dados sobre a saúde relacionados com a toxicodependência), também permite concluir que, neste caso, o tratamento não é suscetível de ser aceitável nos termos do artigo 7.º, alínea f)¹²³. O tratamento poderá ser aceitável se, por exemplo, for regulado por uma lei que preveja garantias específicas (verificações e controlos,

¹²³ Os requisitos previstos no artigo 8.º, relativo a certas categorias específicas de dados (tais como dados relativos à saúde), devem ser igualmente tidos em conta.

transparência, prevenção de decisões automáticas)¹²⁴ que assegurem que o tratamento não conduza a discriminações ou à violação de direitos fundamentais das pessoas. Neste último caso, consoante essa lei específica exija ou apenas permita o tratamento, o artigo 7.º, alínea c), ou o artigo 7.º, alínea f), podem ser invocados como fundamento jurídico.

Monitorização da atividade dos trabalhadores para fins de segurança ou de gestão.

Exemplo 13: Horas de trabalho dos advogados utilizadas para efeitos de faturação e de atribuição de bónus

Numa sociedade de advogados, o número de horas de trabalho dos advogados que podem ser faturadas é objeto de tratamento quer para efeitos de faturação quer para a determinação dos bónus anuais. O sistema é explicado de forma transparente aos trabalhadores, que têm o direito, expressamente conferido, de manifestar o seu desacordo com as conclusões relativas à faturação e ao pagamento dos bónus, as quais são depois discutidas com a administração.

O tratamento afigura-se necessário para a prossecução dos interesses legítimos do responsável pelo tratamento, e parece não existir uma forma menos intrusiva de alcançar a mesma finalidade. O impacto nos trabalhadores é igualmente limitado devido às garantias e aos procedimentos instituídos. Por conseguinte, neste caso, o artigo 7.º, alínea f), pode constituir um fundamento jurídico adequado. Pode argumentar-se ainda que o tratamento para uma das finalidades, ou para ambas, é também necessário para a execução do contrato.

¹²⁴ Ver o Documento de trabalho sobre listas negras (WP65), adotado em 3 de outubro de 2002.

Exemplo 14: Monitorização eletrónica da utilização da Internet¹²⁵

O empregador monitoriza a utilização da Internet pelos seus trabalhadores durante as horas de trabalho para verificar que não estão a utilizar de forma excessiva as tecnologias de informação da empresa para fins pessoais. Os dados recolhidos incluem ficheiros temporários e cookies gerados nos computadores dos trabalhadores, que mostram os sítios Web visitados e os descarregamentos efetuados durante as horas de trabalho. Os dados são tratados sem consultar previamente as pessoas em causa e os delegados sindicais/conselho de trabalhadores da empresa. Também não é fornecida informação suficiente sobre essas práticas às pessoas em causa.

O volume e a natureza dos dados recolhidos constituem uma intromissão significativa na vida privada dos trabalhadores. Para além das questões de proporcionalidade, a transparência no que respeita às práticas, estreitamente ligadas às expectativas razoáveis das pessoas em causa, é igualmente um fator importante a ter em conta. Ainda que o empregador tenha um interesse legítimo em limitar o tempo despendido pelos trabalhadores a visitar sítios Web que não estejam diretamente relacionados com o seu trabalho, os métodos utilizados não preenchem os requisitos do teste da ponderação previsto no artigo 7.º, alínea f). O empregador deve utilizar métodos menos intrusivos (por exemplo, limitar o acesso a determinados sítios Web), que sejam, a título de boas práticas, objeto de discussão e acordo com os representantes dos trabalhadores e comunicados aos trabalhadores de forma transparente.

Sistemas de denúncia

Exemplo 15: Sistema de denúncias para cumprir obrigações legais decorrentes de legislação estrangeira

Uma sucursal europeia de um grupo norte-americano instituiu um sistema de denúncias restrito para reportar irregularidades graves no domínio contabilístico e financeiro. As entidades do grupo estão sujeitas a um código de boa governação que exige o reforço dos procedimentos

¹²⁵ Alguns Estados-Membros consideram que alguma monitorização eletrónica limitada pode ser «necessári[a] para a execução de um contrato» e, por conseguinte, pode basear-se no fundamento jurídico do artigo 7.º, alínea b), em vez do artigo 7.º, alínea f).

de controlo interno e de gestão do risco. Devido às suas atividades internacionais, a sucursal europeia está obrigada a fornecer dados financeiros fiáveis a outros membros do grupo nos Estados Unidos. O sistema está concebido para respeitar quer a legislação dos Estados Unidos quer as orientações fornecidas pelas autoridades nacionais responsáveis pela proteção de dados na UE.

