MANUAL

Manual da Legislação Europeia sobre Proteção de Dados

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

A redação do presente manual foi concluída em abril de 2014.
As atualizações serão publicadas no sítio da Internet da FRA em: fra.europa.eu, no sítio da Internet do Conselho da Europa em: coe.int/dataprotection e no sítio da Internet do Tribunal Europeu dos Direitos do Homem, sob o menu «Case-Law», em: echr.coe.int

Europe Direct é um serviço que responde às suas perguntas sobre a União Europeia

Linha telefónica gratuita (*):

00 800 6 7 8 9 10 11

(*) As informações prestadas são gratuitas, tal como a maior parte das chamadas, embora alguns operadores, cabinas telefónicas ou hotéis as possam cobrar.

Crédito das fotos (portada e interior): © iStockphoto

Mais informações sobre a União Europeia encontram-se disponíveis na rede Internet, via servidor Europa (http://europa.eu).

Uma ficha catalográfica figura no fim desta publicação.

Luxemburgo: Serviço das Publicações da União Europeia, 2014

ISBN 978-92-871-9939-3 (Conselho da Europa)
ISBN 978-92-9239-498-1 (FRA)
doi:10.2811/73790

Printed in Belgium

Impresso em papel branqueado sem cloro elementar (ECF)

Manual da Legislação Europeia sobre Proteção de Dados

Prefácio

O presente Manual da Legislação Europeia sobre Proteção de Dados foi elaborado pela Agência dos Direitos Fundamentais da União Europeia (FRA) e pelo Conselho da Europa, em conjunto com a Secretaria do Tribunal Europeu dos Direitos do Homem. Tratase do terceiro numa série de manuais jurídicos elaborados em conjunto pela FRA e pelo Conselho da Europa. Em março de 2011, foi publicado um primeiro manual sobre a legislação europeia antidiscriminação e, em junho de 2013, um segundo manual sobre a legislação europeia em matéria de asilo, fronteiras e imigração.

Decidimos manter esta nossa colaboração num tema extremamente atual, que nos afeta a todos, todos os dias: a proteção de dados pessoais. A Europa goza de um dos sistemas mais protetores neste domínio, que assenta na Convenção 108 do Conselho da Europa, em instrumentos da União Europeia (UE) e na jurisprudência do Tribunal Europeu dos Direitos do Homem (TEDH) e do Tribunal de Justiça da União Europeia (TJUE).

O presente manual visa divulgar e melhorar os conhecimentos sobre as regras relativas à proteção de dados nos Estados-Membros da União Europeia e do Conselho da Europa, servindo como principal ponto de referência para os leitores. Tem por destinatários profissionais do Direito não especializados nesta área, juízes, autoridades nacionais de proteção de dados e outras pessoas que trabalham no campo da proteção de dados.

Com a entrada em vigor do Tratado de Lisboa em dezembro de 2009, a Carta dos Direitos Fundamentais da UE tornouse juridicamente vinculativa, o que conferiu à proteção de dados pessoais o estatuto de direito fundamental autónomo. Para proteger este direito fundamental, é crucial compreender melhor a Convenção 108 do Conselho da Europa e os instrumentos da UE, que abriram caminho para a proteção de dados na Europa, bem como a jurisprudência do TJUE e do TEDH.

Gostaríamos de agradecer ao Instituto de Direitos Humanos Ludwig Boltzmann pelo seu contributo na redação deste manual. Gostaríamos igualmente de expressar a nossa gratidão ao gabinete da Autoridade Europeia para a Proteção de Dados pelo seu apoio durante a fase de redação do manual. Agradecemos em particular à unidade de proteção de dados da Comissão Europeia pelo seu envolvimento durante a preparação deste manual. Por último, gostaríamos de expressar o nosso agradecimento à Comissão Nacional de Protecção de Dados – CNPD, pela revisão da tradução deste Manual para Português.

Philippe Boillat

Diretor Geral
de Direitos Humanos e Estado de Direito
Conselho da Europa

Morten Kjaerum

Diretor
da Agência dos Direitos Fundamentais
da União Europeia

Índice

PREFÁCIO 3

ABREVIATURAS, SIGLAS E ACRÓNIMOS 9

COMO UTILIZAR ESTE MANUAL 11

1. CONTEXTO E ANTECEDENTES DA LEGISLAÇÃO EUROPEIA SOBRE PROTEÇÃO DE DADOS 13
   - 1.1. O direito à proteção de dados 14
   - Pontos-chave 14
     - 1.1.1. A Convenção Europeia dos Direitos do Homem 14
     - 1.1.2. Convenção 108 do Conselho da Europa 15
     - 1.1.3. Legislação da União Europeia sobre proteção de dados 18
   - 1.2. Conciliação de direitos 22
   - Ponto-chave 22
     - 1.2.1. Liberdade de expressão 23
     - 1.2.2. Acesso aos documentos 27
     - 1.2.3. Liberdade das artes e das ciências 31
     - 1.2.4. Proteção da propriedade 33

2. TERMINOLOGIA SOBRE PROTEÇÃO DE DADOS 35
   - 2.1. Dados pessoais 36
   - Pontos-chave 36
     - 2.1.1. Principais aspetos do conceito de dados pessoais 37
     - 2.1.2. Categorias específicas de dados pessoais 44
     - 2.1.3. Dados anonimizados e pseudonimizados 45
   - 2.2. Tratamento de dados 48
   - Pontos-chave 48
   - 2.3. Os utilizadores de dados pessoais 50
   - Pontos-chave 50
     - 2.3.1. Responsáveis pelo tratamento e subcontratantes 51
     - 2.3.2. Destinatários e terceiros 57
   - 2.4. Consentimento 58
   - Pontos-chave 58
     - 2.4.1. Os elementos de um consentimento válido 59
     - 2.4.2. O direito de revogar o consentimento a todo o tempo 64

3. OS PRINCÍPIOS FUNDAMENTAIS DA LEGISLAÇÃO EUROPEIA SOBRE PROTEÇÃO DE DADOS 65
3.1. O princípio do tratamento lícito 66
Pontos-chave 66
3.1.1. Os requisitos de justificação da ingerência ao abrigo da CEDH 67
3.1.2. As condições do estabelecimento de restrições lícitas ao abrigo da Carta da UE 70
3.2. O princípio da especificação e da limitação da finalidade 72
Pontos-chave 72
3.3. Princípios relativos à qualidade dos dados 74
Pontos-chave 74
3.3.1. O princípio da pertinência dos dados 75
3.3.2. O princípio da exatidão dos dados 76
3.3.3. O princípio da limitação da conservação dos dados 77
3.4. O princípio do tratamento leal 78
Pontos-chave 78
3.4.1. Transparência 79
3.4.2. Criar uma relação de confiança 79
3.5. O princípio da responsabilidade 81
Pontos-chave 81

4. AS REGRAS DA LEGISLAÇÃO EUROPEIA SOBRE PROTEÇÃO DE DADOS 83
4.1. Regras sobre o tratamento lícito 85
Pontos-chave 85
4.1.1. Tratamento lícito de dados não sensíveis 85
4.1.2. Tratamento lícito de dados sensíveis 92
4.2. Regras sobre a segurança do tratamento 95
Pontos-chave 95
4.2.1. Elementos da segurança dos dados 96
4.2.2. Confidencialidade 99
4.3. Regras sobre a transparência do tratamento 100
Pontos-chave 100
4.3.1. Informação 101
4.3.2. Notificação 104
4.4. Regras sobre a promoção do cumprimento 105
Pontos-chave 105
4.4.1. Controlo prévio 106
4.4.2. Encarregados da proteção dos dados pessoais 106
4.4.3. Códigos de conduta 107

5. OS DIREITOS DAS PESSOAS EM CAUSA E A TUTELA DO SEU EXERCÍCIO 109
5.1. Os direitos dos titulares dos dados 111
Pontos-chave 111
5.1.1. Direito de acesso 112
5.1.2. Direito de oposição 119
5.2. Controlo independente 122
Pontos-chave 122
5.3. Recursos e sanções 127
Pontos-chave 127
5.3.1. Pedidos ao responsável pelo tratamento 127
5.3.2. Pedidos deduzidos perante a autoridade de controlo 129
5.3.3. Pedido deduzido perante o tribunal 130
5.3.4. Sanções 135

6. FLUXOS TRANSFRONTEIRIÇOS DE DADOS 137
6.1. Natureza dos fluxos transfronteiriços de dados 138
Pontos-chave 138
6.2. Livre fluxo de dados entre os Estados-Membros ou entre as Partes Contratantes 140
Pontos-chave 140
6.3. Livre fluxo de dados para países terceiros 141
Pontos-chave 141
6.3.1. Livre fluxo de dados devido a uma proteção adequada 142
6.3.2. Livre fluxo de dados em casos específicos 143
6.4. Restrições ao fluxo de dados para países terceiros 145
Pontos-chave 145
6.4.1. Cláusulas contratuais 146
6.4.2. Regras vinculativas para as empresas 148
6.4.3. Acordos internacionais especiais 148

7. PROTEÇÃO DE DADOS NO CONTEXTO DA ATIVIDADE POLICIAL E DA JUSTIÇA PENAL 153
7.1. Legislação do CdE sobre proteção de dados no domínio policial e da justiça penal 154
Pontos-chave 154
7.1.1. A Recomendação sobre a atividade policial 155
7.1.2. Convenção de Budapeste sobre o Cibercrime 158
7.2. Legislação da UE sobre proteção de dados em matéria policial e penal 159
Pontos-chave 159
7.2.1. A Decisão-Quadro relativa à proteção de dados 160

7.2.2. Instrumentos jurídicos mais específicos sobre a proteção de dados no âmbito da cooperação transfronteiriça entre autoridades policiais e judiciárias 162
7.2.3. Proteção de dados na Europol e na Eurojust 163
7.2.4. Proteção de dados nos sistemas de informação comuns ao nível da UE 167

8. OUTRA LEGISLAÇÃO EUROPEIA ESPECÍFICA SOBRE PROTEÇÃO DE DADOS 175
8.1. Comunicações eletrónicas 176
Pontos-chave 176
8.2. Dados sobre o emprego 181
Pontos-chave 181
8.3. Dados médicos 183
Ponto-chave 183
8.4. Tratamento de dados para fins estatísticos 186
Pontos-chave 186
8.5. Dados financeiros 189
Pontos-chave 189

LEITURA COMPLEMENTAR 193

JURISPRUDÊNCIA 199
Jurisprudência selecionada do Tribunal Europeu dos Direitos do Homem 199
Jurisprudência selecionada do Tribunal de Justiça da União Europeia 203

LISTA DE PROCESSOS 207

Abreviaturas, siglas e acrónimos

AEPD	Autoridade Europeia para a Proteção de Dados
BCR	Regras vinculativas para as empresas
Carta	Carta dos Direitos Fundamentais da União Europeia
CCTV	Circuito fechado de televisão
CE	Comunidade Europeia
CdE	Conselho da Europa
CEDH	Convenção Europeia dos Direitos do Homem
Convenção 108	Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Conselho da Europa)
CRM	Gestão do relacionamento com os clientes
C-SIS	Parte central do Sistema de Informação Schengen
DUDH	Declaração Universal dos Direitos do Homem
EEE	Espaço Económico Europeu
EFTA	Associação Europeia de Comércio Livre
ENISA	Agência Europeia para a Segurança das Redes e da Informação
ENU	Unidade Nacional Europol
ESMA	Autoridade Europeia dos Valores Mobiliários e dos Mercados
eTEN	Redes Transeuropeias de Telecomunicações
eu-LISA	Agência Europeia para os Sistemas Informáticos de Grande Escala
EuroPriSe	Selo Europeu de Privacidade
FRA	Agência dos Direitos Fundamentais da União Europeia
GPS	Sistema de posicionamento global
ICC	Instância Comum de Controlo
MDE	Mandado de Detenção Europeu
N-SIS	Parte nacional do Sistema de Informação Schengen

OCDE	Organização para a Cooperação e Desenvolvimento Económico
ONG	Organização não-governamental
ONU	Organização das Nações Unidas
PIN	Número de identificação pessoal
PNR	Registo de identificação dos passageiros
SEPA	Espaço Único de Pagamentos em Euros
SIA	Sistema de Informação Aduaneiro
SIS	Sistema de Informação Schengen
STCE	Série de Tratados do Conselho da Europa
SWIFT	Sociedade das Telecomunicações Financeiras Interbancárias no Mundo
TEDH	Tribunal Europeu dos Direitos do Homem
TFUE	Tratado sobre o Funcionamento da União Europeia
TJUE	Tribunal de Justiça da União Europeia (antes de dezembro de 2009, designavase Tribunal de Justiça das Comunidades Europeias, TJCE)
Tratado UE	Tratado da União Europeia
UE	União Europeia
VIS	Sistema de Informação sobre Vistos

Como utilizar este manual

O presente manual apresenta uma visão geral da legislação aplicável à proteção de dados em relação à União Europeia (UE) e ao Conselho da Europa (CdE).

O manual visa auxiliar os profissionais do Direito que não são especializados na área da proteção de dados; destinase a juristas, advogados, juízes e outros profissionais, bem como a pessoas que trabalham para outros organismos, como organizações não-governamentais (ONG), que poderão ser confrontados com questões jurídicas relacionadas com proteção de dados.

Trata-se de um primeiro ponto de referência sobre a legislação da UE e a Convenção Europeia dos Direitos do Homem (CEDH) em matéria de proteção de dados, explicando de que modo esta área do Direito é regulada na legislação da UE e na CEDH, bem como na Convenção do CdE para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108) e em outros instrumentos do CdE. No início de cada capítulo é apresentado um quadro com as disposições legais aplicáveis, incluindo jurisprudência importante, ao abrigo dos dois sistemas jurídicos europeus. De seguida, são apresentados sucessivamente os instrumentos legislativos destes dois ordenamentos jurídicos aplicáveis a cada tópico. Deste modo, o leitor poderá aperceberse facilmente das semelhanças e diferenças entre os dois sistemas jurídicos.

Os quadros que figuram no início de cada capítulo enumeram os tópicos que nele serão abordados e identificam as disposições legais aplicáveis e outro material relevante, nomeadamente jurisprudência. A ordem dos tópicos poderá ser ligeiramente diferente da estrutura do texto de cada capítulo se tal for considerado conveniente para assegurar uma apresentação concisa do seu conteúdo. Os quadros abrangem o direito do CdE e o direito da UE, o que deverá ajudar os leitores a encontrar as informações mais importantes aplicáveis ao seu caso, especialmente se estiverem unicamente sujeitos ao direito do CdE.

Os profissionais de Estados não pertencentes à UE que sejam membros do CdE e partes na CEDH e na Convenção 108 podem encontrar as informações relevantes para o seu próprio país consultando diretamente as secções sobre o CdE. Os profissionais dos Estados-Membros da UE terão de consultar as duas secções, dado que estão sujeitos a ambos os ordenamentos jurídicos. A secção «Leitura complementar» do manual contém uma lista de material de referência mais especializado que poderá ser útil para aqueles que necessitem de mais informações sobre uma questão específica.

O direito do CdE é apresentado através de breves referências a processos do Tribunal Europeu dos Direitos do Homem (TEDH), que foram selecionados de entre o vasto número de acórdãos e decisões do TEDH sobre questões relacionadas com proteção de dados.

O direito da UE abrange as medidas legislativas adotadas, as disposições relevantes dos Tratados e a Carta dos Direitos Fundamentais da União Europeia, tal como interpretadas na jurisprudência do Tribunal de Justiça da União Europeia (TJUE, que se designava Tribunal de Justiça das Comunidades Europeias [TJCE] antes de 2009).

A jurisprudência descrita ou citada no presente manual fornece exemplos de um importante conjunto de acórdãos e decisões do TEDH e do TJUE. As orientações apresentadas no final deste manual visam ajudar o leitor a pesquisar jurisprudência na Internet.

Além disso, são apresentados exemplos práticos com cenários hipotéticos em caixas de texto para ilustrar melhor a aplicação das regras europeias sobre proteção de dados na prática, sobretudo nos casos em que não existe jurisprudência específica do TEDH ou do TJUE sobre a matéria em causa.

O manual começa com uma breve descrição do papel dos dois sistemas jurídicos estabelecidos pela CEDH e pelo direito da UE (capítulo 1). Os capítulos 2 a 8 abrangem as seguintes questões:

- terminologia sobre proteção de dados;
- princípios fundamentais da legislação europeia sobre proteção de dados;
- regras da legislação europeia sobre proteção de dados;
- direitos dos titulares dos dados e a tutela do seu exercício;
- fluxos transfronteiriços de dados;
- proteção de dados no contexto da atividade policial e da justiça penal;
- outra legislação europeia específica sobre proteção de dados.

1

Contexto e antecedentes da legislação europeia sobre proteção de dados

UE	Questões abrangidas	CdE
O direito à proteção de dados		
Diretiva 95/46/CE relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Diretiva de Proteção de Dados), JO L 281, 1995		CEDH, artigo 8.º (direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência) Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108)
Conciliação de direitos		
TJUE, acórdão de 9 de novembro de 2010 nos processos apensos C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen*	**Em geral**	
TJUE, acórdão de 16 de dezembro de 2008 no processo C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy e Satamedia Oy*	**Liberdade de expressão**	TEDH, acórdão *Axel Springer AG c. Alemanha* de 7 de fevereiro de 2012 TEDH, acórdão *Mosley c. Reino Unido* de 10 de maio de 2011
	Liberdade das artes e das ciências	TEDH, acórdão *Vereinigung bildender Künstler c. Áustria* de 25 de janeiro de 2007
TJUE, acórdão de 29 de janeiro de 2008 no processo C275/06, *Productores de Música de España (Promusicae)/ Telefónica de España SAU*	**Proteção da propriedade**	
TJUE, acórdão de 29 de junho de 2010 no processo C28/08 P, *Comissão Europeia/The Bavarian Lager Co. Ltd*	**Acesso aos documentos**	TEDH, acórdão *Társaság a Szabadságjogokért c. Hungria* de 14 de abril de 2009

1.1. O direito à proteção de dados

Pontos-chave

- Nos termos do artigo 8.º da CEDH, o direito à proteção contra a recolha e utilização de dados pessoais faz parte do direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência.
- A Convenção 108 do CdE é o primeiro instrumento internacional juridicamente vinculativo que regula expressamente a proteção de dados.
- Ao nível da UE, a proteção de dados foi regulada pela primeira vez pela Diretiva de Proteção de Dados.
- No direito da UE, a proteção de dados é reconhecida como um direito fundamental.

O direito à proteção contra intromissões de terceiros, especialmente do Estado, na vida privada foi consagrado pela primeira vez num instrumento jurídico internacional no artigo 12.º da Declaração Universal dos Direitos do Homem (DUDH) das Nações Unidas, de 1948, relativo ao respeito pela vida privada e familiar.[1] A DUDH influenciou a formulação de outros instrumentos sobre direitos humanos na Europa.

1.1.1. A Convenção Europeia dos Direitos do Homem

Criado no rescaldo da II Guerra Mundial, o Conselho da Europa reúne os Estados da Europa com o objetivo de promover o Estado de direito, a democracia, os direitos humanos e o desenvolvimento social. Para este efeito, adotou a Convenção Europeia dos Direitos do Homem (CEDH) em 1950, que entrou em vigor em 1953.

Os Estados estão sujeitos a uma obrigação internacional de cumprimento da CEDH. Todos os Estados membros do CdE incorporaram ou deram cumprimento à CEDH no seu direito nacional, pelo que são obrigados a atuar em conformidade com as disposições da Convenção.

Em 1959, foi criado em Estrasburgo, França, o Tribunal Europeu dos Direitos do Homem (TEDH) para garantir que as Partes Contratantes cumprem as obrigações assumidas ao abrigo da CEDH. O TEDH assegura o cumprimento das obrigações assumidas pelos Estados ao abrigo da Convenção através da apreciação de queixas apresentadas por cidadãos, grupos de cidadãos, ONG ou pessoas coletivas que

1 Declaração Universal dos Direitos do Homem (DUDH) das Nações Unidas, de 10 de dezembro de 1948.

aleguem violações da Convenção. Em 2013, o Conselho da Europa era constituído por 47 Estados membros, 28 dos quais são também Estados-Membros da UE. Para apresentar uma petição ao TEDH, não é necessário ser nacional de um dos Estados membros. O TEDH também pode conhecer de ações instauradas por um ou mais Estados membros do CdE contra outro Estado membro.

O direito à proteção de dados pessoais faz parte dos direitos tutelados pelo artigo 8.º da CEDH, que garante o direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência e estabelece as condições em que são permitidas restrições a este direito.[2]

Através da sua jurisprudência, o TEDH pronunciouse sobre muitas situações em que foi suscitada a questão da proteção de dados, entre as quais importa destacar questões relacionadas com a interceção de comunicações,[3] várias formas de vigilância[4] e proteção contra o armazenamento de dados pessoais pelas autoridades públicas.[5] O TEDH esclareceu que o artigo 8.º da CEDH não só obriga os Estados a absteremse de praticar atos suscetíveis de violar este direito consagrado na Convenção como impõe também, em certos casos, uma obrigação positiva de assegurar ativamente o respeito efetivo pela vida privada e familiar.[6] Muitos destes casos serão mencionados, em pormenor, nos capítulos adequados.

1.1.2. Convenção 108 do Conselho da Europa

O surgimento da tecnologia da informação na década de 60 foi acompanhado por uma crescente necessidade de adotar regras mais pormenorizadas para salvaguardar as pessoas através da proteção dos seus dados (pessoais). Em meados da década de 70, o Comité de Ministros do Conselho da Europa adotou várias resoluções sobre a proteção de dados pessoais que faziam referência ao artigo 8.º da

2 CdE, Convenção Europeia dos Direitos do Homem, STCE n.º. 005, 1950.

3 Ver, por exemplo, TEDH, acórdão *Malone c. Reino Unido* de 2 de agosto de 1984, petição n.º 8691/79; TEDH, acórdão *Copland c. Reino Unido* de 3 de abril de 2007, petição n.º 62617/00.

4 Ver, por exemplo, TEDH, acórdão *Klass e o. c. Alemanha* de 6 de setembro de 1978, petição n.º 5029/71; TEDH, acórdão *Uzun c. Alemanha* de 2 de Setembro de 2010, petição n.º 35623/05.

5 Ver, por exemplo, TEDH, acórdão *Leander c. Suécia* de 26 de março de 1987, petição n.º 9248/81; TEDH, acórdão *S. and Marper c. Reino Unido* de 4 de dezembro de 2008, petições n.ºs 30562/04 e 30566/04.

6 Ver, por exemplo, TEDH, acórdão *I. c. Finlândia* de 17 de julho de 2008, petição n.º 20511/03; TEDH, acórdão *K.U. c. Finlândia* de 2 de dezembro de 2008, petição n.º 2872/02.

CEDH.[7] Em 1981, foi aberta a assinatura a Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal (Convenção 108)[8]. A Convenção 108 era, e ainda é, o único instrumento internacional juridicamente vinculativo no domínio da proteção de dados.

A Convenção 108 aplica-se a todos os tratamentos de dados pessoais realizados tanto pelo setor privado como pelo setor público, incluindo os tratamentos de dados efetuados pelas autoridades policiais e judiciárias. Protege as pessoas contra os abusos que podem acompanhar a recolha e o tratamento de dados pessoais e procura simultaneamente regular o fluxo transfronteiriço de dados pessoais. Quanto à recolha e tratamento de dados pessoais, os princípios estabelecidos na Convenção respeitam, em especial, à recolha e tratamento automatizado de dados de forma leal e lícita, armazenados para finalidades determinadas e legítimas, não podendo ser utilizados para fins incompatíveis com essas finalidades nem conservados por tempo superior ao necessário. Dizem também respeito à qualidade dos dados, estabelecendo, em especial, que têm de ser adequados, pertinentes e não excessivos (proporcionalidade), bem como exatos.

Além de prever garantias relativas à recolha e tratamento de dados pessoais, a Convenção proíbe, na ausência de garantias jurídicas adequadas, o tratamento de dados «sensíveis», tais como dados sobre a raça, a opinião política, a saúde, as convicções religiosas, a vida sexual ou o registo criminal de uma pessoa.

A Convenção consagra igualmente o direito das pessoas a saberem que existem informações armazenadas a seu respeito e, se necessário, a que as mesmas sejam retificadas. Só são admitidas restrições aos direitos estabelecidos na Convenção quando estiverem em causa interesses superiores, como a proteção da segurança do Estado.

7 CdE, Comité de Ministros (1973), *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector* (Resolução (73) 22 relativa à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de dados no setor privado), de 26 de setembro de 1973; CdE, Comité de Ministros (1974), *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector* (Resolução (74) 29 relativa à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de dados no setor público), 20 de Setembro de 1974.

8 CdE, Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, Conselho da Europa, STCE n.º 108, 1981.

Embora a Convenção preveja o livre fluxo de dados pessoais entre os Estados signatários, também impõe algumas restrições aos fluxos para Estados cuja regulamentação não proporcione uma proteção equivalente.

O Comité de Ministros do CdE adotou várias recomendações (que não são juridicamente vinculativas) para desenvolver os princípios gerais e as regras estabelecidos na Convenção 108 (ver capítulos 7 e 8).

Todos os Estados-Membros da UE ratificaram a Convenção 108. Em 1999, a Convenção foi alterada para permitir a adesão da UE.[9] Em 2001, foi adotado um protocolo adicional à Convenção 108 que estabelece disposições sobre fluxos transfronteiriços de dados para Estados não signatários, os chamados países terceiros, e sobre a criação obrigatória de autoridades nacionais de controlo de proteção de dados. [10]

Perspetivas

Na sequência da decisão de modernizar a Convenção 108, foi realizada uma consulta pública em 2011 que permitiu confirmar os dois principais objetivos daquele trabalho: reforçar a proteção da privacidade no espaço digital e fortalecer o mecanismo de acompanhamento da Convenção.

A Convenção 108 está aberta à adesão de Estados que não sejam membros do CdE, incluindo países não europeus. O potencial da Convenção para se afirmar como uma norma universal e o seu caráter aberto poderiam servir de base para promover a proteção de dados a nível mundial.

Atualmente, 45 das 46 Partes Contratantes da Convenção 108 são Estados membros do CdE. O Uruguai foi o primeiro país não europeu a aderir à Convenção 108 em agosto de 2013 e Marrocos, que foi convidado a aderir à Convenção pelo Comité de Ministros, está a formalizar a sua adesão.

9 CdE, Alterações à Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (STCE n.º 108) que permitem a adesão das Comunidades Europeias, adotadas pelo Comité de Ministros em Estrasburgo, em 15 de junho de 1999; artigo 23.º, n.º 2, da Convenção 108 na redação em vigor.

10 CdE, Protocolo Adicional à Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, respeitante às autoridades de controlo e aos fluxos transfronteiriços de dados, STCE n.º 181, 2001.

1.1.3. Legislação da União Europeia sobre proteção de dados

O direito da UE é constituído pelos tratados e pelo direito secundário. Os tratados, nomeadamente o Tratado da União Europeia (TUE) e o Tratado sobre o Funcionamento da União Europeia (TFUE), foram aprovados por todos os Estados-Membros da UE e também são conhecidos por «direito primário da UE». Os regulamentos, diretivas e decisões da UE foram adotados pelas instituições da UE ao abrigo da competência que lhes foi atribuída pelos tratados; estes instrumentos são frequentemente designados por «direito secundário da UE».

O principal instrumento jurídico da UE sobre proteção de dados é a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (*Diretiva de Proteção de Dados*).[11] Esta Diretiva foi adotada em 1995, numa altura em que vários Estados-Membros tinham já adotado leis nacionais sobre proteção de dados. A livre circulação de mercadorias, capitais, serviços e pessoas no mercado interno exigia o livre fluxo de dados, que só seria possível se os Estados-Membros pudessem confiar na existência de um nível uniformemente elevado de proteção de dados.

Uma vez que o objetivo da aprovação da Diretiva de Proteção de Dados era a harmonização[12] da legislação sobre proteção de dados a nível nacional, é previsto um grau de especificidade comparável ao da legislação nacional sobre proteção de dados (então) em vigor. Para o TJUE, «a Diretiva 95/46 visa [...] tornar equivalente em todos os Estados-Membros o nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais [...] A aproximação das legislações nacionais aplicáveis na matéria não deve fazer diminuir a proteção que asseguram, devendo, pelo contrário, ter por objetivo garantir um elevado nível de proteção na União Assim, [...] a harmonização das referidas legislações nacionais não se limita a uma harmonização mínima, mas conduz a uma harmonização que é, em princípio, completa.»[13]. Consequentemente, os Estados-Membros dispõem apenas de uma pequena margem de manobra na aplicação da Diretiva.

11 Diretiva de Proteção de Dados (JO L 281, 1995, p. 31).

12 Ver, por exemplo, Diretiva de Proteção de Dados, considerandos 1, 4, 7 e 8.

13 TJUE, acórdão de 24 de novembro de 2011, nos processos apensos C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estad*, n.ºs 28 e 29.

A Diretiva de Proteção de Dados visa dar corpo aos princípios do direito à privacidade já consagrados na Convenção 108 e alargar a sua aplicação. O facto de os 15 Estados-Membros da UE em 1995 serem também Partes Contratantes da Convenção 108 exclui a adoção de regras contraditórias nestes dois instrumentos jurídicos. No entanto, a Diretiva de Proteção de Dados explora a possibilidade, prevista no artigo 11.º da Convenção 108, de adotar novos instrumentos de proteção. Em especial, o estabelecimento de autoridades de controlo independentes como meio de melhorar o cumprimento das regras sobre proteção de dados revelouse um importante contributo para a aplicação eficaz da legislação europeia sobre proteção de dados. (Consequentemente, este elemento foi incorporado no direito do CdE em 2001 pelo Protocolo Adicional à Convenção 108).

O âmbito de aplicação territorial da Diretiva de Proteção de Dados não se limita aos 28 Estados-Membros da UE, incluindo também os Estados que não são membros da UE mas que fazem parte do Espaço Económico Europeu (EEE)[14] – a saber, a Islândia, o Listenstaine e a Noruega.

O TJUE no Luxemburgo tem competência para determinar se um Estado-Membro cumpriu as suas obrigações ao abrigo da Diretiva de Proteção de Dados e para proferir decisões a título prejudicial sobre a validade e a interpretação da Diretiva, a fim de assegurar a sua aplicação efetiva e uniforme nos Estados-Membros. Uma importante exceção à aplicação da Diretiva é a chamada «exceção doméstica», que diz respeito ao tratamento de dados pessoais por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas.[15] Este tratamento é geralmente considerado parte das liberdades pessoais.

Correspondendo ao direito primário da UE em vigor à data da adoção da Diretiva de Proteção de Dados, o âmbito de aplicação material da Diretiva abrange apenas matérias do mercado interno. Das matérias que ficam fora do seu âmbito de aplicação importa destacar a cooperação no domínio policial e da justiça penal. A proteção de dados nestas matérias baseiase em instrumentos jurídicos diferentes, que são descritos pormenorizadamente no capítulo 7.

Uma vez que a Diretiva de Proteção de Dados só podia ter por destinatários os Estados Membros da UE, era necessário um outro instrumento jurídico para assegurar a proteção de dados nos casos de tratamento de dados pessoais pelas instituições

14 Acordo sobre o Espaço Económico Europeu, JO 1994 L 1, que entrou em vigor em 1 de janeiro de 1994.

15 Diretiva de Proteção de Dados, artigo 3.º, n.º 2, segundo travessão.

e órgãos da UE. O Regulamento (CE) n.º 45/2001 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 (*Regulamento Proteção de Dados [Instituições da UE]*) desempenha esta função.[16]

Além disso, mesmo em áreas abrangidas pela Diretiva de Proteção de Dados, surge muitas vezes a necessidade de estabelecer disposições mais detalhadas em matéria de proteção de dados para assegurar a necessária clareza na conciliação com outros interesses legítimos. Dois exemplos são a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (*Diretiva relativa à privacidade e às comunicações eletrónicas*)[17] e a Diretiva 2006/24/CE relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE (*Diretiva da Conservação de Dados,* invalidada em 8 de abril de 2014).[18] Serão analisados outros exemplos no capítulo 8. Estas disposições têm de estar conformes com a Diretiva de Proteção de Dados.

A Carta dos Direitos Fundamentais da União Europeia

Os tratados originais das Comunidades Europeias não continham qualquer referência aos direitos humanos ou à sua proteção. Contudo, face aos processos instaurados no então Tribunal de Justiça das Comunidades Europeias (TJCE) com fundamento em alegadas violações dos direitos humanos no âmbito da legislação da UE, este desenvolveu uma nova abordagem. A fim de conceder proteção às pessoas singulares, incorporou os direitos fundamentais nos chamados princípios gerais de direito europeu. Segundo o TJUE, estes princípios gerais refletem as disposições sobre proteção dos direitos humanos constantes das constituições nacionais e dos tratados sobre direitos humanos, em especial a CEDH. O TJUE afirmou que asseguraria a conformidade do direito da UE com estes princípios.

16 Regulamento (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, 2001).

17 Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (*Diretiva relativa à privacidade e às comunicações eletrónicas*), JO L 201, 2002.

18 Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE (*Diretiva Conservação de Dados*), JO L 105, 2006 . Considerada inválida pelo TJUE em 8 de abril de 2014.

Reconhecendo que as suas políticas poderiam afetar os direitos humanos e num esforço para aproximar os cidadãos da União, a UE proclamou, em 2000, a Carta dos Direitos Fundamentais da União Europeia (Carta). Esta Carta incorpora todos os direitos civis, políticos, económicos e sociais dos cidadãos europeus, sintetizando as tradições constitucionais e as obrigações internacionais comuns aos Estados-Membros. Os direitos descritos na Carta estão divididos em seis secções: dignidade, liberdades, igualdade, solidariedade, cidadania e justiça.

Embora originalmente não passasse de um documento político, a Carta tornouse juridicamente vinculativa[19] como direito primário da UE (ver artigo 6.º, n.º 1, do TUE) com a entrada em vigor do Tratado de Lisboa em 1 de dezembro de 2009.[20]

O direito primário da UE também atribui à UE competência genérica para legislar sobre matérias relacionadas com a proteção de dados (artigo 16.º do TFUE).

Para além de garantir o respeito pela vida privada e familiar (artigo 7.º), a Carta consagra também o direito à proteção de dados (artigo 8.º), elevando expressamente o nível desta proteção ao de um direito fundamental no direito da UE. As instituições da UE e os Estados-Membros têm de observar e garantir este direito, que também é aplicável aos Estados-Membros quando aplicam o direito da União (artigo 51.º da Carta). Tendo sido formulado vários anos após a adoção da Diretiva de Proteção de Dados, o artigo 8.º da Carta deve ser interpretado no sentido de incorporar a legislação da UE sobre proteção de dados preexistente. Por conseguinte, a Carta não só menciona expressamente o direito à proteção de dados no artigo 8.º, n.º 1, como também faz referência a princípios fundamentais da proteção de dados no artigo 8.º, n.º 2. Por último, o artigo 8.º, n.º 3, da Carta assegura a fiscalização da aplicação destes princípios por uma autoridade independente.

Perspetivas

Em janeiro de 2012, a Comissão Europeia propôs um pacote de reforma legislativa sobre a proteção de dados, afirmando que era necessário modernizar as atuais regras sobre proteção de dados à luz da rápida evolução tecnológica e da globalização. O pacote de reforma legislativa consiste numa proposta de Regulamento geral

19 UE (2012), Carta dos Direitos Fundamentais da União Europeia, JO C 326, 2012 .

20 Ver versões consolidadas de Comunidades Europeias (2012), Tratado da União Europeia, JO C 326, 2012 ; e de Comunidades Europeias (2012), TFUE, JO C 326, 2012.

sobre a proteção de dados[21], que deverá substituir a Diretiva de Proteção de Dados, bem como numa nova Diretiva de Proteção de Dados,[22] que conterá disposições sobre a proteção de dados na área da cooperação policial e judiciária em matéria penal. À data da publicação do presente manual, estava em curso o debate sobre o pacote de reforma legislativa.

1.2. Conciliação de direitos

Ponto-chave

- O direito à proteção de dados não é um direito absoluto; tem de ser conciliado com outros direitos.

O direito fundamental à proteção de dados pessoais, consagrado no artigo 8.º da Carta, «não é uma prerrogativa absoluta, mas deve ser tomado em consideração relativamente à sua função na sociedade».[23] Assim, o artigo 52.º, n.º 1, da Carta admite a introdução de restrições ao exercício de direitos como os consagrados nos seus artigos 7.º e 8.º, desde que essas restrições estejam previstas na lei, respeitem o conteúdo essencial desses direitos e liberdades e, na observância do princípio da proporcionalidade, sejam necessárias e correspondam efetivamente a objetivos de interesse geral reconhecidos pela União Europeia, ou à necessidade de proteção dos direitos e liberdades de terceiros.[24]

No sistema da CEDH, a proteção de dados é garantida pelo artigo 8.º (direito ao respeito pela vida privada e familiar) e, tal como no sistema da Carta, este direito tem de ser exercido respeitando o âmbito de outros direitos concorrentes. Nos termos do artigo 8.º, n.º 2, da CEDH, «Não pode haver ingerência da autoridade pública no

21 Comissão Europeia (2012), *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) 11 final, Bruxelas, 25 de janeiro de 2012.

22 Comissão Europeia (2012), *Proposta de Diretiva do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados (Diretiva geral sobre a proteção de dados)*, COM(2012) 10 final, Bruxelas, 25 de janeiro de 2012.

23 Ver, por exemplo, TJUE, acórdão de 9 de novembro de 2010 nos processos apensos C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen*, n.º 48.

24 *Ibid.* n.º 50.

exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para [...] a proteção dos direitos e das liberdades de terceiros.»

Consequentemente, tanto o TEDH como o TJUE têm afirmado repetidamente que a aplicação e a interpretação do artigo 8.º da CEDH e do artigo 8.º da Carta exigem a conciliação com outros direitos.[25] Vários exemplos importantes ilustrarão como poderá ser feita esta conciliação.

1.2.1. Liberdade de expressão

Um dos direitos que entrará provavelmente em conflito com o direito à proteção de dados é o direito à liberdade de expressão.

A liberdade de expressão é um direito protegido pelo artigo 11.º da Carta («Liberdade de expressão e de informação»). Este direito abrange a «liberdade de opinião e a liberdade de receber e de transmitir informações ou ideias, sem que possa haver ingerência de quaisquer poderes públicos e sem consideração de fronteiras». O artigo 11.º corresponde ao artigo 10.º da CEDH. Nos termos do artigo 52.º, n.º 3, da Carta, na medida em que contenha direitos correspondentes aos direitos garantidos pela CEDH, «o sentido e o âmbito desses direitos são iguais aos conferidos por essa Convenção». As restrições que podem ser licitamente impostas sobre o direito garantido pelo artigo 11.º da Carta não poderão, portanto, ultrapassar as previstas no artigo 10.º, n.º 2, da CEDH, ou seja, têm de estar previstas na lei e constituir providências necessárias, numa sociedade democrática «para a [...] proteção da honra ou dos direitos de outrem». Este conceito abrange o direito à proteção de dados.

A relação entre a proteção de dados pessoais e a liberdade de expressão é regulada pelo artigo 9.º da Diretiva de Proteção de Dados, sob a epígrafe «Tratamento de dados pessoais e liberdade de expressão».[26] Nos termos deste artigo, os

25 TEDH, acórdão *Von Hannover c. Alemanha (n.º 2)* [GS] de 7 de fevereiro de 2012, petições n.ºs 40660/08 e 60641/08; TJUE, acórdão de 24 de novembro de 2011 nos processos apensos C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, n.º 48; TJUE, acórdão de 29 de janeiro de 2008 no processo C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, n.º 68. Ver também Conselho da Europa (2013), Case law of the European Court of Human Rights concerning the protection of personal data, DP (2013) Case law, disponível em: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_FINAL.pdf.

26 Diretiva de Proteção de Dados, artigo 9.º.

Estadosmembros são chamados a instituir determinadas isenções ou derrogações à proteção de dados, e portanto ao direito fundamental à vida privada, prevista nos capítulos II, IV e VI dessa diretiva. Essas derrogações devem ser criadas para fins exclusivamente jornalísticos ou de expressão artística ou literária, que se enquadram no âmbito do direito fundamental à liberdade de expressão, apenas na medida em que sejam necessárias para conciliar o direito à vida privada com as normas que regem a liberdade de expressão.

Exemplo: No processo que deu origem ao acórdão *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy e Satamedia Oy*,[27] foi pedido ao TJUE que interpretasse o artigo 9.º da Diretiva de Proteção de Dados e definisse a relação entre a proteção de dados e a liberdade de imprensa. O Tribunal de Justiça analisou a divulgação pela Markkinapörssi e pela Satamedia dos dados fiscais de cerca de 1,2 milhões de pessoas singulares licitamente obtidos junto das autoridades fiscais finlandesas. Em especial, o Tribunal de Justiça teve de determinar se o tratamento dos dados pessoais disponibilizados pelas autoridades fiscais para que os utilizadores de telemóveis recebessem dados fiscais relativos a outras pessoas singulares deve ser considerado uma atividade realizada para fins exclusivamente jornalísticos. Tendo concluído que as atividades da Satakunnan constituíam «tratamento de dados pessoais» na aceção do artigo 3.º, n.º 1, da Diretiva de Proteção de Dados, o Tribunal de Justiça passou então a interpretar o artigo 9.º da Diretiva. Em primeiro lugar, chamou a atenção para a importância da liberdade de expressão nas sociedades democráticas e defendeu que os conceitos relacionados com essa liberdade, como o de jornalismo, deveriam ser interpretados de forma ampla. Seguidamente, observou que, para obter uma ponderação equilibrada entre os dois direitos fundamentais, as isenções e derrogações à proteção de dados devem ser aplicadas apenas na medida estritamente necessária. Naquelas circunstâncias, o Tribunal de Justiça considerou que atividades como as que eram desenvolvidas pela Markkinapörssi e pela Satamedia relativas a dados contidos em documentos que são públicos nos termos da legislação nacional podem ser qualificadas de «atividades jornalísticas» se tiverem por finalidade a divulgação ao público de informações, opiniões ou ideias, independentemente do respetivo meio de transmissão. O Tribunal de Justiça também entendeu que essas atividades não estão reservadas às empresas de comunicação social e podem ter fins lucrativos. Contudo, o TJUE

27 TJUE, acórdão de 16 de dezembro de 2008 no processo C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy e Satamedia Oy*, n.ºs 56, 61 e 62.

considerou que competia ao órgão jurisdicional nacional apreciar se era esse o caso no processo principal.

O TEDH proferiu vários acórdãos históricos sobre a conciliação entre o direito à proteção de dados e o direito à liberdade de expressão.

Exemplo: No acórdão *Axel Springer AG c. Alemanha,*[28] o TEDH entendeu que a proibição imposta por um tribunal nacional sobre o proprietário de um jornal que pretendia publicar um artigo sobre a detenção e condenação de um ator muito conhecido violava o artigo 10.º da CEDH. O TEDH reiterou os critérios que tinha estabelecido na sua jurisprudência no domínio da conciliação entre o direito à liberdade de expressão e o direito ao respeito pela vida privada.