Entre as garantias, são dadas orientações claras aos trabalhadores quanto às condições em que o sistema deve ser utilizado, através de sessões de formação e de outros meios. Os funcionários são alertados para não abusarem do sistema – por exemplo, fazendo acusações falsas ou infundadas contra outros funcionários. É-lhes explicado igualmente que, se preferirem, podem utilizar o sistema anonimamente ou, se o desejarem, podem identificar-se. Neste último caso, os trabalhadores são informados sobre as condições em que a informação que os identifica será enviada ao seu empregador ou transmitida a outras agências.

Se o sistema tivesse de ser instituído de acordo com a legislação da UE ou de acordo com a legislação de um Estado-Membro da UE, o tratamento poderia basear-se no artigo 7.º, alínea c). No entanto, as obrigações legais decorrentes de legislação estrangeira não são consideradas obrigações legais para efeitos do artigo 7.º, alínea c), pelo que tal obrigação não pode legitimar o tratamento nos termos do artigo 7.º, alínea c). No entanto, o tratamento poderá basear-se no artigo 7.º, alínea f), por exemplo, se existir um interesse legítimo em garantir a estabilidade dos mercados financeiros, ou o combate à corrupção, e desde que o sistema inclua garantias suficientes, de acordo com as orientações das autoridades reguladoras competentes da UE.

Exemplo 16: Sistema «interno» de denúncias sem procedimentos coerentes

Uma empresa de serviços financeiros decide instituir um sistema de denúncias porque suspeita que existem práticas generalizadas de furto e de corrupção entre o seu pessoal e deseja incentivar os trabalhadores a fornecer informações sobre os colegas. Para poupar dinheiro, a empresa decide gerir o sistema internamente, recorrendo a funcionários do departamento de recursos humanos. Para incentivar os trabalhadores a utilizar o sistema, oferece uma recompensa monetária «sem fazer quaisquer perguntas» aos trabalhadores cujas denúncias conduzam à deteção de condutas impróprias e à recuperação de fundos.

A empresa tem, de facto, um interesse legítimo em detetar e prevenir práticas de furto e de corrupção. No entanto, o seu sistema de denúncias está tão mal concebido e desprovido de garantias que sobre os interesses da empresa prevalecem quer os interesses quer o direito ao respeito pela vida privada dos seus trabalhadores – em especial dos que podem ser vítimas de denúncias falsas apresentadas apenas com o objetivo de obter ganhos financeiros. Outro problema que se coloca neste caso é o facto de o sistema ser gerido internamente e não de forma independente, a par da falta de formação e de orientações sobre a utilização do sistema.

Segurança física, tecnologias de informação e segurança das redes

Exemplo 17: Controlos biométricos num laboratório de investigação

Um laboratório de investigação científica que trabalha com vírus mortais utiliza um sistema biométrico para controlar os acessos devido ao elevado risco para a saúde pública no caso de esses vírus saírem das instalações. São aplicadas garantias adequadas, incluindo o facto de os dados biométricos serem armazenados nos cartões pessoais dos trabalhadores e não num sistema centralizado.

Ainda que se trate de dados sensíveis, em sentido lato, o motivo do seu tratamento é de interesse público. Por essa razão, bem como pelo facto de os riscos de utilização abusiva serem reduzidos devido à utilização adequada de garantias, o artigo 7.º, alínea f), constitui uma base jurídica adequada para o tratamento.

Exemplo 18: Câmaras ocultas para identificar visitantes e trabalhadores fumadores

Uma empresa utiliza câmaras ocultas para identificar trabalhadores e visitantes que fumem em zonas do edifício onde não é permitido fumar.

Ainda que o responsável pelo tratamento tenha um interesse legítimo em garantir o cumprimento das normas que proíbem as pessoas de fumar, os meios utilizados para atingir esse objetivo são – de uma forma geral – desproporcionados e desnecessariamente intrusivos. Existem métodos menos intrusivos e mais transparentes (tal como detetores de fumo e sinais

de proibição visíveis). Assim, o tratamento não cumpre o disposto no artigo 6.º, que dispõe que os dados pessoais devem ser «não excessivos» relativamente às finalidades para as quais são recolhidos ou para as quais são tratados posteriormente. Ao mesmo tempo, provavelmente não preencherá os requisitos do teste da ponderação previsto no artigo 7.º.

Investigação científica

Exemplo 19: Investigação sobre os efeitos do divórcio ou da situação de desemprego dos pais nos resultados escolares dos filhos

No âmbito de um programa de investigação adotado pelo governo, e autorizado por uma comissão de ética competente, é realizada uma investigação sobre a relação entre o divórcio, a situação de desemprego dos pais e os resultados escolares dos filhos. Embora não sejam classificados como «categorias específicas de dados», a investigação incide sobre assuntos que muitas famílias consideram que envolvem informação muito íntima. A investigação permitirá que seja dado apoio educativo especial a crianças que de outro modo podem vir a cair no absentismo, ter fracos resultados escolares, ficar desempregados quando forem adultos ou enveredar pela criminalidade. A legislação do Estado-Membro em causa permite expressamente o tratamento de dados pessoais (que não sejam categorias específicas de dados) para fins de investigação, desde que a investigação seja necessária para a prossecução de interesses públicos importantes e realizada sob reserva de garantias adequadas, as quais são depois descritas com mais pormenor na legislação aplicável. Este quadro jurídico inclui requisitos específicos mas igualmente um quadro em matéria de responsabilidade, que permite avaliar caso a caso a admissibilidade da investigação (se for realizada sem o consentimento das pessoas em causa) e as medidas específicas a aplicar para proteger as pessoas em causa.

O investigador dirige um centro de investigação seguro e a informação relevante é fornecida ao centro de investigação, em condições de segurança, por conservatórias do registo civil,

tribunais, centros de emprego e escolas. Em seguida, o centro de investigação «encripta» a identidade das pessoas de modo a que os registos relativos a divórcios, situações de desemprego e educação possam ser relacionados mas sem revelar a identidade «civil» das pessoas – por exemplo, os nomes e as moradas. Todos os dados originais são depois eliminados definitivamente. São igualmente tomadas medidas para garantir a separação funcional (ou seja, que os dados serão utilizados apenas para fins de investigação) e reduzir qualquer risco de as pessoas serem novamente identificadas.

Os funcionários que trabalham no centro de investigação recebem formação rigorosa sobre segurança e respondem pessoalmente – e é possível que até criminalmente – por qualquer falha de segurança que seja da sua responsabilidade. São adotadas medidas técnicas e organizativas, por exemplo, para assegurar que os funcionários que utilizam dispositivos de memória USB não possam levar dados pessoais das instalações.

É do interesse legítimo do centro de investigação realizar a investigação, que se reveste de grande interesse público. É igualmente do interesse legítimo dos organismos ligados ao emprego e à educação, e de outros que estejam envolvidos no sistema, na medida em que os ajudará a planear e a prestar serviços aos que deles mais necessitam. Os aspetos do sistema relacionados com a vida privada foram bem concebidos e as garantias instituídas fazem com que sobre os interesses legítimos das organizações envolvidas na realização da investigação não prevaleçam os interesses ou o direito ao respeito pela vida privada nem dos pais nem dos filhos cujos registos serviram de base para a investigação.

Exemplo 20: Estudo sobre obesidade

Uma universidade pretende realizar uma investigação sobre os níveis de obesidade infantil em várias cidades e comunidades rurais. Apesar de ter geralmente dificuldade em obter autorização de escolas e de outras instituições para aceder aos dados relevantes, acaba por conseguir convencer algumas dezenas de professores a monitorizar, durante um determinado período, os alunos das suas turmas que pareçam obesos e a colocar-lhes questões sobre os seus hábitos alimentares, níveis de atividade física, utilização de jogos de computador, entre outros. Esses professores registam igualmente os nomes e as moradas dos alunos entrevistados para que lhes possa ser enviados um voucher de música em linha como

recompensa por participarem na investigação. Em seguida, os investigadores criam uma base de dados dos alunos, relacionando os níveis de obesidade com a atividade física e com outros fatores. As cópias em papel dos questionários da entrevista preenchidos – ainda num formulário que permite identificar determinadas crianças – são guardadas nos arquivos da universidade por um período não definido e sem medidas de segurança adequadas. Fotocópias de todos os questionários são partilhadas, a pedido, por qualquer estudante de mestrado ou de doutoramento dessa universidade e de universidades parceiras em todo o mundo, que manifeste interesse em utilizar os dados da investigação.