- em primeiro lugar, se o acontecimento a que o artigo publicado se referia era de interesse geral: a detenção e condenação de uma pessoa era um facto judicial público e, como tal, de interesse público;

- em segundo lugar, se a pessoa em causa era uma figura pública: a pessoa em causa era um ator suficientemente conhecido para ser considerado uma figura pública; e

- em terceiro lugar, o modo como as informações foram obtidas e se eram fidedignas: as informações tinham sido fornecidas pelos serviços do Ministério Público e nenhuma das partes contestava a exatidão das informações contidas em ambas as publicações.

Por conseguinte, o TEDH considerou que as restrições à publicação impostas sobre a empresa não eram razoavelmente proporcionais ao objetivo legítimo de proteger a vida privada do requerente. O TEDH concluiu que tinha havido uma violação do artigo 10.º da CEDH.

Exemplo: No acórdão *Von Hannover c. Alemanha (n.º 2),*[29] o TEDH concluiu que o facto de os tribunais nacionais terem indeferido o pedido de medidas cautelares apresentado pela Princesa Carolina do Mónaco requerendo a proibição da

28 TEDH, acórdão *Axel Springer AG c. Alemanha* [GS] de 7 de fevereiro de 2012, petição n.º 39954/08, n.ºs 90 e 91.

29 TEDH, acórdão *Von Hannover c. Alemanha (n.º 2)* [GS] de 7 de fevereiro de 2012, petições n.ºs 40660/08 e 60641/08, n.ºs 118 e 124.

publicação de uma fotografia sua e do seu marido tirada durante umas férias numa estância de esqui não constituía uma violação do direito ao respeito pela vida privada nos termos do artigo 8.º da CEDH. A fotografia era acompanhada por um artigo que mencionava, entre outros assuntos, os problemas de saúde do Príncipe Rainier. O TEDH concluiu que os tribunais nacionais tinham conseguido conciliar o direito das editoras à liberdade de expressão com o direito dos requerentes ao respeito pela sua vida privada. A qualificação da doença do Príncipe Rainier como um acontecimento da sociedade contemporânea pelos tribunais nacionais não podia ser considerada desrazoável e o TEDH reconheceu que a fotografia, considerada no contexto do artigo, contribuía, pelo menos em certa medida, para um debate de interesse geral. O TEDH concluiu que não tinha havido uma violação do artigo 8.º da CEDH.

Na jurisprudência do TEDH, um dos critérios cruciais relativamente à conciliação destes direitos é o contributo da expressão em causa para um debate de interesse público geral.

Exemplo: No processo que deu origem ao acórdão *Mosley c. Reino Unido*,[30] um jornal semanal de circulação nacional publicou fotografias íntimas do requerente. Este alegou uma violação do artigo 8.º da CEDH porque não lhe tinha sido possível requerer uma medida cautelar antes da publicação das fotografias em causa devido à inexistência de qualquer obrigação de notificação prévia do jornal em caso de publicação de material suscetível de violar o direito à privacidade. Embora a divulgação do referido material se destinasse a fins de entretenimento e não a fins pedagógicos, beneficiava inquestionavelmente da proteção do artigo 10.º da CEDH, que poderia ser afastada pelos requisitos do artigo 8.º da CEDH nos casos em que as informações tivessem natureza íntima e privada e não existisse qualquer interesse público na sua divulgação. No entanto, era necessário exercer especial cuidado na apreciação de restrições que poderiam funcionar como uma espécie de censura antes da publicação. Relativamente ao efeito inibidor que uma obrigação de notificação prévia poderia produzir, às dúvidas quanto à sua eficácia e à ampla margem de apreciação naquela área, o TEDH entendeu que o artigo 8.º não exige o estabelecimento de uma obrigação de notificação prévia juridicamente vinculativa. Nesta conformidade, o TEDH concluiu que não tinha havido qualquer violação do artigo 8.º.

30 TEDH, acórdão *Mosley c. Reino Unido* de 10 de maio de 2011, petição n.º 48009/08, n.ºs 129 e 130.

Exemplo: No processo que deu origem ao acórdão *Biriuk c. Lituânia*,[31] a requerente pedia a condenação de um jornal diário no pagamento de uma indemnização por ter publicado um artigo em que revelava a sua seropositividade. Esta informação tinha sido alegadamente confirmada pelos médicos do hospital local. O TEDH não considerou que o artigo em causa contribuísse para qualquer debate de interesse geral e reiterou a importância fundamental da proteção dos dados pessoais, sobretudo de dados médicos, para que uma pessoa pudesse gozar o seu direito ao respeito pela vida privada e familiar garantido pelo artigo 8.º da CEDH. O TEDH atribuiu especial importância ao facto de, segundo o artigo publicado no jornal, o pessoal médico de um hospital ter fornecido informações sobre a infeção da requerente pelo VIH, violando manifestamente o seu dever de sigilo médico. Consequentemente, o Estado não tinha conseguido proteger o direito da requerente ao respeito pela sua vida privada. O TEDH concluiu que tinha havido uma violação do artigo 8.º.

1.2.2. Acesso aos documentos

Nos termos do artigo 11.º da Carta e do artigo 10.º da CEDH, a liberdade de informação abrange não só o direito a transmitir como também a *receber* informações. É cada vez mais reconhecida a importância da transparência do Estado para o funcionamento de uma sociedade democrática. Consequentemente, nas duas últimas décadas, o direito de acesso a documentos na posse de autoridades públicas foi reconhecido como um direito importante de todos os cidadãos da UE e de qualquer pessoa singular ou coletiva com residência ou sede num Estado-Membro.

No âmbito do **direito do CdE,** há que referir os princípios consagrados na Recomendação sobre o acesso a documentos oficiais, que serviu de inspiração aos autores da Convenção sobre o Acesso a Documentos Oficiais (*Convenção 205*).[32] No âmbito do **direito da UE**, o direito de acesso aos documentos é garantido pelo Regulamento n.º 1049/2001 relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão (*Regulamento Acesso a Documentos*).[33] O artigo 42.º da Carta e o artigo 15.º, n.º 3, do TFUE alargaram este direito de acesso

31 TEDH, acórdão *Biriuk c. Lituânia* de 25 de novembro de 2008, petição n.º 23373/03.

32 Conselho da Europa, Comité de Ministros (2002), *Recommendation Rec(2002)2 to member states on access to official documents* (Recomendação Rec(2002)2 aos Estados membros sobre o acesso a documentos oficiais), de 21 de fevereiro de 2002; Conselho da Europa, Convenção sobre o Acesso a Documentos Oficiais, de 18 de junho de 2009, STCE n.º 205. A Convenção ainda não entrou em vigor.

33 Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão, JO L 145, 2001 .

«aos documentos das instituições, órgãos e organismos da União, seja qual for o suporte desses documentos». Nos termos do artigo 52.º, n.º 2, da Carta, o direito de acesso aos documentos também é exercido de acordo com as condições e os limites previstos no artigo 15.º, n.º 3, do TFUE. Este direito poderá entrar em conflito com o direito à proteção de dados se o acesso aos documentos revelar dados pessoais de terceiros. Por conseguinte, os pedidos de acesso a documentos ou informações poderão ter de ser analisados à luz do direito à proteção de dados das pessoas cujos dados constam dos documentos solicitados.

Exemplo: No acórdão *Comissão/Bavarian Lager*,[34] o TJUE definiu o âmbito da proteção de dados pessoais no contexto do acesso aos documentos das instituições da UE e a relação entre os Regulamentos n.ºs 1049/2001 (*Regulamento Acesso aos Documentos*) e 45/2001 (*Regulamento Proteção de Dados*). A Bavarian Lager, constituída em 1992, importa cerveja alemã engarrafada para o Reino Unido, que se destina principalmente a consumo em *pubs* e bares. Porém, deparouse com algumas dificuldades porque a legislação britânica favorece, na prática, os produtores nacionais. Em resposta a uma queixa da Bavarian Lager, a Comissão Europeu decidiu instaurar uma ação contra o Reino Unido por incumprimento das suas obrigações, na sequência da qual as disposições controvertidas foram alteradas em conformidade com o direito da UE. A Bavarian Lager solicitou então à Comissão vários documentos, entre os quais uma cópia da ata de uma reunião na qual tinham participado representantes da Comissão, das autoridades britânicas e da *Confédération des Brasseurs du Marché Commun* (CBMC). A Comissão concordou em divulgar certos documentos relacionados com a reunião, mas truncou cinco nomes que constavam da ata, dado que duas pessoas se tinham expressamente oposto à divulgação da sua identidade e a Comissão não tinha conseguido contactar as outras três. Por decisão de 18 de março de 2004, a Comissão indeferiu um novo pedido de acesso à ata integral da reunião apresentado pela Bavarian Lager, com fundamento, em especial, na proteção da vida privada das pessoas em causa, tal como garantida pelo Regulamento Proteção de Dados. Insatisfeita com esta decisão, a Bavarian Lager instaurou uma ação no Tribunal de Primeira Instância, que anulou a decisão da Comissão por acórdão de 8 de novembro de 2007 (acórdão *Bavarian Lager/Comissão* no processo T-194/04), tendo concluído, em especial, que o simples facto de o nome da pessoa em causa figurar na lista dos participantes numa reunião em nome da entidade que essa pessoa representava

34 TJUE, acórdão de 29 de junho de 2010 no processo C-28/08 P, *Comissão Europeia/The Bavarian Lager Co. Ltd,* n.ºs 60, 63, 76, 78 e 79.

não comprometia a vida privada e não representava qualquer risco para a vida privada dessa pessoa.

Em sede de recurso interposto pela Comissão, o TJUE anulou o acórdão do Tribunal de Primeira Instância. O TJUE considerou que o Regulamento Acesso aos Documentos cria «um regime específico e reforçado de proteção de uma pessoa cujos dados pessoais poderiam, eventualmente, ser comunicados ao público». Segundo o TJUE, quando por meio de um pedido baseado no Regulamento Acesso aos Documentos se pretende obter o acesso a documentos que incluem dados pessoais, as disposições desse Regulamento passam a ser integralmente aplicáveis. O TJUE concluiu então que tinha sido com razão que a Comissão tinha indeferido o pedido de acesso à ata completa da reunião realizada em outubro de 1996. Na ausência do consentimento dos cinco participantes naquela reunião, a Comissão tinha dado cumprimento bastante ao seu dever de transparência ao divulgar uma versão do documento em causa do qual tinham sido expurgados os seus nomes.

Acresce que, segundo o TJUE, «[n]ão tendo a Bavarian Lager fornecido nenhuma justificação expressa e legítima nem nenhum argumento convincente demonstrativo da necessidade da transferência desses dados pessoais, a Comissão não pôde ponderar os diferentes interesses das partes em causa. Também não podia verificar se não existiam motivos para supor que os interesses legítimos das pessoas em causa podiam ser prejudicados», tal como exigido pelo Regulamento de Proteção de Dados.

De acordo com este acórdão, a ingerência no exercício do direito à proteção de dados relativamente ao acesso aos documentos exige uma justificação específica e legítima. O direito de acesso aos documentos não pode afastar automaticamente o direito à proteção de dados.[35]

No seguinte acórdão do TEDH, foi analisado um aspeto específico de um pedido de acesso.

35 Ver, contudo, as deliberações detalhadas em Autoridade Europeia para a Proteção de Dados (AEPD) (2011), *Public access to documents containing personal data after the* Bavarian Lager *ruling* (Acesso do público a documentos que contêm dados pessoais após o acórdão *Bavarian Lager*) Bruxelas, 24 de março de 2011, disponível em: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

Exemplo: No processo que deu origem ao acórdão *Társaság a Szabadságjogokért c. Hungria*,[36] a requerente, uma ONG de defesa dos direitos humanos, tinha pedido ao Tribunal Constitucional acesso a informações sobre um processo pendente. Sem consultar o membro do Parlamento que tinha instaurado o processo, o Tribunal Constitucional indeferiu o pedido de acesso, alegando que a divulgação a terceiros de informações sobre as queixas que lhe eram submetidas dependia de autorização do autor da queixa. Os tribunais nacionais confirmaram este indeferimento, alegando que a proteção dos dados pessoais em causa não podia ser afastada por outros interesses legítimos, incluindo a acessibilidade a informações públicas. A requerente tinha agido como um «fiscal» social, cujas atividades mereciam uma proteção semelhante à conferida aos órgãos de comunicação social. Relativamente à liberdade de imprensa, o TEDH tinha afirmado sistematicamente que o público tinha o direito a receber informações de interesse geral. As informações pretendidas pela requerente estavam «imediatamente disponíveis», pelo que não era necessário proceder à recolha de dados. Assim sendo, o Estado tinha a obrigação de não impedir o fluxo de informações pretendido pela requerente. Em resumo, o TEDH considerou que os obstáculos destinados a dificultar o acesso a informações de interesse público poderiam desencorajar aqueles que trabalham na área da comunicação social ou em áreas conexas de desempenhar o seu papel crucial de «fiscal» público. O TEDH concluiu que tinha havido uma violação do artigo 10.º.

No direito da UE, a importância da transparência é inquestionável. O princípio da transparência está consagrado nos artigos 1.º e 10.º do Tratado UE e no artigo 15.º, n.º 1, do TFUE. [37] Segundo o considerando 2 do Regulamento (CE) n.º 1049/2001, permite assegurar uma melhor participação dos cidadãos no processo de decisão e garantir uma maior legitimidade, eficácia e responsabilidade da Administração perante os cidadãos num sistema democrático.[38]

Seguindo este raciocínio, o Regulamento (CE) n.º 1290/2005 do Conselho relativo ao financiamento da política agrícola comum e o Regulamento (CE) n.º 259/2008 da Comissão que estabelece as regras da sua execução exigem a publicação de informações sobre os beneficiários de certos fundos da UE no setor agrícola e os

36 TEDH, acórdão *Társaság a Szabadságjogokért c. Hungria* de 14 de abril de 2009, petição n.º 37374/05, n.ºs 27, 3638.

37 UE (2012), Versões consolidadas do Tratado da União Europeia e do TFUE, JO 2012 C 326.

38 TJUE, acórdão de 6 de março de 2003 no processo C-41/00 P, *Interporc Im- und Export GmbH/Comissão das Comunidades Europeias*, n.º 39; e TJUE, acórdão de 29 de junho de 2010 no processo C-28/08 P, *Comissão Europeia/The Bavarian Lager Co. Ltd.*, n.º 54.

montantes recebidos por cada beneficiário.[39] Esta publicação deverá contribuir para o controlo público da utilização de fundos públicos pela Administração. A proporcionalidade desta publicação foi contestada por vários beneficiários.

Exemplo: No processo que deu origem ao acórdão *Volker und Markus Schecke e Hartmut Eifert/Land Hessen*,[40] o TJUE foi chamado a pronunciarse sobre a proporcionalidade da publicação, exigida pela legislação da União, dos nomes dos beneficiários de subsídios agrícolas da UE e dos montantes por eles recebidos.

O Tribunal de Justiça, salientando que o direito à proteção de dados não é uma prerrogativa absoluta, considerou que a publicação num sítio Internet de dados nominativos relativos aos beneficiários de dois fundos agrícolas da UE e dos montantes exatos que receberam constitui uma ingerência na sua vida privada e, em especial, na proteção dos seus dados pessoais.

O Tribunal de Justiça considerou que tal ingerência nos direitos consagrados nos artigos 7.º e 8.º da Carta estava prevista na lei e prosseguia um objetivo de interesse geral reconhecido pela UE, ou seja, aumentar a transparência da utilização dos fundos comunitários. Contudo, o TJUE entendeu que a publicação dos nomes das pessoas singulares que beneficiavam de ajudas agrícolas da UE provenientes destes dois fundos e os montantes exatos que receberam constituía uma medida desproporcional e não se justificava à luz do artigo 52.º, n.º 1, da Carta. Por conseguinte, o Tribunal de Justiça declarou a invalidade parcial da legislação da UE relativa à publicação de informação sobre os beneficiários de fundos agrícolas europeus.

1.2.3. Liberdade das artes e das ciências

Outro direito que é necessário conciliar com o direito ao respeito pela vida privada e à proteção de dados é a liberdade das artes e das ciências, expressamente protegida pelo artigo 13.º da Carta. Este direito é, antes de mais, um corolário do direito à

39 Regulamento (CE) n.º 1290/2005 do Conselho, de 21 de junho de 2005, relativo ao financiamento da política agrícola comum, JO 2005 L 209; e Regulamento (CE) n.º 259/2008 da Comissão, de 18 de março de 2008, que estabelece as regras de execução do Regulamento (CE) n.º 1290/2005 do Conselho no que respeita à publicação de informação sobre os beneficiários de fundos provenientes do Fundo Europeu Agrícola de Garantia (FEAGA) e do Fundo Europeu Agrícola de Desenvolvimento Rural (Feader), JO 2008 L 76.

40 TJUE, acórdão de 9 de novembro de 2010 nos processos apensos C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen*, n.ºs 47–52, 58, 66–67, 75, 86 e 92.

liberdade de pensamento e de expressão e deve ser exercido à luz do disposto no artigo 1.º da Carta (Dignidade do ser humano). O TEDH considera que a liberdade das artes está protegida pelo artigo 10.º da CEDH.[41] O direito garantido pelo artigo 13.º da Carta também poderá estar sujeito às restrições permitidas pelo artigo 10.º da CEDH.[42]

Exemplo: No processo que deu origem ao acórdão *Vereinigung bildender Künstler c. Áustria*,[43] os tribunais austríacos proibiram a associação requerente de continuar a exibir um quadro que continha fotografias das cabeças de várias figuras públicas em posições sexuais. Um deputado austríaco, cuja fotografia tinha sido utilizada no quadro, instaurou uma ação contra a associação requerente, pedindo que esta fosse proibida de exibir o quadro. O tribunal nacional deu provimento a este pedido. O TEDH reiterou que o artigo 10.º da CEDH era aplicável à transmissão de ideias que ofendessem, chocassem ou perturbassem o Estado ou qualquer segmento da população. Aqueles que criavam, executavam, distribuíam ou exibiam obras de arte contribuíam para o intercâmbio de ideias e opiniões e o Estado tinha a obrigação de não restringir injustificadamente a sua liberdade de expressão. Uma vez que o quadro era uma *collage* e utilizava fotografias apenas da cabeça das pessoas, sendo os corpos representados de forma irrealista e exagerada, que obviamente não pretendia refletir nem mesmo aludir à realidade, o TEDH afirmou igualmente que o quadro não poderia ser considerado uma representação de aspetos da vida privada da pessoa em causa, mas apenas de aspetos relacionados com a sua imagem pública como político e que, nessa qualidade, a pessoa representada no quadro tinha de mostrar maior tolerância às críticas. Após ponderação dos diferentes interesses em causa, o TEDH considerou que a proibição absoluta da continuação da exibição do quadro era desproporcionada. O TEDH concluiu que tinha havido uma violação do artigo 10.º da CEDH.

No que respeita às ciências, a legislação europeia sobre proteção de dados reconhece o valor especial da ciência para a sociedade. Por este motivo, as restrições gerais à utilização de dados pessoais são menos rigorosas. Tanto a Diretiva de Proteção de Dados como a Convenção 108 permitem a conservação de dados para fins de investigação científica quando já não sejam necessários para o fim para o qual

41 TEDH, acórdão *Müller e outros c. Suíça* de 24 de maio de 1988, petição n.º 10737/84.

42 Anotações relativas à Carta dos Direitos Fundamentais, JO 2007 C 303.

43 TEDH, acórdão *Vereinigung bildender Künstler c. Áustria*, de 25 de janeiro de 2007, petição n.º 68345/01; ver, em especial, n.ºs 26 e 34.

foram inicialmente recolhidos. Além disso, a utilização posterior de dados pessoais para fins de investigação científica não será considerada uma finalidade incompatível. Cabe ao legislador nacional estabelecer disposições mais detalhadas, incluindo as garantias necessárias, para conciliar o interesse na investigação científica com o direito à proteção de dados (ver também as secções 3.3.3 e 8.4).

1.2.4. Proteção da propriedade

O direito à proteção da propriedade está consagrado no artigo 1.º do Primeiro Protocolo à CEDH e também no artigo 17.º, n.º 1, da Carta. Um aspeto importante do direito de propriedade é a proteção da propriedade intelectual, expressamente mencionada no artigo 17.º, n.º 2, da Carta. Existem várias diretivas na ordem jurídica da UE que visam a proteção efetiva da propriedade intelectual, em especial dos direitos de autor. A propriedade intelectual abrange não apenas a propriedade literária e artística como também direitos sobre patentes, marcas e direitos conexos.

Tal como deixa bem claro a jurisprudência do TJUE, a proteção do direito fundamental à propriedade privada tem de ser conciliado com a proteção de outros direitos fundamentais, especialmente com o direito à proteção de dados.[44] Há casos em que as instituições responsáveis pela proteção dos direitos de autor exigiram que os prestadores de serviços de Internet divulgassem a identidade dos utilizadores de plataformas de partilha de ficheiros. Muitas vezes, essas plataformas permitem aos utilizadores da Internet descarregar gratuitamente temas musicais que estão protegidos pelo direito de autor.

Exemplo: O processo que deu origem ao acórdão *Promusicae/Telefónica de España*[45] dizia respeito à recusa de um prestador de serviços de acesso à Internet, a Telefónica, em divulgar à Promusicae, uma associação sem fins lucrativos que agrupa produtores musicais e editores de gravações musicais e audiovisuais, os dados pessoais de certas pessoas a quem prestava serviços de acesso à Internet. A Promusicae pretendia obter as referidas informações para assim poder mover uma ação cível contra aquelas pessoas, que alegadamente utilizavam um programa de troca de ficheiros que permitia o acesso a fonogramas cujos direitos de exploração pertenciam a membros da associação.

44 TEDH, acórdão *Ashby Donald e outros c. França* de 10 de janeiro de 2013, petição n.º 36769/08.

45 TJUE, acórdão de 29 de janeiro de 2008 no processo C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU,* n.ºs 54 e 60.