Embora seja do interesse legítimo da universidade realizar a investigação, há vários aspetos da conceção da investigação que fazem com que sobre esse interesse prevaleçam os interesses e o direito ao respeito pela vida privada dos alunos. Para além da metodologia de investigação, que carece de rigor científico, o problema decorre, em especial, da falta de abordagens que reforcem a privacidade na conceção da investigação e do acesso alargado aos dados pessoais recolhidos. Em momento algum os registos dos alunos são codificados ou objeto de anonimização e não são adotadas quaisquer outras medidas para garantir quer a segurança dos dados quer a separação funcional. Também não é obtido consentimento válido nos termos do artigo 7.º, alínea a), e do artigo 8.º, n.º 2, alínea a), nem resulta claro que tenha sido explicado, quer aos alunos quer aos respetivos pais, de que forma os dados serão utilizados e com quem serão partilhados.

Obrigação legal decorrente de legislação estrangeira

Exemplo 21: Cumprimento de exigências em matéria de direito fiscal de um país terceiro

Os bancos da UE recolhem e transferem dados de alguns dos seus clientes para efeitos de cumprimento, por parte destes, de obrigações fiscais em países terceiros. A recolha e a transferência são especificadas e efetuadas de acordo com as condições e as garantias acordadas entre a UE e o país estrangeiro num acordo internacional.

Ainda que uma obrigação legal decorrente de legislação estrangeira não possa, em si mesma, ser considerada uma base legítima para o tratamento nos termos do artigo 7.º, alínea c), tal é possível se essa obrigação estiver prevista num acordo internacional. Neste caso, o tratamento

pode ser considerado necessário para cumprir uma obrigação legal integrada no quadro jurídico interno pelo acordo internacional. No entanto, se tal acordo não existir, a recolha e a transferência deverão ser apreciadas nos termos dos requisitos previstos no artigo 7.º, alínea f), e apenas podem ser consideradas admissíveis se forem instituídas garantias adequadas, tal como as aprovadas pela autoridade responsável pela proteção de dados competente (ver igualmente o *Exemplo 15 supra*).

Exemplo 22: Transferência de dados sobre dissidentes

Quando solicitada, uma empresa da UE transfere dados de residentes estrangeiros para um regime autoritário num país terceiro, que pretende aceder aos dados de dissidentes (por exemplo, dados relativos ao tráfego de correio eletrónico, conteúdo das mensagens de correio eletrónico, histórico de navegação ou mensagens privadas em redes sociais).

Neste caso, ao contrário do exemplo anterior, não existe qualquer acordo internacional que permita a aplicação do artigo 7.º, alínea c), como fundamento jurídico. Além disso, vários elementos opõem-se à utilização do artigo 7.º, alínea f), como fundamento jurídico adequado. Embora o responsável pelo tratamento possa ter um interesse económico em assegurar que os pedidos do governo estrangeiro sejam satisfeitos (caso contrário, pode ser objeto de um tratamento menos favorável por parte do governo do país terceiro em comparação com outras empresas), a legitimidade e a proporcionalidade da transferência é altamente questionável à luz do quadro dos direitos fundamentais da UE. O seu impacto, potencialmente enorme, nas pessoas singulares em causa (por exemplo, discriminação, prisão, pena de morte) milita também, de forma muito significativa, a favor dos interesses e dos direitos das pessoas em causa.

Reutilização de dados publicamente disponíveis

Exemplo 23: Classificações de políticos¹²⁶

¹²⁶ Ver e comparar igualmente com o Exemplo 7 supra.

Uma ONG especializada em questões de transparência utiliza dados publicamente disponíveis sobre políticos (promessas realizadas na altura da sua eleição e resultados eleitorais efetivos) para classificá-los em função do cumprimento das promessas que realizaram.

Ainda que o impacto nos políticos em causa possa ser significativo, o facto de o tratamento se basear em informações públicas e dizer respeito às suas responsabilidades públicas, com a clara finalidade de reforçar a transparência e a responsabilidade, o equilíbrio é favorável ao interesse do responsável pelo tratamento¹²⁷.

Crianças e outras pessoas vulneráveis

Exemplo 24: Sítio Web de informação para jovens

Um sítio Web de uma ONG, que disponibiliza aconselhamento aos jovens sobre questões como o consumo de drogas, a gravidez indesejada e o consumo de álcool, recolhe dados, através do seu próprio servidor, sobre as pessoas que visitam o sítio. Em seguida, procede imediatamente à anonimização desses dados e transforma-os em estatísticas gerais sobre as partes do sítio Web que são mais populares entre os visitantes oriundos de diferentes regiões geográficas do país.

O artigo 7.º, alínea f), pode ser utilizado como fundamento jurídico, ainda que estejam em causa dados relativos a pessoas vulneráveis, porque o tratamento é de interesse público e são instituídas garantias rigorosas (os dados são imediatamente tornados anónimos e apenas utilizados para a criação de estatísticas), o que contribui para que o equilíbrio seja favorável ao responsável pelo tratamento.

Soluções de privacidade desde a conceção como garantias complementares

¹²⁷ Tal como nos *Exemplos 1 e 2*, parte-se do princípio de que a publicação é efetuada de forma correta e proporcionada – dependendo das circunstâncias do caso, a falta de garantias e outros fatores podem alterar o equilíbrio de interesses.

Exemplo 25: Acesso aos números de telemóvel de utilizadores e não-utilizadores de uma aplicação: «comparar e esquecer»

Os dados pessoais das pessoas são tratados para verificar se estas alguma vez deram o seu consentimento inequívoco (ou seja, «comparar e esquecer» como garantia).

Uma empresa que desenvolveu uma aplicação é obrigada a ter o consentimento inequívoco das pessoas em causa para poder proceder ao tratamento dos seus dados pessoais: por exemplo, a empresa que desenvolveu a aplicação pretende aceder e recolher todos os dados do livro de endereços eletrónico dos utilizadores da aplicação, incluindo os números de telemóvel dos contactos que não utilizam a aplicação. Para conseguir fazê-lo, pode ter de verificar primeiro se os detentores dos números de telemóvel constantes dos livros de endereços dos utilizadores da aplicação deram o seu consentimento inequívoco (nos termos do artigo 7.º, alínea a)) para o tratamento dos seus dados.

Para este tratamento inicial limitado (ou seja, o acesso breve, para efeitos de leitura, a todo o livro de endereços de um utilizador da aplicação), a empresa que desenvolveu a aplicação pode invocar o artigo 7.º, alínea f), como fundamento jurídico, sob reserva de garantias. Essas garantias devem incluir medidas técnicas e organizativas que assegurem que a empresa apenas utilize esse acesso para ajudar o utilizador a identificar quais são as pessoas, de entre os seus contactos, que já utilizam a aplicação e que, por conseguinte, já anteriormente deram o seu consentimento inequívoco à empresa para recolher e tratar dados de números de telefone para esse fim. Os números de telemóvel dos não-utilizadores apenas podem ser recolhidos e utilizados com o objetivo, rigorosamente limitado, de verificar se estes deram o seu consentimento inequívoco para o tratamento dos seus dados, devendo ser apagados imediatamente a seguir.

Combinação de informações pessoais nos serviços de Internet

Exemplo 26: Combinação de informações pessoais nos serviços de Internet

Uma empresa que disponibiliza vários serviços de Internet, incluindo motor de busca, partilha de vídeos e rede social, adota uma política de privacidade que contém uma cláusula que lhe

permite «combinar todas as informações pessoais» recolhidas sobre cada um dos seus utilizadores no que se refere aos vários serviços que estes utilizam, sem definir qualquer período de conservação dos dados. De acordo com a empresa, tal visa «garantir a melhor qualidade possível do serviço».

A empresa disponibiliza algumas ferramentas a várias categorias de utilizadores para que estes possam exercer os seus direitos (por exemplo, desativar publicidade dirigida, opor-se à instalação de determinado tipo de cookies).

No entanto, as ferramentas disponíveis não permitem aos utilizadores controlar efetivamente o tratamento dos seus dados: os utilizadores não conseguem controlar as combinações específicas dos seus dados entre serviços e não conseguem opor-se à combinação de dados que lhes dizem respeito. No âmbito geral, existe um desequilíbrio entre o interesse legítimo da empresa e a proteção dos direitos fundamentais dos utilizadores, e o artigo 7.º, alínea f), não deve ser invocado como fundamento jurídico para o tratamento. O artigo 7.º, alínea a), é um fundamento mais adequado, desde que estejam reunidas as condições para um consentimento válido.