O tribunal espanhol apresentou um pedido de decisão prejudicial ao TJUE, perguntando se a legislação comunitária estabelece a obrigação de comunicar esses dados pessoais no contexto de uma ação cível para garantir a efetiva proteção dos direitos de autor. O referido tribunal invocou as Diretivas 2000/31, 2001/29 e 2004/48, lidas à luz dos artigos 17.º e 47.º da Carta. O Tribunal de Justiça concluiu que estas três Diretivas, assim como a Diretiva relativa à privacidade e às comunicações eletrónicas (Diretiva 2002/58), não se opõem a que os Estados-Membros estabeleçam a obrigação de divulgar dados pessoais no contexto de uma ação cível para garantir a efetiva proteção dos direitos de autor.

O TJUE sublinhou que, consequentemente, o caso suscitava a questão da necessidade de conciliar as exigências ligadas à proteção de diferentes direitos fundamentais, nomeadamente o direito ao respeito pela vida privada, por um lado, e os direitos à proteção da propriedade e a uma tutela jurisdicional efetiva, por outro.

O Tribunal de Justiça concluiu que «o direito comunitário exige que os [Estados-Membros], na transposição das diretivas supramencionadas, zelem por que seja seguida uma interpretação das mesmas que permita assegurar o justo equilíbrio entre os direitos fundamentais protegidos pela ordem jurídica comunitária. Seguidamente, na execução das medidas de transposição dessas diretivas, compete às autoridades e aos órgãos jurisdicionais dos Estados-Membros não só interpretar o seu direito nacional em conformidade com essas mesmas diretivas mas também seguir uma interpretação destas que não entre em conflito com os referidos direitos fundamentais ou com os outros princípios gerais do direito comunitário, como o princípio da proporcionalidade.»[46]

46 *Ibid.*, n.ºs 65 e 68; ver também TJUE, acórdão de 16 de fevereiro de 2012 no processo C-360/10, *SABAM/Netlog N.V.*

2

Terminologia sobre proteção de dados

UE	Questões abrangidas	CdE
Dados pessoais		
Diretiva de Proteção de Dados, artigo 2.º, al. a) TJUE, acórdão de 9 de novembro de 2010 nos processos apensos C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen* TJUE, acórdão de 29 de janeiro de 2008 no processo C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*	**Definição legal**	Convenção 108, artigo 2.º, al. a) TEDH, acórdão *Bernh Larsen Holding AS e outros c. Noruega* de 14 de março de 2013, petição n.º 24117/08
Diretiva de Proteção de Dados, artigo 8.º, n.º 1 TJUE, acórdão de 6 de novembro de 2003 no processo C-101/01, *Bodil Lindqvist*	**Categorias específicas de dados pessoais (dados sensíveis)**	Convenção 108, artigo 6.º
Diretiva de Proteção de Dados, artigo 6.º, n.º 1, al. e)	**Dados anonimizados e pseudonimizados**	Convenção 108, artigo 5.º, al. e) Convenção 108, Relatório explicativo, artigo 42.º
Tratamento de dados		
Diretiva de Proteção de Dados, artigo 2.º, al. b) TJUE, acórdão de 6 de novembro de 2003 no processo C-101/01, *Bodil Lindqvist*	**Definições**	Convenção 108, artigo 2.º, al. c)

UE	Questões abrangidas	CdE
Utilizadores dos dados		
Diretiva de Proteção de Dados, artigo 2.º, al. d)	**Responsável pelo tratamento**	Convenção 108, artigo 2.º, al. d) Recomendação sobre a definição de perfis, artigo 1.º, al. g) *
Diretiva de Proteção de Dados, artigo 2.º, al. e) TJUE, acórdão de 6 de novembro de 2003 no processo C-101/01, *Bodil Lindqvist*	**Subcontratante**	Recomendação sobre a definição de perfis, artigo 1.º, al. h)
Diretiva de Proteção de Dados, artigo 2.º, al. g)	**Destinatário**	Convenção 108, Protocolo Adicional, artigo 2.º, n.º 1
Diretiva de Proteção de Dados, artigo 2.º, al. f)	**Terceiro**	
Consentimento		
Diretiva de Proteção de Dados, artigo 2.º, al. h) TJUE, acórdão de 5 de maio de 2011 no processo C-543/09, *Deutsche Telekom AG/ Bundesrepublik Deutschland*	**Definição e requisitos de validade do consentimento**	Recomendação sobre os dados médicos, artigo 6.º, e várias recomendações posteriores

*Nota: *Conselho da Europa, Comité de Ministros (2010), Recomendação Rec(2010)13 aos Estados membros sobre a proteção das pessoas singulares relativamente ao tratamento automatizado de dados de caráter pessoal no contexto da definição de perfis (Recomendação sobre a definição de perfis), 23 de novembro de 2010.*

2.1. Dados pessoais

Pontos-chave

- Consideramse dados pessoais os dados relativos a uma pessoa identificada ou, pelo menos, identificável: o titular dos dados ou a pessoa em causa
- Considerase que uma pessoa é identificável se for possível obter informações adicionais, sem um esforço desproporcionado, que permitam a identificação do titular dos dados.
- A autenticação consiste no ato de provar que uma certa pessoa possui uma certa identidade e/ou está autorizada a realizar certas atividades.

- Existem categorias específicas de dados (os chamados «dados sensíveis»), elencados na Convenção 108 e na Diretiva de Proteção de Dados, os quais exigem uma proteção acrescida e, como tal, estão sujeitos a um regime jurídico especial.
- Considerase que os dados foram anonimizados se já não contiverem quaisquer elementos de identificação; consideramse "pseudonimizados" se os elementos de identificação estiverem encriptados.
- Contrariamente ao que acontece com os dados anonimizados, os dados "pseudonimizados" são dados pessoais.

2.1.1. Principais aspetos do conceito de dados pessoais

No direito da UE, assim como **no direito do CdE**, o termo «dados pessoais» é definido como informações relativas a uma pessoa singular identificada ou identificável,[47] ou seja, informações sobre uma pessoa cuja identidade é evidente ou que pode, pelo menos, ser determinada através da obtenção de informações adicionais.

Se forem tratados dados sobre essa pessoa, esta é designada «titular dos dados».

Uma pessoa

O direito à proteção de dados nasceu do direito ao respeito pela vida privada. O conceito de vida privada está associado aos seres humanos. As pessoas singulares são, portanto, as principais beneficiárias da proteção de dados. Além disso, segundo o Parecer do Grupo de Trabalho do artigo 29.º, apenas as *pessoas vivas* estão protegidas pela legislação europeia sobre proteção de dados.[48]

A jurisprudência do TEDH relativa ao artigo 8.º da CEDH ilustra a dificuldade em separar completamente assuntos da vida privada e da vida profissional.[49]

47 Diretiva Proteção de Dados, artigo 2.º, al. a); Convenção 108, artigo 2.º, alínea a).

48 Grupo de Trabalho do artigo 29.º (2007), Parecer 4/2007 sobre o conceito de dados pessoais, WP 136, 20 de junho de 2007, p. 23.

49 Ver, por exemplo, TEDH, acórdão *Rotaru c. Roménia* [GS] de 4 de maio de 2000, n.º 43, petição n.º 28341/95; TEDH, acórdão *Niemitz c. Alemanha*, de 16 de dezembro de 1992, n.º 29, petição n.º 13710/88.

Exemplo: No processo que deu origem ao acórdão *Amann c. Suíça*,[50] as autoridades intercetaram uma chamada telefónica de natureza profissional para o requerente. Com base nessa chamada telefónica, as autoridades lançaram uma investigação sobre o requerente e submeteram uma ficha sobre o mesmo, destinada ao registo de fichas de segurança. Embora a interceção respeitasse a uma chamada telefónica de natureza profissional, o TEDH considerou que o armazenamento de dados sobre esta chamada estava relacionado com a vida privada do requerente, tendo sublinhado que o termo «vida privada» não podia ser objeto de uma interpretação restritiva, sobretudo porque o respeito pela vida privada abrangia o direito de estabelecer e desenvolver relações com outros seres humanos. Além disso, não existia qualquer razão de princípio que justificasse a exclusão de atividades de natureza profissional ou comercial do conceito de «vida privada». Esta interpretação mais ampla do conceito correspondia à da Convenção 108. O TEDH considerou ainda que, no caso do requerente, a ingerência das autoridades não estava em conformidade com a lei dado que a legislação nacional não estabelecia disposições específicas e detalhadas sobre a recolha, gravação e armazenamento de informações. Por conseguinte, concluiu que tinha havido uma violação do artigo 8.º da CEDH.

Além disso, se a vida profissional também pode ser objeto da proteção de dados, é questionável que apenas as pessoas singulares possam beneficiar dessa proteção. Os direitos garantidos pela CEDH não respeitam apenas às pessoas singulares.

Existe jurisprudência do TEDH em que este se pronunciou sobre alegados casos de violação do direito de pessoas coletivas a proteção contra a utilização dos seus dados nos termos do artigo 8.º da CEDH. Porém, o TEDH apreciou os factos à luz do direito ao respeito pelo domicílio e pela correspondência e não ao respeito pela vida privada.

Exemplo: O processo que deu origem ao acórdão *Bernh Larsen Holding AS e outros c. Noruega*[51] dizia respeito a uma queixa apresentada por três empresas norueguesas relativa a uma decisão das autoridades fiscais ordenando que estas fornecessem aos inspetores fiscais uma cópia de todos os dados armazenados num servidor utilizado em conjunto pelas três empresas.

50 TEDH, acórdão *Amann c. Suíça* [GS] de 16 de fevereiro de 2000, n.º 65, petição n.º 27798/95.

51 TEDH, acórdão *Bernh Larsen Holding AS e outros c. Noruega* de 14 de março de 2013, petição n.º 24117/08. Ver também, porém, TEDH, acórdão *Liberty e outros c. Reino Unido* de 1 de julho de 2008, petição n.º 58243/00.

O TEDH concluiu que a imposição de tal obrigação sobre as empresas requerentes constituía uma ingerência no exercício dos seus direitos ao respeito pelo «domicílio» e pela «correspondência». Contudo, o TEDH entendeu que as autoridades fiscais tinham implementado garantias eficazes e adequadas contra abusos: as empresas requerentes tinham sido notificadas com grande antecedência, estavam presentes e tiveram a oportunidade de se pronunciar durante a diligência no local e o material deveria ser destruído quando a inspeção fiscal estivesse concluída. Neste caso, tinha sido alcançado um equilíbrio justo entre o direito das empresas requerentes ao respeito pelo «domicílio» e pela «correspondência» e o seu interesse em proteger a privacidade das pessoas que trabalhavam para elas, por um lado, e o interesse público em assegurar uma inspeção eficiente para efeitos de liquidação do imposto, por outro. O TEDH concluiu que tinha havido, assim, uma violação do artigo 8.º.

De acordo com a Convenção 108, a proteção de dados respeita, em primeira linha, à proteção das pessoas singulares; no entanto, as Partes Contratantes podem alargar essa proteção a pessoas coletivas, tais como sociedades comerciais e associações, no seu direito interno. **A legislação da UE sobre proteção de dados** não abrange, de um modo geral, a proteção de pessoas coletivas relativamente ao tratamento de dados que lhes digam respeito. Esta matéria pode ser regulada pelas autoridades nacionais competentes.[52]

Exemplo: No acórdão *Volker und Markus Schecke e Hartmut Eifert/Land Hessen*,[53] o TJUE, reportandose à publicação de dados pessoais relativos aos beneficiários de ajudas agrícolas, entendeu que «as pessoas coletivas só podem invocar a proteção dos artigos 7.º e 8.º da Carta a respeito de tal identificação desde que a denominação legal da pessoa coletiva identifique uma ou mais pessoas singulares. [...O] respeito pelo direito à vida privada (*sic*) relativamente ao tratamento de dados pessoais, reconhecido pelos artigos 7.º e 8.º da Carta, abrange todas as informações relativas a qualquer pessoa singular identificada ou identificável [...]».[54]

52 Diretiva Proteção de Dados, considerando 24.

53 TJUE, acórdão de 9 de novembro de 2010 nos processos apensos C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen*, n.º 53.

54 *Ibid*. n.º 52.

Identificabilidade de uma pessoa

Nos termos do direito da UE, bem como **nos termos do direito do CdE**, considera-se que as informações contêm dados sobre uma pessoa se:

- essa pessoa estiver identificada nessas informações; ou
- essa pessoa, embora não esteja identificada, estiver descrita nestas informações de forma que permita descobrir quem é a pessoa em causa efetuando pesquisas adicionais.

Ambos os tipos de informações são protegidos da mesma forma na legislação europeia sobre proteção de dados. O TEDH tem afirmado repetidamente que o conceito de «dados pessoais» é o mesmo na CEDH e na Convenção 108, especialmente no que respeita à exigência de serem relativos a pessoas singulares identificadas ou identificáveis.[55]

As definições legais de dados pessoais não esclarecem em que casos se considera que uma pessoa está identificada.[56] Evidentemente, a identificação exige elementos que descrevam uma pessoa de forma a distinguila de todas as outras e de a tornar reconhecível enquanto indivíduo. O nome de uma pessoa é um exemplo perfeito desse tipo de elementos descritivos. Em casos excecionais, outros elementos de identificação poderão produzir o mesmo efeito que um nome. Por exemplo, no caso das figuras públicas, poderá ser suficiente mencionar o cargo da pessoa (por ex., Presidente da Comissão Europeia).

Exemplo: No acórdão *Promusicae*,[57] o TJUE afirmou que «é pacífico que a transmissão, pedida pela Promusicae, dos nomes e endereços de determinados utilizadores de [uma certa plataforma de partilha de ficheiros na Internet] implica a disponibilização de dados pessoais, isto é, de informações sobre pessoas singulares identificadas ou identificáveis, de acordo com a definição constante do artigo 2.º, alínea a), da Diretiva 95/46 [...]. Essa transmissão de informações, que, segundo a Promusicae, são armazenadas pela Telefónica – o que a mesma

55 Ver TEDH, acórdão *Amann c. Suíça* [GS] de 16 de fevereiro de 2000, n.º 65 *et al.*, petição n.º 27798/95.

56 Ver também TEDH, acórdão *Odièvre c. França* [GS] de 13 de fevereiro de 2003, petição n.º 42326/98; e TEDH, acórdão *Godelli c. Itália* de 25 de Setembro de 2012, petição n.º 33783/09.

57 TJUE, acórdão de 29 de janeiro de 2008 no processo C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU,* n.º 45.

não contesta , constitui um tratamento de dados pessoais, na aceção do artigo 2.º, primeiro parágrafo, da Diretiva 2002/58, em conjugação com o artigo 2.º, alínea b), da Diretiva 95/46».

Uma vez que muitos nomes não são únicos, a determinação da identidade de uma pessoa poderá exigir outros elementos de identificação para garantir que uma pessoa não seja confundida com outra. Muitas vezes são utilizadas informações como a data e o local de nascimento. Em alguns países, foram também estabelecidos números personalizados para distinguir melhor os cidadãos entre si. Os dados biométricos, como as impressões digitais, as fotografias digitais ou o reconhecimento da íris, estão a tornarse cada vez mais importantes para identificar as pessoas na era tecnológica.

Para a aplicabilidade da legislação europeia sobre proteção de dados, porém, não é necessária uma identificação de alta qualidade da pessoa em causa, bastando que esta seja identificável. Uma pessoa é considerada identificável se uma informação contiver elementos de identificação que permitam identificar essa pessoa, direta ou indiretamente.[58] Segundo o considerando 26 da Diretiva de Proteção de Dados, o critério é a probabilidade de utilizadores previsíveis das informações (incluindo terceiros destinatários) terem ao seu dispor e aplicarem meios razoáveis de identificação (ver secção 2.3.2).

Exemplo: Uma autoridade local decide recolher dados sobre os veículos que ultrapassam o limite de velocidade nas ruas daquela localidade. Para tal, fotografa os veículos, registando automaticamente a hora e o local, a fim de transmitir os dados à autoridade competente para que esta possa aplicar multas àqueles que violaram os limites de velocidade. Uma das pessoas em causa apresenta uma queixa, alegando que nenhuma disposição da legislação sobre proteção de dados habilita a autoridade local a recolher esses dados. A autoridade local entende que não está a recolher dados pessoais, afirmando que as matrículas são dados sobre pessoas anónimas. A autoridade local não tem competência para consultar o registo automóvel geral para saber a identidade do proprietário ou condutor do veículo.

Este argumento é incompatível com o disposto no considerando 26 da Diretiva de Proteção de Dados. Uma vez que a finalidade da recolha dos dados é

58 Diretiva Proteção de Dados, artigo 2.º, al. a).

claramente identificar e multar aqueles que ultrapassam os limites de velocidade, é previsível que se tente proceder àquela identificação. Embora as autoridades locais não tenham diretamente ao seu dispor meios de identificação, os dados serão transmitidos à autoridade competente – a polícia – que possui tais meios. O considerando 26 também prevê expressamente um cenário em que é previsível que outros destinatários dos dados, para além do utilizador imediato, possam tentar identificar a pessoa. À luz do considerando 26, os atos da autoridade local equivalem à recolha de dados sobre pessoas identificáveis e, como tal, necessitam de uma base legal ao abrigo da legislação sobre proteção de dados.

No **direito do CdE**, a identificabilidade é entendida de modo semelhante. O artigo 1.º, n.º 2, da Recomendação sobre os dados de pagamento,[59] por exemplo, estabelece que uma pessoa não será considerada «identificável» se a identificação implicar um esforço desrazoável a nível de tempo, custos ou trabalho.

Autenticação

A autenticação é o procedimento através do qual uma pessoa pode provar que possui uma certa identidade e/ou está autorizada a praticar certos atos, tais como movimentar uma conta bancária ou entrar numa área de acesso reservado. A autenticação pode ser efetuada através da comparação de dados biométricos, tais como a fotografia ou as impressões digitais constantes do passaporte, com os dados da pessoa que se apresenta, por exemplo, nos serviços de controlo da imigração; de perguntas cuja resposta só deveria ser conhecida da pessoa com uma certa identidade ou autorização, tais como o número de identificação pessoal (PIN) ou a palavrapasse; ou exigindo a apresentação de um determinado objeto que deveria estar exclusivamente na posse da pessoa com uma certa identidade ou autorização, tais como um cartão com chip especial ou a chave de um cofre bancário. Para além das palavraspasse e dos cartões com chip, por vezes em conjunto com PIN, as assinaturas eletrónicas são um instrumento particularmente eficaz para a identificação e autenticação de uma pessoa nas comunicações eletrónicas.

59 CdE, Comité de Ministros (1990), *Recommendation No. R Rec(90) 19 on the protection of personal data used for payment and other related operations* (Recomendação n.º R Rec(90) 19 sobre a proteção de dados pessoais utilizados para fins de pagamento e outras operações conexas), de 13 de Setembro de 1990.

Natureza dos dados

Qualquer tipo de informação pode ser considerado dados pessoais desde que seja relativa a uma pessoa.

Exemplo: A avaliação do desempenho profissional de um funcionário realizada pelo superior hierárquico e guardada no respetivo processo individual constitui dados pessoais sobre o funcionário, ainda que traduza apenas, no todo ou em parte, a opinião pessoal desse superior hierárquico, como, por ex., «o funcionário não é dedicado ao seu trabalho» e não factos objetivos, como, por ex., «o funcionário esteve ausente ao serviço durante cinco semanas nos últimos seis meses».

Os dados pessoais abrangem as informações respeitantes à vida privada de uma pessoa, bem como informações sobre a sua vida profissional ou pública.

No acórdão *Amann*,[60] o TEDH considerou que o termo «dados pessoais» não abrangia apenas assuntos da esfera privada de uma pessoa (ver secção 2.1.1). Esta interpretação do termo «dados pessoais» também é relevante para a Diretiva de Proteção de Dados:

Exemplo: No acórdão *Volker und Markus Schecke e Hartmut Eifert/Land Hessen*,[61] o TJUE afirmou que «[a] este respeito, é irrelevante que os dados publicados sejam relativos a atividades profissionais [...]. O Tribunal Europeu dos Direitos do Homem declarou, a este propósito, relativamente à interpretação do artigo 8.º da CEDH, que a expressão "vida privada" não devia ser interpretada de forma restritiva e que nenhuma razão de princípio permite excluir as atividades profissionais ... do conceito de vida privada».

Os dados também são relativos a pessoas se o teor da informação revelar indiretamente dados sobre uma pessoa. Em alguns casos, quando existe uma estreita ligação entre um objeto ou acontecimento – por ex., um telemóvel, um automóvel, um acidente – por um lado, e uma pessoa – por ex., o seu proprietário, utilizador, vítima

60 Ver TEDH, acórdão *Amann c.a Suíça* de 16 de fevereiro de 2000, n.º 65, petição n.º 27798/95.

61 Acórdão de 9 de novembro de 2010 nos processos apensos C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen*, n.º 59.

– por outro, as informações sobre um objeto ou sobre um acontecimento também deveriam ser consideradas dados pessoais.

> Exemplo: No processo que deu origem ao acórdão *Uzun c. Alemanha*,[62] o requerente e outro homem foram colocados sob vigilância através de um dispositivo GPS (sistema de posicionamento global) montado no veículo do outro homem devido à suspeita de envolvimento num ataque bombista. Neste caso, o TEDH entendeu que a observação do requerente através de GPS correspondia a uma ingerência na sua vida privada, tal como protegida pelo artigo 8.º da CEDH. No entanto, a vigilância por GPS tinha sido efetuada em conformidade com a lei e era proporcional ao objetivo legítimo de investigar vários casos de tentativa de homicídio e, por conseguinte, era necessária numa sociedade democrática. O TEDH concluiu que não tinha havido uma violação do artigo 8.º da CEDH.

Suporte dos dados

O suporte onde os dados pessoais são armazenados ou utilizados não é relevante para a aplicabilidade da legislação sobre proteção de dados. As comunicações escritas ou orais podem conter dados pessoais, assim como imagens,[63] incluindo imagens[64] ou som[65] captados por sistemas de circuito fechado de televisão (CCTV). As informações registadas eletronicamente, bem como as informações em suporte de papel, podem ser dados pessoais; até mesmo as amostras de tecido humano podem conter dados pessoais, na medida em que registam o ADN de uma pessoa.

2.1.2. Categorias específicas de dados pessoais

No **direito da UE**, bem como no **direito do CdE**, existem categorias específicas de dados pessoais que, por natureza, poderão representar um risco para as pessoas em causa quando são tratados, pelo que exigem uma proteção reforçada. Por conseguinte, o tratamento destas categorias específicas de dados («dados sensíveis») só poderá ser permitido se tiverem sido implementadas garantias específicas.

62 TEDH, acórdão *Uzun c. Alemanha* de 2 de setembro de 2010, petição n.º 35623/05.

63 TEDH, acórdão *Von Hannover c. Alemanha* de 24 de junho de 2004, petição n.º 59320/00; TEDH, acórdão *Sciacca c. Itália* de 11 de janeiro de 2005, petição n.º 50774/99.

64 TEDH, acórdão *Peck c. Reino Unido* de 28 de janeiro de 2003, petição n.º 44647/98; TEDH, acórdão *Köpke c. Alemanha* de 5 de outubro de 2010, petição n.º 420/07.

65 Diretiva Proteção de Dados, considerandos 16 e 17; TEDH, acórdão *P.G. e J.H. c. Reino Unido* de 25 de Setembro de 2001, petição n.º 44787/98, n.ºs 59 e 60; TEDH, acórdão *Wisse c. França* de 20 de dezembro de 2005, petição n.º 71611/01.

Quanto à definição de dados sensíveis, tanto a Convenção 108 (artigo 6.º) como a Diretiva de Proteção de Dados (artigo 8.º) identificam as seguintes categorias:

- dados pessoais que revelem a origem racial ou étnica;
- dados pessoais que revelem as opiniões políticas, as convicções religiosas ou outras; e
- dados relativos à saúde e à vida sexual.

> Exemplo: No acórdão *Bodil Lindqvist*,[66] o TJUE afirmou que «a indicação do facto de uma pessoa se ter lesionado num pé e estar com baixa por doença a meio tempo constitui um dado de caráter pessoal relativo à saúde na aceção do artigo 8.º, n.º 1, da Diretiva 95/46.»

A Diretiva de Proteção de Dados qualifica também os dados relativos à filiação sindical como dados sensíveis, já que esta informação pode ser um bom indicador da filiação ou das convicções políticas.

A Convenção 108 também considera sensíveis os dados pessoais relativos a condenações penais.

O artigo 8.º, n.º 7, da Diretiva de Proteção de Dados encarrega os Estados-Membros da UE de «determinar as condições em que um número nacional de identificação ou qualquer outro elemento de identificação de aplicação geral poderá ser objeto de tratamento.»

2.1.3. Dados anonimizados e pseudonimizados

De acordo com o princípio da limitação da conservação dos dados consagrado na Diretiva de Proteção de Dados e na Convenção 108 (e desenvolvido no capítulo 3), os dados têm de ser conservados «de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente.»[67] Consequentemente, se o responsável pelo tratamento pretendesse armazenar os dados depois

66 TJUE, acórdão de 6 de novembro de 2003 no processo C-101/01, *Bodil Lindqvist*, n.º 51.

67 Diretiva Proteção de Dados, artigo 6.º, n.º 1, al. e); Convenção 108, artigo 5.º, al. e).

de estarem desatualizados ou de terem deixado de servir a sua finalidade inicial, teria de os anonimizar.

Dados anonimizados

Os dados consideramse anonimizados se todos os elementos de identificação tiverem sido eliminados de um conjunto de dados pessoais. Não pode ser deixado nas informações nenhum elemento que possa servir, exercendo um esforço razoável, para reidentificar a(s) pessoa(s) em questão.[68] Quando os dados são eficazmente anonimizados, deixam de ser dados pessoais.

Se os dados pessoais deixarem de servir a sua finalidade inicial, a Diretiva de Proteção de Dados e a Convenção 108 permitem que estes sejam conservados sem anonimização para fins históricos, estatísticos ou científicos, desde que sejam aplicadas garantias adequadas contra a sua utilização abusiva.[69]

Dados pseudonimizados

As informações pessoais contêm elementos de identificação, tais como o nome, a data de nascimento, o sexo e a morada. Quando as informações pessoais são pseudonimizadas, os elementos de identificação são substituídos por um pseudónimo. A pseudonimização é realizada, por exemplo, através da encriptação dos elementos de identificação constantes dos dados pessoais.

As definições legais da Convenção 108 e da Diretiva de Proteção de Dados não mencionam expressamente os dados pseudonimizados. No entanto, o Relatório Explicativo da Convenção 108 refere, no seu artigo 42.º, que o requisito relativo ao prazo máximo de armazenamento dos dados na sua forma nominativa não significa que, passado algum tempo, esses dados devem ser irrevogavelmente separados do nome da pessoa a quem dizem respeito, mas apenas que não deverá ser fácil estabelecer a ligação entre os dados e os elementos de identificação. Este objetivo poderá ser alcançado através da pseudonimização dos dados. Para aqueles que não possuam a chave de desencriptação, os dados pseudonimizados só dificilmente podem ser identificáveis. A ligação a uma identidade ainda existe sob a forma do pseudónimo mais a chave de desencriptação. Para quem esteja autorizado a utilizar

68 *Ibid.*, considerando 26.

69 *Ibid.*, artigo 6.º, n.º 1, al. e); Convenção 108, artigo 5.º, al. e).

essa chave, a re-identificação é possível com facilidade. É necessário assegurar a proteção contra a utilização de chaves de encriptação por pessoas não autorizadas.

Uma vez que a pseudonimização dos dados é um dos meios mais importantes de assegurar a proteção de dados em grande escala, sempre que não for possível evitar totalmente o uso de dados pessoais, a lógica e os efeitos dessa medida têm de ser explicados mais detalhadamente.

Exemplo: A frase «Charles Spencer, nascido em 3 de abril de 1967, tem quatro filhos: dois rapazes e duas raparigas» pode ser pseudonimizada, por exemplo, da seguinte forma:

«C.S. 1967 tem quatro filhos: dois rapazes e duas raparigas»; ou

«324 tem quatro filhos: dois rapazes e duas raparigas»; ou

«YESz320l tem quatro filhos: dois rapazes e duas raparigas».

Os utilizadores que acedam a estes dados pseudonimizados não terão geralmente capacidade para identificar «Charles Spencer, nascido em 3 de abril de 1967» a partir de «324» ou «YESz3201». Por conseguinte, os dados pseudonimizados estão mais protegidos contra utilizações abusivas.

Porém, no primeiro exemplo, a proteção é menor. Se a frase «C.S. 1967 tem quatro filhos: dois rapazes e duas raparigas» for utilizada na pequena aldeia onde vive Charles Spencer, este poderá ser facilmente reconhecido. O método de pseudonimização afeta a eficácia da proteção de dados.

São utilizados dados pessoais com elementos de identificação encriptados em muitos contextos como forma de manter secreta a identidade das pessoas. É uma técnica particularmente útil quando os responsáveis pelo tratamento necessitam de se certificar de que estão a lidar com as mesmas pessoas em causa, mas não precisam, nem devem, conhecer a verdadeira identidade dessas pessoas. É o caso, por exemplo, de um investigador que acompanha a evolução do estado de saúde de determinados doentes, cuja identidade é conhecida apenas do hospital onde recebem tratamento e que fornece os respetivos processos clínicos pseudonimizados ao investigador. A pseudonimização é, assim, um instrumento muito útil no arsenal da tecnologia de proteção da privacidade. Pode ser um elemento muito importante

na implementação da privacidade desde a conceção, que implica a incorporação da proteção de dados no tecido dos sistemas avançados de tratamento de dados.

2.2. Tratamento de dados

Pontos-chave

- O termo «tratamento» respeita sobretudo ao tratamento automatizado.
- Nos termos do direito da UE, o termo «tratamento» respeita igualmente ao tratamento manual em ficheiros estruturados.
- Nos termos do direito do CdE, o direito nacional pode incluir o tratamento manual na definição de «tratamento».

A proteção de dados ao abrigo da Convenção 108 e da Diretiva de Proteção de Dados incide essencialmente sobre o tratamento automatizado de dados.

No âmbito do **direito do CdE**, a definição de tratamento automatizado reconhece, porém, que poderão existir necessariamente algumas etapas de utilização manual dos dados pessoais entre as operações automatizadas. Do mesmo modo, no âmbito do **direito da UE**, o tratamento automatizado de dados é definido como «operações efetuadas sobre dados pessoais [...] por meios total ou parcialmente automatizados».[70]

Exemplo: No acórdão *Bodil Lindqvist*,[71] o TJUE entendeu que:

«a referência, feita numa página da Internet, a várias pessoas e a sua identificação pelo nome ou por outros meios, por exemplo, o número de telefone ou informações relativas às suas condições de trabalho e aos seus passatempos constitui um "tratamento de dados pessoais por meios total ou parcialmente automatizados" na aceção do artigo 3.º, n.º 1, da Diretiva 95/46.»

O tratamento manual de dados também exige proteção de dados.

70 Convenção 108, artigo 2.º, al. c); Diretiva Proteção de Dados, artigo 2.º, al. b) e artigo 3.º, n.º 1.

71 TJUE, acórdão de 6 de novembro de 2003 no processo C-101/01, *Bodil Lindqvist*, n.º 27.

A proteção de dados no **direito da UE** não está de modo algum limitada ao tratamento automatizado de dados. Consequentemente, nos termos do direito da UE, a proteção de dados é aplicável ao tratamento de dados pessoais contidos em ficheiros em papel especialmente estruturados.[72] Este alargamento da proteção de dados devese ao facto de que:

- os ficheiros em papel podem ser estruturados de modo a permitir a localização das informações de forma fácil e rápida; e

- o armazenamento de dados pessoais em ficheiros em papel estruturados permite contornar com maior facilidade as restrições impostas pela lei ao tratamento automatizado de dados.[73]

No âmbito do direito do CdE, a Convenção 108 regula, antes de mais, o tratamento de dados em ficheiros automatizados.[74] No entanto, também prevê a possibilidade de alargamento da proteção ao tratamento manual no direito interno. Muitas Partes na Convenção 108 aproveitaram esta possibilidade e dirigiram declarações naquele sentido ao SecretárioGeral do CdE.[75] O alargamento da proteção de dados nos termos dessa declaração tem de abranger todas as operações de tratamento manual de dados, não podendo restringirse ao tratamento de dados em ficheiros manuais.[76]

No que respeita à natureza das operações de tratamento incluídas**,** tanto o **direito da UE** como o **direito do CdE** estabelecem uma definição abrangente do termo «tratamento»: «"Tratamento de dados pessoais" [...] qualquer operação [...] tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição»[77] efetuada sobre dados pessoais. O termo «tratamento» também inclui os atos através dos quais a responsabilidade pelos dados é transferida de um responsável pelo tratamento para outro responsável pelo tratamento.

72 Diretiva Proteção de Dados, artigo 3.º, n.º 1.

73 *Ibid*., considerando 27.

74 Convenção 108, artigo 2.º, alínea b).

75 Ver as declarações efetuadas ao abrigo da Convenção 108, artigo 3.º, n.º 2, al. c).

76 Ver a redação da Convenção 108, artigo 3.º, n.º 2.

77 Diretiva Proteção de Dados, artigo 2.º, al. b). No mesmo sentido, ver também a Convenção 108, artigo 2.º, al. c).

Exemplo: Os empregadores recolhem e tratam dados sobre os seus funcionários, incluindo informações relativas aos seus salários. A base legal para este tratamento legítimo é o contrato de trabalho.

Os empregadores são obrigados a reencaminhar os dados sobre os salários do seu pessoal para as autoridades fiscais. Este reencaminhamento também constitui «tratamento» na aceção da Convenção 108 e da Diretiva. Contudo, a base legal para esta comunicação não é o contrato de trabalho. Terá de existir outra base legal para as operações de tratamento que resultam na transferência de dados sobre salários do empregador para as autoridades fiscais. Em regra, esta base legal encontrase nas disposições da legislação fiscal nacional. Na ausência destas disposições, a transferência dos dados constituiria um tratamento ilegal.

2.3. Os utilizadores de dados pessoais

Pontos-chave

- A pessoa que decide proceder ao tratamento de dados pessoais de terceiros é o «responsável pelo tratamento» nos termos da legislação sobre proteção de dados; se a decisão for tomada em conjunto por várias pessoas, estas poderão ser consideradas «responsáveis conjuntos pelo tratamento».
- Um «subcontratante» é uma entidade juridicamente distinta que trata os dados pessoais por conta do responsável pelo tratamento.
- Um subcontratante passa a ser considerado responsável pelo tratamento se utilizar os dados para os seus fins e não em conformidade com as instruções do responsável pelo tratamento.
- Qualquer pessoa que receba dados de um responsável pelo tratamento é um «destinatário».
- Um «terceiro» é uma pessoa singular ou coletiva que não atua sob as instruções do responsável pelo tratamento (e não é pessoa em causa, titular dos dados).
- Um «terceiro destinatário» é uma pessoa ou entidade juridicamente distinta do responsável pelo tratamento, mas que recebe dados pessoais fornecidos por este.

2.3.1. Responsáveis pelo tratamento e subcontratantes

A consequência mais importante da qualificação como responsável pelo tratamento ou subcontratante é a responsabilidade pelo cumprimento das obrigações que a legislação sobre proteção de dados impõe sobre cada um deles. Por conseguinte, só quem puder ser responsabilizado ao abrigo da lei aplicável é que poderá desempenhar aquelas funções. No setor privado, é geralmente uma pessoa singular ou coletiva; no setor público, é geralmente uma autoridade. Outras entidades, como organismos ou instituições sem personalidade jurídica, só podem ser responsáveis pelo tratamento ou subcontratantes quando tal estiver previsto em disposições legais especiais.

Exemplo: Se a divisão de marketing da empresa Sunshine planear proceder ao tratamento de dados para fins de um estudo de mercado, o responsável por esse tratamento será a empresa Sunshine e não a divisão de marketing. A divisão de marketing não pode ser o responsável pelo tratamento porque não tem personalidade jurídica autónoma.

Nos grupos de empresas, a empresamãe e cada uma das filiais são consideradas responsáveis pelo tratamento ou subcontratantes distintos, dado que são pessoas coletivas distintas. Uma vez que estas entidades possuem personalidades jurídicas distintas, a transferência de dados entre os membros de um grupo de empresas necessitará de uma base legal especial. Não existe nenhuma prerrogativa que permita o intercâmbio de dados pessoais, enquanto tal, entre entidades jurídicas distintas do mesmo grupo de empresas.

Neste contexto, importa mencionar o papel das pessoas singulares. No âmbito do **direito da UE**, as pessoas singulares, quando tratam dados pessoais sobre terceiros no exercício de atividades exclusivamente pessoais ou domésticas, não estão sujeitas às regras da Diretiva de Proteção de Dados e não são consideradas responsáveis pelo tratamento.[78]

No entanto, existe jurisprudência que defende, ainda assim, a aplicabilidade da legislação sobre proteção de dados quando uma pessoa singular, no contexto da utilização da Internet, publica dados sobre terceiros.

78 Diretiva Proteção de Dados, considerando 12 e artigo 3.º, n.º 2, último travessão.

Exemplo: O TJUE considerou no acórdão *Bodil Lindqvist*[79] que:

«a referência, feita numa página da Internet, a várias pessoas e a sua identificação pelo nome ou por outros meios [...] constitui um "tratamento de dados pessoais por meios total ou parcialmente automatizados" na aceção do artigo 3.º, n.º 1, da Diretiva 95/46».[80]

Este tratamento de dados pessoais não constitui uma atividade exclusivamente pessoal ou doméstica, que está fora do âmbito de aplicação da Diretiva de Proteção de Dados, dado que esta exceção «deve [...] ser interpretada como tendo unicamente por objeto as atividades que se inserem no âmbito da vida privada ou familiar dos particulares, o que não é manifestamente o caso do tratamento de dados de caráter pessoal que consiste na sua publicação na Internet de maneira que esses dados são disponibilizados a um número indefinido de pessoas.»[81]

Responsável pelo tratamento

No âmbito do **direito da UE**, um responsável pelo tratamento é definido como alguém que «individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais».[82] Na sua decisão, o responsável pelo tratamento explica porquê e como os dados serão tratados. No âmbito do **direito do CdE**, a definição de «responsável» refere ainda que o responsável decide as categorias de dados de caráter pessoal que devem ser registadas.[83]

Na sua definição de responsável, a Convenção 108 menciona um outro aspeto da responsabilidade pelo tratamento que merece atenção. Esta definição faz referência à questão da competência para proceder licitamente ao tratamento de certos dados para um determinado fim. Contudo, sempre que tenham lugar operações de tratamento alegadamente ilegais e seja necessário identificar o responsável pelo tratamento, este será a pessoa ou entidade (como uma empresa ou uma autoridade) que decidiu que os dados deveriam ser tratados, independentemente de ter ou

79 TJUE, acórdão de 6 de novembro de 2003 no processo C-101/01, *Bodil Lindqvist*.

80 *Ibid.* n.º 27.

81 *Ibid.* n.º 47.

82 Diretiva Proteção de Dados, artigo 2.º, al. d).

83 Convenção 108, artigo 2.º, al. d).

não competência legal para o fazer[84]. Por conseguinte, os pedidos de apagamento devem ser sempre dirigidos ao responsável «real» pelo tratamento.

Responsabilidade conjunta pelo tratamento

A definição de «responsável pelo tratamento» na Diretiva de Proteção de Dados prevê a possibilidade de existirem várias entidades juridicamente distintas que, em conjunto com outras, desempenhem o papel de responsável pelo tratamento, o que significa que decidem, em conjunto, tratar os dados para uma finalidade comum.[85] Porém, isto só será possível nos casos em que exista uma base legal para o tratamento conjunto de dados para uma finalidade comum.

Exemplo: Uma base de dados sobre clientes em situação de incumprimento gerida em conjunto por várias instituições de crédito é um exemplo comum de responsabilidade conjunta pelo tratamento. Quando alguém apresenta um pedido de crédito a um banco que é um dos responsáveis conjuntos pelo tratamento, os bancos consultam a base de dados para os ajudar a tomar decisões informadas sobre a solvabilidade do requerente.

Os regulamentos não esclarecem se a responsabilidade conjunta pelo tratamento exige que a finalidade comum seja a mesma para cada um dos responsáveis pelo tratamento ou se é suficiente que as finalidades coincidam apenas em parte. Porém, ainda não existe jurisprudência relevante ao nível europeu e as consequências em matéria de responsabilidade também não estão claramente definidas. O Grupo de Trabalho do artigo 29.º defende uma interpretação mais ampla do conceito de responsabilidade conjunta pelo tratamento com o objetivo de adotar uma certa flexibilidade para ter em conta a crescente complexidade da realidade do tratamento de dados.[86] Um caso que envolve a Sociedade das Telecomunicações Financeiras Interbancárias no Mundo (Society for Worldwide Interbank Financial Telecommunication – SWIFT) ilustra a posição do Grupo de Trabalho.

Exemplo: Naquele que ficou conhecido como o caso SWIFT, algumas instituições bancárias europeias contrataram a SWIFT, inicialmente na qualidade de

84 Ver também Grupo de Trabalho do artigo 29.º (2010), *Parecer 1/ 2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»*, WP 169, Bruxelas, 16 de fevereiro de 2010, p. 19.

85 Diretiva Proteção de Dados, artigo 2.º, al. d).

86 Grupo de Trabalho do artigo 29.º (2010), *Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»*, WP 169, Bruxelas, 16 de fevereiro de 2010, p. 23.

subcontratante, para realizar transferências de dados no decurso de transações bancárias. A SWIFT divulgou os dados dessas transações bancárias, que estavam armazenados num centro de serviços de computação nos Estados Unidos, ao Departamento do Tesouro dos EUA sem ordem expressa das instituições bancárias que a tinham contratado. Ao apreciar a legalidade desta situação, o Grupo de Trabalho do artigo 29.º chegou à conclusão de que as instituições bancárias europeias que tinham contratado a SWIFT, assim como a própria SWIFT, tinham de ser consideradas responsáveis conjuntas pelo tratamento e, como tal, partilhavam a responsabilidade, perante os seus clientes europeus, pela divulgação dos seus dados às autoridades norteamericanas.[87] Ao decidir proceder à divulgação, a SWIFT tinha assumido – ilegalmente – o papel de responsável pelo tratamento; é evidente que as instituições bancárias não tinham cumprido cabalmente a sua obrigação de supervisionar o subcontratante e, por conseguinte, não podiam ser completamente exoneradas da sua responsabilidade como responsáveis pelo tratamento. Esta situação gera responsabilidade conjunta pelo tratamento.

Subcontratante

No **direito da UE**, o subcontratante é definido como alguém que trata dados pessoais por conta do responsável pelo tratamento.[88] As atividades confiadas ao subcontratante podem limitarse a uma tarefa ou contexto muito específico ou serem muito genéricas e abrangentes.

No **direito do CdE**, o termo «subcontratante» é utilizado na mesma aceção que no direito da UE.

Para além de tratarem dados por conta de outrem, os subcontratantes também serão responsáveis pelo tratamento por direito próprio em relação às operações de tratamento que realizarem para os seus próprios fins (por ex., a administração dos seus próprios funcionários, vendas e contas).

87 Grupo de Trabalho do artigo 29.º (2006), *Parecer 10/2006 sobre o tratamento de dados pessoais pela Sociedade das Telecomunicações Financeiras Interbancárias no Mundo (Society for Worldwide Interbank Financial Telecommunication SWIFT)*, WP 128, Bruxelas, 22 de novembro de 2006.

88 Diretiva Proteção de Dados, artigo 2.º, al. e).

Exemplos: A Everready é uma empresa especializada no tratamento de dados para fins de administração de dados sobre recursos humanos para outras empresas. Nesta função, a Everready é um subcontratante.

Porém, quando a Everready trata os dados dos seus próprios funcionários, é ela a responsável pelas operações de tratamento de dados para fins de cumprimento das suas obrigações enquanto empregador.

A relação entre responsável pelo tratamento e subcontratante

Tal como vimos, o responsável pelo tratamento é aquele que determina as finalidades e os meios do tratamento.

Exemplo: O diretor da empresa Sunshine decide que a empresa Moonlight, especializada em análises do mercado, deverá realizar uma análise de mercado dos dados dos clientes da Sunshine. Embora a tarefa de determinar os meios do tratamento seja, assim, delegada à Moonlight, a empresa Sunshine continua a ser o responsável pelo tratamento e a Moonlight é um mero subcontratante, dado que, nos termos do contrato, a Moonlight só poderá utilizar os dados dos clientes da Sunshine para as finalidades que esta determinar.

Se o poder de determinar os meios do tratamento for delegado a um subcontratante, o responsável pelo tratamento deve, ainda assim, poder interferir nas decisões daquele sobre esses meios. A responsabilidade global continua a recair sobre o responsável pelo tratamento, o qual está obrigado a supervisionar o subcontratante para assegurar que as decisões tomadas por este cumprem a legislação sobre proteção de dados. Por conseguinte, um contrato que proíba o responsável pelo tratamento de interferir nas decisões do subcontratante seria provavelmente interpretado como dando origem a uma situação de responsabilidade conjunta pelo tratamento, em que ambas as partes partilham a responsabilidade que a lei atribui aos responsáveis pelo tratamento.

Além disso, se um subcontratante não respeitar os limites de utilização dos dados estipulados pelo responsável pelo tratamento, passará a ser considerado, ele próprio, responsável pelo tratamento, pelo menos na parte respeitante às operações realizadas em violação das instruções do responsável pelo tratamento. Neste caso, o subcontratante passará muito provavelmente a ser considerado um responsável pelo tratamento, que age ilicitamente. Por sua vez, o responsável pelo tratamento

inicial terá de explicar como foi possível que o subcontratante violasse o seu mandato. Com efeito, o Grupo de Trabalho do artigo 29.º presume geralmente a existência de responsabilidade conjunta pelo tratamento nestes casos, dado que esta qualificação permite proteger melhor os interesses das pessoas em causa.[89] Uma importante consequência da responsabilidade conjunta pelo tratamento seria a responsabilidade solidária dos responsáveis pelo tratamento pelos danos causados, proporcionando assim às pessoas em causa um leque mais vasto de meios de recurso.

Poderão também suscitarse questões sobre a divisão da responsabilidade nos casos em que o responsável pelo tratamento seja uma pequena empresa e o subcontratante seja uma grande sociedade comercial com o poder de ditar as condições dos seus serviços. Nestes casos, porém, o Grupo de Trabalho do artigo 29.º considera que o desequilíbrio económico não justifica a redução do grau de responsabilidade e que a definição do conceito de responsável pelo tratamento deve ser mantida.[90]

Por uma questão de clareza e transparência, os elementos concretos da relação entre o responsável pelo tratamento e o subcontratante devem constar de um contrato reduzido a escrito.[91] A inexistência de tal contrato corresponde a uma violação da obrigação do responsável pelo tratamento de fornecer documentação sobre as responsabilidades mútuas, estando sujeita a sanções.[92]

Os subcontratantes poderão querer delegar certas tarefas noutros subcontratantes. Esta delegação é permitida por lei e dependerá, em concreto, das cláusulas do contrato celebrado entre o responsável pelo tratamento e o subcontratante, nomeadamente se é sempre exigida a autorização do primeiro ou se será suficiente informálo.

No âmbito do **direito do CdE**, a interpretação dos conceitos de responsável pelo tratamento e subcontratante, tal como explicado anteriormente, é plenamente

89 Grupo de Trabalho do artigo 29.º (2010), *Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»*, WP 169, Bruxelas, 16 de fevereiro de 2010**,** p. 30; e Grupo de Trabalho do artigo 29.º (2006), *Parecer 10/2006 sobre o tratamento de dados pessoais pela Sociedade das Telecomunicações Financeiras Interbancárias no Mundo (Society for Worldwide Interbank Financial Telecommunication SWIFT)*, WP 128, Bruxelas, 22 de novembro de 2006.

90 Grupo de Trabalho do artigo 29.º (2010), *Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»*, WP 169, Bruxelas, 16 de fevereiro de 2010, p. 31.

91 Diretiva Proteção de Dados, artigo 17.º, n.ºs 3 e 4.

92 Grupo de Trabalho do artigo 29.º (2010), *Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»*, WP 169, Bruxelas, 16 de fevereiro de 2010, p. 32.

aplicável, conforme demonstram as recomendações que têm sido adotadas em conformidade com a Convenção 108.[93]

2.3.2. Destinatários e terceiros

A diferença entre estas duas categorias de pessoas ou entidades, estabelecidas pela Diretiva de Proteção de Dados, reside sobretudo na sua relação com o responsável pelo tratamento e, consequentemente, na sua autorização para aceder a dados pessoais na posse do responsável pelo tratamento.

Um «terceiro» é alguém juridicamente distinto do responsável pelo tratamento. Por conseguinte, a divulgação de dados a um terceiro exige sempre uma base legal específica. Nos termos do artigo 2.º, alínea f), da Diretiva de Proteção de Dados, um terceiro é «a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que não a pessoa em causa, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão habilitadas a tratar dos dados». Deste modo, as pessoas que trabalham para uma organização juridicamente distinta do responsável pelo tratamento – ainda que pertença ao mesmo grupo ou empresamãe – serão consideradas «terceiros» ou pertencentes a um «terceiro». Por outro lado, os balcões de um banco que procedem ao tratamento das contas dos clientes sob a autoridade direta da sede não serão considerados «terceiros».[94]

«Destinatário» é um termo mais amplo do que «terceiro». Na aceção do artigo 2.º, alínea g), da Diretiva de Proteção de Dados, um destinatário é «a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que receba comunicações de dados, independentemente de se tratar ou não de um terceiro». O destinatário poderá ser uma pessoa ou entidade não pertencente ao responsável pelo tratamento ou ao subcontratante – caso em que seria então um terceiro – ou pertencente ao responsável pelo tratamento ou ao subcontratante, tal como um funcionário ou outra divisão da mesma empresa ou autoridade.

A distinção entre destinatários e terceiros só é importante devido às condições para que a divulgação dos dados seja válida. Os funcionários de um responsável pelo tratamento ou subcontratante podem, sem necessidade de cumprimento de qualquer

93 Ver, por exemplo, Recomendação sobre a definição de perfis, artigo 1.º.

94 Grupo de Trabalho do artigo 29.º (2010), *Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»*, WP 169, Bruxelas, 16 de fevereiro de 2010, p. 36.

outro requisito legal, ser destinatários de dados pessoais se estiverem envolvidos nas operações de tratamento do empregador. Por outro lado, um terceiro, sendo uma entidade juridicamente distinta do responsável pelo tratamento ou do subcontratante, não está autorizado a utilizar dados pessoais tratados pelo responsável pelo tratamento, salvo se existir uma base legal específica para tal no caso concreto. Consequentemente, os «terceiros destinatários» necessitarão sempre de uma base legal para receberem licitamente dados pessoais.

Exemplo: O funcionário de um subcontratante, que utiliza dados pessoais no âmbito das tarefas que o empregador lhe confiou, é um destinatário de dados, mas não um terceiro, pois utiliza os dados por conta e sob as instruções do subcontratante.

Porém, se esse mesmo funcionário decidir utilizar os dados a que tem acesso na qualidade de funcionário do subcontratante para os seus próprios fins e os vender a outra empresa, terá agido como um terceiro. Já não estará a seguir as ordens do subcontratante (o empregador). Enquanto terceiro, o funcionário necessitaria de uma base legal para adquirir e vender os dados. Neste exemplo, essa base legal é certamente inexistente, pelo que os atos do funcionário são ilegais.

2.4. Consentimento

Pontos-chave

- O consentimento, enquanto base legal do tratamento de dados pessoais, tem de ser livre, informado e específico.
- O consentimento tem de ser dado de forma inequívoca. O consentimento pode ser dado explicitamente ou implicitamente através de atos que não deixem dúvidas de que a pessoa em causa concorda com o tratamento dos seus dados.
- O tratamento de dados sensíveis com base no consentimento exige um consentimento explícito.
- O consentimento pode ser revogado a todo o tempo.

Entendese por consentimento «qualquer manifestação de vontade, livre, específica e informada» da pessoa em causa.[95] Em muitos casos, é a base legal do tratamento legítimo de dados (ver secção 4.1).

2.4.1. Os elementos de um consentimento válido

O **direito da UE** estabelece três requisitos da validade do consentimento, que visam assegurar que as pessoas em causa pretendiam genuinamente autorizar a utilização dos seus dados.

- a pessoa em causa não pode estar sob qualquer pressão quando presta o seu consentimento;
- a pessoa em causa deve ter sido devidamente informada sobre o objeto e as consequências do consentimento; e
- o âmbito do consentimento deve ser razoavelmente concreto.

O consentimento só será válido na aceção da legislação sobre proteção de dados se todos estes requisitos estiverem preenchidos.

A Convenção 108 não contém uma definição de consentimento; esta tarefa incumbe ao legislador nacional. No entanto, **no direito do CdE**, os elementos de um consentimento válido correspondem aos referidos anteriormente, tal como previsto nas recomendações adotadas ao abrigo da Convenção 108.[96] Os requisitos de validade do consentimento são iguais aos requisitos de validade da declaração negocial estipulados no direito civil europeu.

Outros requisitos de validade do consentimento previstos no direito civil, tais como a capacidade jurídica, também serão naturalmente aplicáveis no contexto da proteção de dados, na medida em que são requisitos jurídicos fundamentais. O consentimento inválido de pessoas sem capacidade jurídica não constitui uma base legal para o tratamento de dados sobre essas pessoas.

95 Diretiva Proteção de Dados, artigo 2.º, al. h).

96 Ver, por exemplo, Convenção 108, Recomendação sobre os dados estatísticos, ponto 6.

O consentimento pode ser dado de forma explícita[97] ou não explícita. O primeiro não deixa dúvidas quanto à intenção da pessoa em causa e pode ser dado verbalmente ou por escrito; o segundo é deduzido a partir das circunstâncias. O consentimento tem de ser dado sempre de forma inequívoca,[98] o que significa que não devem existir dúvidas razoáveis de que a pessoa em causa pretendia comunicar a sua permissão para o tratamento dos seus dados. O consentimento deduzido da mera inércia, por exemplo, não constitui um consentimento inequívoco. Quando esteja em causa o tratamento de dados sensíveis, o consentimento tem de ser obrigatoriamente explícito e inequívoco.

Consentimento livre

A existência de consentimento livre só é válida «se a pessoa em causa puder exercer uma verdadeira escolha e não existir nenhum risco de fraude, intimidação, coação ou consequências negativas importantes se o consentimento for recusado».[99]

Exemplo: Em muitos aeroportos, os passageiros são submetidos a scâneres corporais no acesso à área de embarque.[100] Uma vez que os dados dos passageiros estão a ser tratados durante a utilização do scâner, o tratamento deve basearse num dos fundamentos legais previstos no artigo 7.º da Diretiva de Proteção de Dados (ver secção 4.1.1). Passar ou não pelos scâneres corporais é por vezes apresentado aos passageiros como uma opção, o que permitiria inferir que o tratamento poderia ser justificado pelo seu consentimento. No entanto, os passageiros poderão recear que a recusa de passar pelos scâneres corporais levante suspeitas ou desencadeie medidas de controlo adicionais, como as revistas pessoais. Muitos passageiros darão o seu consentimento à utilização do scâner porque, ao fazêlo, evitarão potenciais problemas ou atrasos. Provavelmente, este consentimento não será suficientemente livre.

Por conseguinte, um fundamento legal sólido só poderá ser um ato do legislador, com base no artigo 7.º, alínea e), da Diretiva de Proteção de Dados, criando assim para os passageiros a obrigação de cooperar devido a um interesse público superior. Essa legislação poderá, ainda assim, prever uma escolha entre

97 Diretiva Proteção de Dados, artigo 8.º, n.º 2.

98 *Ibid.*, artigo 7.º, al. a) e artigo 26.º, n.º 1.

99 Ver também Grupo de Trabalho do artigo 29.º (2011), *Parecer 15/2011 sobre a definição de consentimento*, WP 187, Bruxelas, 13 de julho de 2011, p. 14.

100 Este exemplo é retirado de *Ibid.*, p. 17.

o scâner e o controlo manual, mas apenas como parte de medidas adicionais de controlo fronteiriço necessárias no caso concreto. Foi este o entendimento consagrado pela Comissão Europeia em dois regulamentos sobre scâneres de segurança em 2011.[101]

A liberdade do consentimento também poderá estar ameaçada em situações de subordinação, em que exista um desequilíbrio económico ou de outro tipo significativo entre o responsável pelo tratamento que obtém o consentimento e a pessoa em causa que dá o consentimento.[102]

Exemplo: Uma grande empresa tenciona criar um diretório com os nomes de todos os funcionários, a sua função na empresa e a sua morada profissional, tendo como único objetivo melhorar as comunicações internas. O diretor de Recursos Humanos propõe a inclusão de uma fotografia de cada funcionário no diretório, o que permitiria, por exemplo, reconhecer com maior facilidade os colegas numa reunião. Os representantes dos funcionários exigem que, para tal, seja previamente obtido o consentimento de cada funcionário.

Nesta situação, o consentimento do funcionário deve ser considerado a base legal para o tratamento das fotografias no diretório porque é óbvio que a publicação da fotografia no diretório, em si mesma, não tem consequências negativas e, além disso, é pouco provável que o empregador penalize o funcionário se este não concordar com a publicação da sua fotografia no diretório.

Porém, isto não significa que o consentimento nunca poderá ser válido em casos em que a recusa desse consentimento tenha consequências negativas. Por exemplo, se a recusa de consentimento para emissão de um cartão de cliente de um supermercado tiver como única consequência a impossibilidade de aproveitar certos descontos, o consentimento é uma base legal válida para o tratamento dos dados pessoais

101 Regulamento (UE) n.º 1141/2011 da Comissão, de 10 de novembro de 2011, que altera o Regulamento (CE) n.º 272/2009 que complementa as normas de base comuns para a proteção da aviação civil, no que respeita à utilização de scâneres de segurança nos aeroportos da União Europeia, JO 2011 L 293, e Regulamento de Execução (UE) n.º 1147/2011 da Comissão, de 11 de novembro de 2011, que altera o Regulamento (UE) n.º 185/2010 que estabelece as medidas de execução das normas de base comuns sobre a segurança da aviação, no que respeita à utilização de scâneres de segurança nos aeroportos da UE, JO 2011 L 294.

102 Ver também Grupo de Trabalho do artigo 29.º (2001), *Parecer 8/2001 sobre o tratamento de dados pessoais no âmbito do emprego*, WP 48, Bruxelas, 13 de setembro de 2001; e Grupo de Trabalho do artigo 29.º (2005), *Documento de trabalho sobre uma interpretação comum do n.º 1 do artigo 26.º Diretiva 95/46/CE de 24 de outubro de 1995*, WP 114, Bruxelas, 25 de novembro de 2005.

dos clientes que deram o seu consentimento. Não existe uma relação de subordinação entre a empresa e o cliente e as consequências do não consentimento não são suficientemente graves para inibir a liberdade de escolha da pessoa em causa.

Por outro lado, sempre que a obtenção de bens ou serviços suficientemente importantes depender da divulgação de certos dados pessoais a terceiros, o consentimento da pessoa em causa para a divulgação dos seus dados não pode, em regra, ser considerado uma decisão livre e, como tal, não é válido nos termos da legislação sobre proteção de dados.

Exemplo: O consentimento manifestado pelos passageiros a uma companhia aérea para que transfira os chamados registos de identificação dos passageiros (PNR), nomeadamente dados sobre a sua identidade, hábitos alimentares ou problemas de saúde, aos serviços de imigração de um determinado país estrangeiro não pode ser considerado válido nos termos da legislação sobre proteção de dados, uma vez que os passageiros que desejam visitar esse país não têm escolha. Para esses dados serem transferidos licitamente, a base legal terá de ser outra, muito provavelmente uma lei especial.

Consentimento informado

A pessoa em causa deve possuir informações suficientes antes de tomar a sua decisão. A suficiência ou insuficiência das informações fornecidas só poderá ser determinada caso a caso. Em regra, essas informações incluirão uma descrição rigorosa e facilmente compreensível do objeto do consentimento e também das consequências do consentimento e da recusa do consentimento. A linguagem utilizada deve ser adaptada aos destinatários previsíveis das informações.

Além disso, a pessoa em causa deve poder aceder com facilidade a essas informações. A acessibilidade e a visibilidade das informações são elementos importantes. Num ambiente em linha, os avisos com vários níveis poderão ser uma boa solução, dado que a pessoa em causa terá assim acesso a uma versão concisa das informações, bem como a uma versão mais completa.

Consentimento específico

Para ser válido, o consentimento também tem de ser específico. Esta característica está intrinsecamente ligada à qualidade das informações fornecidas sobre o objeto

do consentimento. Neste contexto, são relevantes as expectativas razoáveis de uma pessoa em causa média. Se estiverem previstas novas operações de tratamento ou alterações que não poderiam razoavelmente ter sido previstas quando a pessoa em causa deu inicialmente o seu consentimento, é necessário pedir-lhe novamente o seu consentimento.

Exemplo: No acórdão *Deutsche Telekom AG*,[103] o TJUE pronunciouse sobre a questão da necessidade de um prestador de serviços de telecomunicações, que estava obrigado a transmitir dados pessoais dos assinantes nos termos do artigo 12.º da *Diretiva relativa à privacidade e às comunicações eletrónicas*,[104] obter novamente o consentimento das pessoas em causa, dado que os destinatários não tinham sido originalmente identificados quando o consentimento foi prestado.

O TJUE considerou que o referido artigo não impunha a obtenção de um novo consentimento das pessoas em causa antes da transmissão dos dados, uma vez que estas tinham, nos termos desta disposição, a possibilidade de dar apenas o seu consentimento em relação à finalidade do tratamento, que é a publicação dos seus dados, e não podiam escolher entre as diferentes listas em que esses dados poderiam ser publicados.

Tal como salientou o Tribunal de Justiça, «resulta de uma interpretação contextual e sistemática do artigo 12.º da diretiva relativa à privacidade e às comunicações eletrónicas que o consentimento nos termos do n.º 2 deste artigo diz respeito ao fim a que se destina a publicação dos dados de caráter pessoal numa lista pública e não à identidade de um fornecedor de lista em concreto.»[105] Acresce que «é a própria publicação dos dados de caráter pessoal numa lista com uma finalidade especial que se pode revelar prejudicial para o assinante»[106]e não a identidade do autor desta publicação.

103 TJUE, acórdão de 5 de maio de 2011 no processo C543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*; ver, em especial, n.ºs 53 e 54.

104 Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, JO 2002 L 201 (*Diretiva relativa à privacidade e às comunicações eletrónicas*).

105 TJUE, acórdão de 5 de maio de 2011 no processo C543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*; ver, em especial, n.º 61.

106 *Ibid.*, ver especialmente, n.º 62.

2.4.2. O direito de revogar o consentimento a todo o tempo

A Diretiva de Proteção de Dados não menciona o direito geral de revogar o consentimento a todo o tempo. No entanto, presumese, em regra, que esse direito existe e que a pessoa em causa deverá poder exercêlo discricionariamente. Não deve ser exigida qualquer justificação para a revogação nem deve existir qualquer risco de consequências negativas, exceto as que resultam da cessação dos benefícios eventualmente decorrentes da utilização de dados objeto do consentimento dado anteriormente.

Exemplo: Um cliente concorda em receber material promocional num endereço que fornece a um responsável pelo tratamento. Se o cliente revogar o consentimento, o responsável pelo tratamento tem de parar imediatamente de enviar material promocional. Não devem existir quaisquer consequências punitivas, tais como taxas.

Se um cliente beneficiar de um desconto de 5 % no preço de um quarto de hotel em troca do seu consentimento para a utilização dos seus dados para efeitos de envio de material promocional, a revogação posterior desse consentimento não deve gerar a obrigação de devolver esses descontos.

3

Os princípios fundamentais da legislação europeia sobre proteção de dados

UE	Questões abrangidas	CdE
Diretiva de Proteção de Dados, artigo 6.º, n.º 1, al. a) e b) TJUE, acórdão de 16 de dezembro de 2008 no processo C-524/06, *Huber/Alemanha* TJUE, acórdão de 9 de novembro de 2010 nos processos apensos C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen*	**O princípio do tratamento lícito**	Convenção 108, artigo 5.º, al. a) e b) TEDH, acórdão *Rotaru c. Roménia* [GS] de 4 de maio de 2000, petição n.º 28341/95. TEDH, acórdão *Taylor-Sabori c. Reino Unido* de 22 de outubro de 2002, petição n.º 47114/99 TEDH, acórdão *Peck c. Reino Unido* de 28 de janeiro de 2003, petição n.º 44647/98 TEDH, acórdão *Khelili c. Suíça* de 18 de outubro de 2011, petição n.º 16188/07. TEDH, acórdão *Leander c. Suécia* de 26 de março de 1987, petição n.º 9248/81.
Diretiva de Proteção de Dados, artigo 6.º, n.º 1, al. b)	**O princípio da especificação e da limitação da finalidade**	Convenção 108, artigo 5.º, al. b)
	Os princípios relativos à qualidade dos dados:	
Diretiva de Proteção de Dados, artigo 6.º, n.º 1, al. c)	**Pertinência dos dados**	Convenção 108, artigo 5.º, al. c)
Diretiva de Proteção de Dados, artigo 6.º, n.º 1, al. d)	**Exatidão dos dados**	Convenção 108, artigo 5.º, al. d)

UE	Questões abrangidas	CdE
Diretiva de Proteção de Dados, artigo 6.º, n.º 1, al. e)	Limitação da conservação dos dados	Convenção 108, artigo 5.º, al. e)
Diretiva de Proteção de Dados, artigo 6.º, n.º 1, al. e)	Derrogação para fins estatísticos e de investigação científica	Convenção 108, artigo 9.º, n.º 3
Diretiva de Proteção de Dados, artigo 6.º, n.º 1, al. a)	O princípio do tratamento leal	Convenção 108, artigo 5.º, al. a) TEDH, acórdão *Haralambie c. Roménia* de 27 de outubro de 2009, petição n.º 21737/03. TEDH, acórdão *K.H. e outros c. Eslováquia* de 6 de novembro de 2009, petição n.º 32881/04
Diretiva de Proteção de Dados, artigo 6.º, n.º 2	O princípio da responsabilidade	

Os princípios estabelecidos no artigo 5.º da Convenção 108 consagram a essência da legislação europeia sobre proteção de dados. Surgem igualmente no artigo 6.º da Diretiva de Proteção de Dados, constituindo o ponto de partida para disposições mais detalhadas nos artigos seguintes da Diretiva. Toda a legislação sobre proteção de dados adotada posteriormente ao nível do CdE ou da UE tem de cumprir estes princípios, que devem também pautar a interpretação dessa legislação. Poderão ser estabelecidas derrogações e restrições a estes princípios fundamentais ao nível nacional,[107] desde que estejam previstas na lei, prossigam um objetivo legítimo e sejam necessárias numa sociedade democrática. Estas três condições são cumulativas.

3.1. O princípio do tratamento lícito

Pontos-chave

- Para compreender o princípio do tratamento lícito, é necessário analisar as condições do estabelecimento de restrições lícitas ao direito à proteção de dados à luz do artigo 52.º, n.º 1, da Carta e aos requisitos de justificação da ingerência nos termos do artigo 8.º, n.º 2, da CEDH.

107 Convenção 108, artigo 9.º, n.º 2; Diretiva Proteção de Dados, artigo 13.º, n.º 2.

- Nesta conformidade, o tratamento de dados pessoais só é lícito se:
  - estiver de acordo com a lei;
  - prosseguir um objetivo legítimo; e
  - for necessário numa sociedade democrática para alcançar o objetivo legítimo.

Na legislação sobre proteção de dados da UE e do CdE, o princípio do tratamento lícito é o primeiro princípio identificado e encontrase formulado em termos praticamente idênticos no artigo 5.º da Convenção 108 e no artigo 6.º da Diretiva de Proteção de Dados.

Nenhuma destas disposições contém uma definição de «tratamento lícito». Para compreender este termo jurídico, é necessário analisar o conceito de ingerência justificada na aceção da CEDH, tal como interpretado pelo TEDH, bem como as condições do estabelecimento de restrições lícitas nos termos do artigo 52.º da Carta.

3.1.1. Os requisitos de justificação da ingerência ao abrigo da CEDH

O tratamento de dados pessoais poderá constituir uma ingerência no exercício do direito ao respeito pela vida privada da pessoa em causa. Porém, este não é um direito absoluto, devendo, pelo contrário, ser conciliado com outros interesses legítimos, sejam de outras pessoas (interesses privados) ou da sociedade no seu todo (interesses públicos).

A ingerência das autoridades públicas é justificada nas seguintes condições:

De acordo com a lei

Segundo a jurisprudência do TEDH, considerase que a ingerência está de acordo com a lei se tiver por base uma disposição do direito interno com determinadas características. Os interessados têm de ter acesso à lei e esta deve ter efeitos previsíveis.[108] Considerase que uma regra é previsível se for formulada com precisão suficiente para permitir a qualquer pessoa pautar o comportamento, solicitando, se necessário,

108 TEDH, acórdão *Amann c. Suíça* [GS] de 16 de fevereiro de 2000, n.º 50, petição n.º 27798/95; ver também TEDH, acórdão *Kopp c. Suíça* de 25 de março de 1998, n.º 55, petição n.º 23224/94 e TEDH, acórdão *Iordachi e outros c. Moldávia* de 10 de fevereiro de 2009, n.º 50, petição n.º 25198/02.

um parecer profissional.[109] O grau de precisão exigido da «lei» neste contexto dependerá da matéria em causa.[110]

Exemplo: No acórdão *Rotaru c. Roménia*,[111] o TEDH concluiu que tinha havido uma violação do artigo 8.º da CEDH porque o direito romeno permitia a recolha, registo e arquivo, em ficheiros secretos, de informações que afetassem a segurança nacional sem estabelecer limites ao exercício desses poderes pelas autoridades, que era assim discricionário. Por exemplo, o direito nacional não definia o tipo de informações que poderiam ser tratadas, os grupos de pessoas que poderiam ser objeto de medidas de vigilância, as circunstâncias em que essas medidas poderiam ser adotadas ou o procedimento a seguir. Face as estas deficiências, o TEDH concluiu que o direito interno não cumpria o requisito de previsibilidade previsto no artigo 8.º da CEDH e que este artigo tinha sido violado.

Exemplo: No processo que deu origem ao acórdão *Taylor-Sabori c. Reino Unido*,[112] o requerente tinha sido alvo de medidas de vigilância policial. Utilizando um «clone» do *pager* do requerente, a polícia conseguiu intercetar mensagens que lhe tinham sido enviadas. O requerente foi então detido e acusado de associação criminosa pela distribuição de uma substância controlada. Parte das provas reunidas pelo Ministério Público consistia em transcrições contemporâneas das mensagens do *pager* efetuadas pela polícia. No entanto, à data do julgamento do requerente, a interceção de comunicações transmitidas através de um sistema privado de telecomunicações não estava regulada no direito britânico. Por conseguinte, a ingerência no exercício dos seus direitos não estava «de acordo com a lei». O TEDH concluiu que tinha havido uma violação do artigo 8.º da CEDH.

109 TEDH, acórdão *Amann c. Suíça* [GS] de 16 de fevereiro de 2000, petição n.º 27798/95, n.º 56; ver também TEDH, acórdão *Malone c. Reino Unido* de 2 de agosto de 1984, petição n.º 8691/79, n.º 66; TEDH, acórdão *Silver e outros c. Reino Unido* de 25 de março de 1983, petições n.ºs 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, n.º 88.

110 TEDH, acórdão *The Sunday Times c. Reino Unido* de 26 de abril de 1979, petição n.º 6538/74, n.º 49; ver também TEDH, acórdão *Silver e outros c. Reino Unido* de 25 de março de 1983, petições n.ºs 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, n.º 88.

111 TEDH, acórdão *Rotaru c. Roménia* [GS] de 4 de abril de 2000, petição n.º 28341/95, n.º 57; ver também TEDH, acórdão *Association for European Integration and Human Rights e Ekimdzhiev c. Bulgária* de 28 de junho de 2007, petição n.º 62540/00; TEDH, acórdão *Shimovolos c. Rússia* de 21 de junho de 2011, petição n.º 30194/09; e TEDH, acórdão *Vetter c. França* de 31 de maio de 2005, petição n.º 59842/00.

112 TEDH, acórdão *Taylor-Sabori c. Reino Unido* de 22 de outubro de 2002, petição n.º 47114/99.

Na prossecução de um objetivo legítimo

O objetivo legítimo poderá ser um dos interesses públicos identificados ou os direitos e liberdades dos outros.

Exemplo: No processo que deu origem ao acórdão *Peck c. Reino Unido,*[113] o requerente tentou suicidar-se na rua cortando os pulsos, sem se aperceber de que o ato tinha sido filmado por uma câmara CCTV. A polícia, que estava a observar as câmaras CCTV, salvouo e, depois, facultou as imagens à comunicação social, que as publicou sem ocultar a face do requerente. O TEDH considerou que não existiam motivos relevantes ou suficientes que justificassem a divulgação direta das imagens pelas autoridades ao público sem obter previamente o consentimento do requerente ou sem ocultar a sua identidade. O TEDH concluiu que tinha havido uma violação do artigo 8.º da CEDH.

Necessário numa sociedade democrática

O TEDH afirmou que o conceito de necessidade significa que a ingerência corresponde a uma necessidade social imperiosa e, em especial, que é proporcional ao objetivo legítimo prosseguido.[114]

Exemplo: No processo que deu origem ao acórdão *Khelili c. Suíça*,[115] durante um controlo policial, a polícia encontrou cartões de visita na posse da requerente, onde se lia: «Mulher atraente, simpática, de 38 anos, gostaria de conhecer um cavalheiro para beber um copo ou sair de vez em quando. Tel. n.º [...]». A requerente alegou que, depois de ter descoberto o cartão, a polícia inseriu o seu nome nos registos policiais como prostituta, uma profissão que ela negou constantemente possuir. A requerente pediu que a palavra «prostituta» fosse eliminada dos registos informáticos da polícia. O TEDH reconheceu, em princípio, que a conservação de dados pessoais com fundamento na possibilidade de a pessoa em causa cometer outro crime poderá, em certos casos, ser proporcional. Porém, no caso da requerente, a alegação de exercício ilegal da prostituição parecia demasiado vaga e genérica, não se fundamentava em factos concretos

113 TEDH, acórdão *Peck c. Reino Unido* de 28 de janeiro de 2003, petição n.º 44647/98, especialmente n.º 85.

114 TEDH, acórdão *Leander c. Suécia* de 11 de julho de 1985, petição n.º 9248/81, n.º 58.

115 TEDH, acórdão *Khelili c. Suíça* de 18 de outubro de 2011, petição n.º 16188/07.

dado que ela nunca tinha sido condenada pela prática desse crime e, como tal, não podia ser considerada uma resposta a uma «necessidade social imperiosa» na aceção do artigo 8.º da CEDH. Considerando que competia às autoridades provar a exatidão dos dados armazenados sobre a requerente e tendo em conta a gravidade da ingerência no exercício dos direitos da mesma, o TEDH entendeu que a manutenção da palavra «prostituta» nos arquivos policiais durante anos não tinha sido necessária numa sociedade democrática. O TEDH concluiu que tinha havido uma violação do artigo 8.º da CEDH.

Exemplo: No acórdão *Leander c. Suécia*,[116] o TEDH considerou que a investigação secreta de pessoas que se candidatavam a cargos importantes para a segurança nacional não era, enquanto tal, contrária ao requisito da necessidade numa sociedade democrática. Perante as garantias especiais estabelecidas no direito nacional para proteger os interesses da pessoa em causa – por exemplo, controlos exercidos pelo Parlamento e pelo Chanceler da Justiça , o TEDH concluiu que o sistema sueco de controlo do pessoal cumpria os requisitos do artigo 8.º, n.º 2, da CEDH. Tendo em conta a larga margem de apreciação ao seu dispor, o Estado demandado podia considerar que, no caso do requerente, os interesses de segurança nacional prevaleciam sobre os interesses individuais. O TEDH concluiu que não tinha havido uma violação do artigo 8.º da CEDH.

3.1.2. As condições do estabelecimento de restrições lícitas ao abrigo da Carta da UE

A estrutura e a redação da Carta e da CEDH são diferentes. Embora não mencione ingerências no exercício de direitos garantidos, a Carta contém uma disposição sobre restrições ao exercício dos direitos e liberdades por ela reconhecidos.

De acordo com o artigo 52.º, n.º 1, as restrições ao exercício dos direitos e liberdades reconhecidos pela Carta e, consequentemente, ao exercício do direito à proteção de dados pessoais, tal como o tratamento de dados pessoais, só são admissíveis se:

- forem previstas por lei;
- respeitarem o conteúdo essencial do direito à proteção de dados;
- forem necessárias, na observância do princípio da proporcionalidade; e

116 TEDH, acórdão *Leander c. Suécia* de 11 de julho de 1985, petição n.º 9248/81, n.º 59 e 67.

- corresponderem a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros.

Exemplos: No acórdão *Volker und Markus Schecke*,[117] o TJUE concluiu que, ao imporem a obrigação de publicar dados pessoais relativos a cada pessoa singular beneficiária de ajudas de [certos fundos agrícolas] sem fazer distinções em função de critérios pertinentes, como os períodos durante os quais receberam essas ajudas, a sua frequência ou ainda o tipo ou a importância das mesmas, o Conselho e a Comissão tinham excedido os limites impostos pelo princípio da proporcionalidade.

Por conseguinte, o TJUE considerou que era necessário declarar a invalidade de certas disposições do Regulamento (CE) n.º 1290/2005 do Conselho e de declarar a invalidade total do Regulamento n.º 259/2008.[118]

Apesar da redação ser diferente, as condições de licitude do tratamento previstas no artigo 52.º, n.º 1, da Carta evocam o artigo 8.º, n.º 2, da CEDH. Com efeito, deve considerarse que as condições enumeradas no artigo 52.º, n.º 1, da Carta cumprem as condições estipuladas no artigo 8.º, n.º 2, da CEDH, dado que o artigo 52.º, n.º 3, da Carta refere, no primeiro período, que, «[n]a medida em que a presente Carta contenha direitos correspondentes aos direitos garantidos pela Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, o sentido e o âmbito desses direitos são iguais aos conferidos por essa Convenção.»

Porém, nos termos do último período do artigo 52.º, n.º 3, «[e]sta disposição não obsta a que o direito da União confira uma proteção mais ampla.» No contexto da comparação entre o artigo 8.º, n.º 2, da CEDH e o primeiro período do artigo 52.º, n.º 3, a única conclusão possível é a de que os requisitos de justificação da ingerência nos termos do artigo 8.º, n.º 2, da CEDH correspondem aos requisitos mínimos para o estabelecimento de restrições lícitas ao direito de proteção dos dados nos termos da Carta. Consequentemente, para que o tratamento de dados pessoais seja

117 TJUE, acórdão de 9 de novembro de 2010 nos processos apensos C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen*, n.ºs 89 e 86.

118 Regulamento (CE) n.º 1290/2005 do Conselho, de 21 de junho de 2005, relativo ao financiamento da política agrícola comum, JO 2005 L 209; Regulamento (CE) n.º 259/2008 da Comissão, de 18 de março de 2008, que estabelece as regras de execução do Regulamento (CE) n.º 1290/2005 do Conselho no que respeita à publicação de informação sobre os beneficiários de fundos provenientes do Fundo Europeu Agrícola de Garantia (FEAGA) e do Fundo Europeu Agrícola de Desenvolvimento Rural (Feader), JO 2008 L 76.

considerado lícito ao abrigo do direito da UE, é necessário que, pelo menos, as condições do artigo 8.º, n.º 2, da CEDH estejam preenchidas; no entanto, o direito da UE poderá estabelecer requisitos adicionais para casos específicos.

A correspondência entre o princípio do tratamento lícito nos termos do direito da UE e as disposições relevantes da CEDH é reforçada pelo artigo 6.º, n.º 3, do Tratado UE, que estabelece que «[d]o direito da União fazem parte, enquanto princípios gerais, os direitos fundamentais tal como os garante a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais».

3.2. O princípio da especificação e da limitação da finalidade

Pontos-chave

- A finalidade do tratamento de dados tem de estar visivelmente definida antes das operações de tratamento terem início.
- Nos termos do direito da UE, a finalidade do tratamento tem de estar especificamente definida; o direito do CdE deixa esta questão ao critério do legislador nacional.
- O tratamento para finalidades indeterminadas não cumpre a legislação sobre proteção de dados.
- A utilização posterior dos dados para uma finalidade incompatível com a finalidade original exige outra base legal.
- A transferência de dados para terceiros constitui uma nova finalidade que exige uma outra base legal.

Essencialmente, o princípio da especificação e da limitação da finalidade significa que a legitimidade do tratamento de dados pessoais dependerá da finalidade do tratamento.[119] Essa finalidade deverá ter sido especificada e claramente comunicada pelo responsável pelo tratamento antes do início do tratamento de dados.[120] No âmbito do **direito da UE**, esta comunicação deverá ter lugar por meio de uma declaração ou, por outras palavras, de uma notificação, à autoridade de controlo compe-

119 Convenção 108, artigo 5.º, al. b); Diretiva Proteção de Dados, artigo 6.º, n.º 1, al. b).

120 Ver também Grupo de Trabalho do artigo 29.º (2013), *Parecer 03/2013 sobre a limitação da finalidade*, WP 203, Bruxelas, 2 de abril de 2013.

tente ou, pelo menos, através de documentação interna, que deverá ser disponibilizada pelo responsável pelo tratamento às autoridades de controlo para inspeção e à pessoa em causa para consulta.

O tratamento de dados pessoais para finalidades indeterminadas e/ou ilimitadas é ilícito.

Sempre que os dados forem tratados para uma nova finalidade, é necessária uma base legal específica, sendo irrelevante o facto de os dados terem sido inicialmente adquiridos ou tratados para outra finalidade legítima. Por seu lado, o tratamento legítimo restringese à finalidade inicialmente especificada, pelo que qualquer nova finalidade do tratamento exigirá uma base legal autónoma. A divulgação de dados a terceiros terá de ser ponderada com especial cuidado, uma vez que a divulgação constitui habitualmente uma nova finalidade e, por conseguinte, exige uma base legal distinta da base legal para a recolha dos dados.

Exemplo: Uma companhia aérea recolhe dados dos seus passageiros para efetuar reservas, com vista a assegurar a correta operação do voo. A companhia aérea necessitará de dados sobre: os números dos lugares dos passageiros; limitações físicas especiais, tais como necessidade de uma cadeira de rodas; e requisitos alimentares especiais, tais como alimentos kosher ou halal. Se for pedido às companhias aéreas que transfiram esses dados (contidos no PNR) para as autoridades de imigração no aeroporto de destino, esses dados estarão a ser utilizados para fins de controlo da imigração, que são diferentes da finalidade para que foram inicialmente recolhidos. Como tal, a transferência desses dados para uma autoridade de imigração exigirá uma base legal autónoma.

Na definição do âmbito e dos limites de uma determinada finalidade, a Convenção 108 e a Diretiva de Proteção de Dados recorrem ao conceito de compatibilidade: a utilização de dados para finalidades compatíveis é permitida com fundamento na base legal inicial. O conceito de «compatível», porém, não está definido, devendo ser interpretado caso a caso.

Exemplo: A venda dos dados dos clientes da empresa Sunshine, que foram adquiridos no âmbito da gestão do relacionamento com os clientes (CRM), a uma empresa de marketing direto, a Moonlight, que pretende utilizar estes dados para apoiar as campanhas de marketing de empresas terceiras, é uma finalidade nova, que é incompatível com a CRM, a finalidade inicial da recolha

de dados dos clientes pela Sunshine. Consequentemente, a venda de dados à empresa Moonlight necessita da sua própria base legal.

Em contrapartida, a utilização de dados de CRM pela empresa Sunshine para as suas próprias finalidades de marketing que consiste em enviar mensagens de marketing sobre os seus próprios produtos para os seus próprios clientes – é normalmente aceite como uma finalidade compatível.

A Diretiva de Proteção de Dados declara expressamente que o «tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-membros estabeleçam garantias adequadas».[121]

Exemplos: A empresa Sunshine recolheu e armazenou dados de CRM sobre os seus clientes. A utilização posterior destes dados pela empresa Sunshine para fins de análise estatística do comportamento de compra dos seus clientes é admissível, uma vez que as estatísticas são fins compatíveis. Não é necessária outra base legal, nomeadamente o consentimento das pessoas em causa.

Se esses dados fossem transmitidos a um terceiro, a empresa Starlight, para fins exclusivamente estatísticos, essa transmissão seria admissível sem necessidade de uma nova base legal, mas apenas sob a condição de terem sido estabelecidas garantias adequadas, tais como a dissimulação da identidade das pessoas em causa, uma vez que a identidade não é geralmente necessária para fins estatísticos.

3.3. Princípios relativos à qualidade dos dados

Pontos-chave

- O responsável pelo tratamento tem de aplicar os princípios relativos à qualidade dos dados em todas as operações de tratamento.

121 Um exemplo deste tipo de disposições nacionais é a Lei da Proteção de Dados austríaca (*Datenschutzgesetz*), Jornal Oficial I n.º 165/1999, n.º 46, disponível em inglês em: www.dsk.gv.at/DocView.axd?CobId=41936.

- O princípio da limitação da conservação dos dados exige que os dados sejam apagados logo que deixem de ser necessários para as finalidades para que foram recolhidos.
- As derrogações ao princípio da limitação da conservação dos dados têm de ser estabelecidas por lei e exigem garantias especiais para assegurar a proteção dos titulares dos dados.

3.3.1. O princípio da pertinência dos dados

Apenas serão objeto de tratamento os dados que forem «adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente».[122] As categorias de dados escolhidas para tratamento têm de ser necessárias à concretização do objetivo geral das operações de tratamento que foi comunicado e o responsável pelo tratamento deve restringir rigorosamente a recolha de dados às informações que sejam diretamente pertinentes para a finalidade específica prosseguida pelo tratamento.

Na sociedade contemporânea, o princípio da pertinência dos dados implica a ponderação de um outro aspeto: o recurso a tecnologias especiais de proteção da privacidade permite, por vezes, evitar a utilização de quaisquer dados pessoais ou utilizar dados pseudonimizados, o que constitui uma solução que promove o respeito pela privacidade. Esta é uma solução particularmente desejável em sistemas de tratamento mais vastos.

Exemplo: Uma câmara municipal oferece um cartão com chip («passe») a utilizadores regulares do sistema municipal de transportes públicos mediante o pagamento de uma determinada importância. O cartão contém o nome do utilizador em forma escrita na face do cartão e em forma eletrónica no chip. Sempre que utiliza o autocarro ou o elétrico, o passageiro tem de passar o cartão por um dispositivo de leitura instalado no autocarro ou elétrico. Os dados lidos pelo dispositivo são eletronicamente comparados com uma base de dados com os nomes das pessoas que compraram o passe.

Este sistema não cumpre da melhor forma o princípio da pertinência: para verificar se uma pessoa está ou não autorizada a utilizar determinados meios de transporte, não é necessário comparar os dados pessoais constantes do chip do cartão com uma base de dados. Bastaria, por exemplo, incluir uma imagem

122 Convenção 108, artigo 5.º, al. c); Diretiva Proteção de Dados, artigo 6.º, n.º 1, al. c).

eletrónica especial, como um código de barras, no chip do cartão, que o passageiro passaria em frente do dispositivo de leitura para confirmar se o cartão era ou não válido. Este sistema não registaria o nome dos utilizadores, o transporte utilizado ou a hora da utilização. Não seriam recolhidos quaisquer dados pessoais, o que é a solução ideal em termos do princípio da pertinência, uma vez que um dos seus corolários é a obrigação de minimizar a recolha de dados.

3.3.2. O princípio da exatidão dos dados

Um responsável pelo tratamento que tenha em seu poder informações pessoais não deverá utilizar essas informações sem tomar medidas para se certificar, com um grau de certeza razoável, que os dados são exatos e estão atualizados.

A obrigação de assegurar a exatidão dos dados tem de ser interpretada no contexto da finalidade do tratamento dos dados.

Exemplo: Uma empresa de comercialização de mobiliário recolheu dados sobre a identidade e a morada de um cliente para fins de faturação. Seis meses depois, esta empresa pretende lançar uma campanha de marketing e deseja contactar antigos clientes. Para tal, a empresa pretende ter acesso ao registo de residentes nacionais, que conterá provavelmente moradas atualizadas, dado que os residentes estão obrigados por lei a comunicar a sua atual morada ao registo. Apenas têm acesso aos dados deste registo as pessoas e entidades que apresentem uma justificação válida para tal.

Nesta situação, a empresa não pode utilizar o argumento de que está obrigada a manter a exatidão e atualidade dos dados para fundamentar o seu direito a consultar o registo de residentes a fim de recolher novos dados sobre a morada de todos os seus antigos clientes. Os dados foram recolhidos para fins de faturação; neste caso, é relevante a morada à data da venda. Não existe qualquer base legal para recolher novos dados sobre a morada, uma vez que o marketing não é um interesse que prevaleça sobre o direito à proteção de dados e, como tal, não pode justificar o acesso aos dados constantes do registo.

Poderão existir também casos em que a atualização de dados armazenados seja proibida por lei porque a finalidade do armazenamento dos dados é principalmente documentar acontecimentos.

Exemplo: Os protocolos de cirurgia não podem ser alterados (por outras palavras, «atualizados»), ainda que as conclusões neles mencionadas posteriormente se revelem incorretas. Nesses casos, apenas serão admissíveis aditamentos às observações constantes do protocolo, desde que seja claramente indicado que constituem contributos efetuados numa fase posterior.

Por outro lado, existem situações em que o controlo regular da exatidão dos dados, incluindo a sua atualização, é uma necessidade absoluta devido aos potenciais danos que a pessoa em causa poderá sofrer se os dados não forem exatos.

Exemplo: Se uma pessoa quiser fazer um contrato com uma instituição bancária, o banco verifica geralmente a situação financeira do potencial cliente. Para tal, existem bases de dados especiais que contêm dados sobre o historial de crédito de pessoas singulares. Se essa base de dados contiver dados incorretos ou desatualizados sobre uma pessoa, esta poderá enfrentar sérios problemas. Por este motivo, os responsáveis pelo tratamento dessas bases de dados têm de envidar esforços especiais para cumprir o princípio da exatidão dos dados.

Além disso, é permitida a recolha e o armazenamento de dados que não digam respeito a factos, mas sim a suspeitas, tal como nos inquéritos criminais, desde que o responsável pelo tratamento disponha de uma base legal para recolher essas informações e essa suspeita seja suficientemente justificada.

3.3.3. O princípio da limitação da conservação dos dados

Tanto o artigo 6.º, n.º 1, alínea e), da Diretiva de Proteção de Dados como o artigo 5.º, alínea e), da Convenção 108 exigem que os Estados-Membros assegurem que os dados pessoais sejam «conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente.» Assim, os dados têm de ser apagados quando essas finalidades forem atingidas.

No acórdão *S. e Marper,* o TEDH concluiu que os princípios nucleares dos instrumentos relevantes do Conselho da Europa, bem como a lei e a prática de outras Partes

Contratantes, exigem que a conservação dos dados seja proporcional à finalidade da recolha e limitada no tempo, especialmente no setor policial.[123]

Porém, a limitação temporal do armazenamento de dados pessoais só é aplicável aos dados conservados sob uma forma que permita a identificação das pessoas em causa. Deste modo, é possível armazenar licitamente dados que já não sejam necessários mediante a sua anonimização ou pseudonimização.

A conservação de dados para fins científicos, históricos ou estatísticos constitui uma derrogação ao princípio da limitação da conservação dos dados expressamente prevista na Diretiva de Proteção de Dados.[124] Contudo, a continuação do armazenamento e utilização de dados pessoais nestes casos deve ser acompanhada por garantias especiais estabelecidas no direito nacional.

3.4. O princípio do tratamento leal

Pontos-chave

- O tratamento leal significa que o tratamento tem de ser transparente, especialmente em relação às pessoas em causa.
- Os responsáveis pelo tratamento são obrigados a informar as pessoas em causa pelo menos sobre a finalidade do tratamento e sobre a sua própria identidade e morada antes do tratamento dos seus dados.
- Salvo nos casos expressamente permitidos por lei, é proibido o tratamento secreto e dissimulado de dados pessoais.
- As pessoas em causa têm direito de acesso aos seus dados sempre que estes forem objeto de tratamento.

O princípio do tratamento leal regula, acima de tudo, a relação entre o responsável pelo tratamento e o titular dos dados.

123 TEDH, acórdão *S. e Marper c. Reino Unido* de 4 de dezembro de 2008, petições n.ºs 30562/04 e 30566/04; ver também, por exemplo, TEDH, acórdão *M.M. c. Reino Unido* de 13 de novembro de 2012, petição n.º 24029/07.

124 Diretiva Proteção de Dados, artigo 6.º, n.º 1, al. e).

3.4.1. Transparência

Este princípio impõe sobre o responsável pelo tratamento a obrigação de manter as pessoas em causa informadas sobre o modo como os seus dados estão a ser utilizados.

> Exemplo: No processo que deu origem ao acórdão *Haralambie c. Roménia*,[125] o requerente requereu o acesso ao processo que os serviços secretos tinham conservado sobre ele, mas o seu pedido só foi deferido cinco anos depois. O TEDH reiterou que as pessoas que eram objeto de processos individuais detidos pelas autoridades públicas tinham um interesse vital em aceder aos mesmos. As autoridades tinham o dever de estabelecer um procedimento eficaz para obter acesso àquelas informações. O TEDH considerou que nem a quantidade de processos transferidos, nem as deficiências do sistema de arquivo justificavam um atraso de cinco anos no deferimento do pedido de acesso do requerente ao seu processo. As autoridades não tinham colocado à disposição do requerente um procedimento eficaz e acessível que lhe permitisse obter acesso ao seu processo individual dentro de um prazo razoável. O TEDH concluiu que tinha havido uma violação do artigo 8.º da CEDH.

As operações de tratamento têm de ser explicadas de forma facilmente acessível às pessoas em causa, a fim de garantir que estas compreendem o que irá acontecer aos seus dados. As pessoas em causa também têm o direito de ser informadas pelo responsável pelo tratamento, caso o solicitem, se os seus dados estão a ser tratados e, em caso afirmativo, que dados estão a ser tratados.

3.4.2. Criar uma relação de confiança

Os responsáveis pelo tratamento devem documentar o modo como se propõem tratar os dados de forma lícita e transparente e colocar esses documentos à disposição das pessoas em causa e do público em geral. As operações de tratamento não podem ser realizadas em segredo e não devem ter efeitos negativos imprevistos. Os responsáveis pelo tratamento devem certificarse de que os clientes ou cidadãos são informados sobre a utilização dos seus dados. Os responsáveis pelo tratamento devem ainda, na medida do possível, atuar de forma a cumprir prontamente os desejos da pessoa em causa, especialmente quando a base legal do tratamento de dados for o seu consentimento.

125 TEDH, acórdão *Haralambie c. Roménia* de 27 de outubro de 2009, petição n.º 21737/03.

Exemplo: No processo que deu origem ao acórdão *K.H. e outros c. Eslováquia*,[126] as autoras da petição eram oito mulheres de etnia cigana que tinham sido tratadas em dois hospitais na região ocidental da Eslováquia durante a gravidez e o parto. Depois disso, nenhuma delas conseguia engravidar, não obstante o terem tentado repetidamente. Os tribunais nacionais ordenaram aos hospitais que autorizassem as autoras da petição e os seus representantes a consultar e a transcrever manualmente excertos dos registos médicos, mas negaram provimento ao pedido de fotocopiar os documentos, alegadamente para evitar que fossem danificados. As obrigações positivas dos Estados ao abrigo do artigo 8.º da CEDH abrangem necessariamente a obrigação de disponibilizar às pessoas em causa cópias dos seus ficheiros de dados. Cabia ao Estado estabelecer providências para a fotocópia dos ficheiros de dados pessoais ou, se fosse o caso, apresentar argumentos convincentes que justificassem o indeferimento do pedido. No caso das autoras da petição, os tribunais nacionais justificaram a proibição de fotocopiar os registos médicos essencialmente com base na necessidade de proteger contra danos as informações relevantes. No entanto, o TEDH não compreendia como é que as autoras da petição, que tinham tido já acesso a todo o processo clínico, poderiam ter danificado as informações que lhes diziam respeito. Além disso, esse risco poderia ter sido evitado por outros meios, nomeadamente limitando os grupos de pessoas com acesso ao processo. O Estado não demonstrou a existência de motivos suficientemente convincentes para negar o acesso efetivo das autoras da petição a informações sobre a sua saúde. O TEDH concluiu que tinha havido uma violação do artigo 8.º.

No que respeita aos serviços de Internet, as funcionalidades dos sistemas de tratamento de dados devem permitir às pessoas em causa compreender verdadeiramente o que está a acontecer com os seus dados.

O princípio do tratamento leal significa ainda que os responsáveis pelo tratamento estão preparados para ir além dos requisitos legais mínimos obrigatórios, caso os legítimos interesses da pessoa em causa assim o exijam.

126 TEDH, acórdão *K.H. e outros c. Eslováquia* de 6 de novembro de 2009, petição n.º 32881/04.

3.5. O princípio da responsabilidade

Pontos-chave

- A responsabilidade exige a implementação ativa de medidas pelos responsáveis pelo tratamento para promoverem e salvaguardarem a proteção de dados nas suas atividades de tratamento.
- Compete aos responsáveis pelo tratamento assegurar a conformidade das suas operações de tratamento com a legislação sobre proteção de dados.
- Os responsáveis pelo tratamento devem estar em condições de demonstrar, a todo o tempo, a conformidade com as disposições sobre proteção de dados às pessoas em causa, ao público em geral e às autoridades de controlo.

Em 2013, a Organização para a Cooperação e Desenvolvimento Económico (OCDE) adotou diretrizes sobre a privacidade que salientam a importância do papel que os responsáveis pelo tratamento desempenham para garantir, na prática, a eficácia da proteção de dados. De acordo com essas diretrizes, o princípio da responsabilidade significa que o responsável pelo tratamento de dados deve ser responsável pelo cumprimento de medidas que concretizem os princípios materiais nelas enunciados.[127]

Enquanto a Convenção 108 não faz qualquer referência à responsabilidade dos responsáveis pelo tratamento, deixando essencialmente esta questão ao critério do legislador nacional, o artigo 6.º, n.º 2, da Diretiva de Proteção de Dados estabelece que incumbe ao responsável pelo tratamento assegurar a observância dos princípios relacionados com a qualidade dos dados enunciados no n.º 1.

Exemplo: A alteração de 2009[128] à Diretiva 2002/58/CE (*Diretiva Privacidade Eletrónica*) constitui um exemplo legislativo que salienta o princípio da responsabilidade. De acordo com o artigo 4.º na redação em vigor, a Diretiva impõe a

127 OCDE (2013), *Guidelines governing the protection of privacy and transborder flows of personal data* (Diretrizes aplicáveis à proteção da privacidade e aos fluxos transfronteiriços de dados pessoais), artigo 14.º.

128 Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor, JO 2009 L 337, p. 11.

obrigação de aplicar uma política de segurança, mais concretamente de garantir «a aplicação de uma política de segurança relativa ao tratamento dos dados pessoais». Deste modo, no que respeita às disposições sobre segurança da referida Diretiva, o legislador considerou que era necessário estabelecer expressamente a obrigação de possuir e aplicar uma política de segurança.

Segundo o parecer do Grupo de Trabalho do artigo 29.º,[129] a essência do princípio da responsabilidade é a obrigação que recai sobre o responsável pelo tratamento de:

- colocar em prática medidas que, em circunstâncias normais, garantiriam a observância das regras sobre proteção de dados no contexto das operações de tratamento; e

- estar em condições de disponibilizar rapidamente às pessoas em causa e às autoridades de controlo documentação que comprove as medidas adotadas para garantir a observância das regras sobre proteção de dados.

O princípio da responsabilidade exige, assim, que os responsáveis pelo tratamento demonstrem ativamente o cumprimento, não se limitando a aguardar que as pessoas em causa ou as autoridades de controlo apontem deficiências.

129 Grupo de Trabalho do artigo 29.º, *Parecer 3/2010 sobre o princípio da responsabilidade*, WP 173, Bruxelas, 13 de julho de 2010.

4

As regras da legislação europeia sobre proteção de dados

UE	Questões abrangidas	CdE
Regras sobre o tratamento lícito de dados não sensíveis		
Diretiva de Proteção de Dados, artigo 7.º, al. a)	Consentimento	Recomendação sobre a definição de perfis, artigos 3.4, al. b) e 3.6
Diretiva de Proteção de Dados, artigo 7.º, al. b)	Relação (pré) contratual	Recomendação sobre a definição de perfis, artigo 3.4, al. b)
Diretiva de Proteção de Dados, artigo 7.º, al. c)	Deveres legais do responsável pelo tratamento	Recomendação sobre a definição de perfis, artigo 3.4, al. a)
Diretiva de Proteção de Dados, artigo 7.º, al. d)	Interesses vitais da pessoa em causa	Recomendação sobre a definição de perfis, artigo 3.4, al. b)
Diretiva de Proteção de Dados, artigo 7.º, al. e) e artigo 8.º, n.º 4 TJUE, acórdão de 16 de dezembro de 2008 no processo C-524/06, *Huber/Alemanha*	Interesse público e exercício de autoridade pública	Recomendação sobre a definição de perfis, artigo 3.4, al. b)
Diretiva de Proteção de Dados, artigo 7.º, alínea f) e artigo 8.º, n.ºs 2 e 3 TJUE, acórdão de 24 de novembro de 2011 nos processos apensos C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD)/ Administración del Estado*	Interesses legítimos de terceiros	Recomendação sobre a definição de perfis, artigo 3.4, al. b)

UE	Questões abrangidas	CdE
Regras sobre o tratamento lícito de dados sensíveis		
Diretiva de Proteção de Dados, artigo 8.º, n.º 1	Proibição geral de tratamento	Convenção 108, artigo 6.º
Diretiva de Proteção de Dados, artigo 8.º, n.ºs 2 a 4	Derrogações à proibição geral	Convenção 108, artigo 6.º
Diretiva de Proteção de Dados, artigo 8.º, n.º 5	Tratamento de dados sobre condenações (penais)	Convenção 108, artigo 6.º
Diretiva de Proteção de Dados, artigo 8.º, n.º 7	Tratamento de números de identificação	
Regras sobre a segurança do tratamento		
Diretiva de Proteção de Dados, artigo 17.º	Obrigação de garantir a segurança do tratamento	Convenção 108, artigo 7.º TEDH, acórdão *I. c. Finlândia* de 17 de julho de 2008, petição n.º 20511/03
Diretiva Privacidade Eletrónica, artigo 4.º, n.º 2	Notificações de violação de dados pessoais	
Diretiva de Proteção de Dados, artigo 16.º	Obrigação de confidencialidade	
Regras sobre a transparência do tratamento		
	Transparência em geral	Convenção 108, artigo 8.º, al. a)
Diretiva de Proteção de Dados, artigos 10.º e 11.º	Informação	Convenção 108, artigo 8.º, al. a)
Diretiva de Proteção de Dados, artigos 10.º e 11.º	Derrogações à obrigação de informar	Convenção 108, artigo 9.º
Diretiva de Proteção de Dados, artigos 18.º e 19.º	Notificação	Recomendação sobre a definição de perfis, artigo 9.2, al. a)
Regras sobre a promoção do cumprimento		
Diretiva de Proteção de Dados, artigo 20.º	Controlo prévio	
Diretiva de Proteção de Dados, artigo 18.º, n.º 2	Encarregado da proteção de dados pessoais	Recomendação sobre a definição de perfis, artigo 8.3
Diretiva de Proteção de Dados, artigo 27.º	Códigos de conduta	

Os princípios têm necessariamente natureza geral. A sua aplicação a situações concretas deixa uma certa margem de interpretação e escolha quanto aos meios. Nos termos do **direito do CdE**, cabe às Partes da Convenção 108 clarificar esta margem de interpretação no seu direito nacional. A situação no **direito da UE** é diferente: para implementar a proteção de dados no mercado interno, foi considerado necessário definir logo regras mais detalhadas ao nível da UE, a fim de harmonizar o nível de proteção de dados conferido pela legislação nacional dos Estados-Membros. A Diretiva de Proteção de Dados estabelece, ao abrigo dos princípios enunciados no seu artigo 6.º uma série de regras detalhadas que têm de ser fielmente implementadas no direito nacional. Por conseguinte, as observações que se seguem sobre regras detalhadas de proteção de dados ao nível europeu respeitam predominantemente ao direito da UE.

4.1. Regras sobre o tratamento lícito

Pontos-chave

- Os dados pessoais podem ser objeto de um tratamento lícito se:
  - o tratamento se basear no consentimento do titular dos dados;
  - interesses vitais do titular dos dados exigirem o tratamento dos seus dados; ou
  - interesses legítimos de terceiros forem a razão do tratamento, mas apenas se não prevalecer o interesse na proteção de direitos fundamentais dos titulares dos dados.
- O tratamento lícito de dados sensíveis está sujeito a um regime especial, mais rigoroso.

A Diretiva de Proteção de Dados estabelece dois grupos de regras distintos para o tratamento lícito de dados: um para dados não sensíveis no artigo 7.º e outro para dados sensíveis no artigo 8.º.

4.1.1. Tratamento lícito de dados não sensíveis

O capítulo II da Diretiva 95/46, sob a epígrafe «Condições gerais de licitude do tratamento de dados pessoais», estabelece que, sem prejuízo das derrogações admitidas ao abrigo do artigo 13.º, qualquer tratamento de dados pessoais deve ser conforme, em primeiro lugar, aos princípios relativos à qualidade dos dados enunciados no artigo 6.º da Diretiva de Proteção de Dados e, em segundo lugar, a um dos princípios

relativos à legitimidade do tratamento de dados, enumerados no artigo 7.º[130] Estas disposições descrevem os casos de tratamento legítimo de dados pessoais não sensíveis.

Consentimento

Relativamente ao **direito do CdE**, o consentimento não é mencionado no artigo 8.º da CEDH nem na Convenção 108. No entanto, é referido na jurisprudência do TEDH e em várias recomendações do CdE. Quanto ao **direito da UE**, o consentimento está firmemente estabelecido no artigo 7.º, al. a), da Diretiva de Proteção de Dados como base para o tratamento legítimo de dados, sendo também expressamente mencionado no artigo 8.º da Carta.

Relação contratual

Outra base para o tratamento legítimo de dados pessoais nos termos do **direito da UE**, enumerada no artigo 7.º, alínea b), da Diretiva de Proteção de Dados, é a sua necessidade «para a execução de um contrato no qual a pessoa em causa é parte». Esta disposição também abrange as relações précontratuais. Por exemplo: uma parte pretende celebrar um contrato, mas ainda não o fez, possivelmente porque ainda é necessário verificar alguns factos. Se uma parte precisar de tratar dados para este fim, esse tratamento é legítimo desde que seja necessário para a execução de «diligências prévias à formação do contrato decididas a pedido da pessoa em causa».

No que respeita ao **direito do CdE**, «a proteção dos direitos e das liberdades de terceiros» é mencionada no artigo 8.º, n.º 2, da CEDH como um dos fundamentos da ingerência legítima no exercício do direito à proteção de dados.

Deveres legais do responsável pelo tratamento

O **direito da UE** menciona expressamente outro princípio relativo à legitimidade do tratamento de dados: se «for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito» (artigo 7.º, alínea c), da Diretiva de

130 TJUE, acórdão de 20 de maio de 2003 nos processos apensos C-465/00, C-138/01 e C-139/01, *Österreichischer Rundfunk e o.*, n.º 65; TJUE, acórdão de 16 de dezembro de 2008 no processo C524/06, *Huber/Alemanha*, n.º 48; TJUE, acórdão de 24 de novembro de 2011 nos processos apensos C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, n.º 26.

Proteção de Dados). Esta disposição diz respeito aos responsáveis pelo tratamento no setor privado; às obrigações legais dos responsáveis pelo tratamento no setor público é aplicável o artigo 7.º, alínea e), da Diretiva. Há muitos casos em que os responsáveis pelo tratamento do setor privado são obrigados, por lei, a tratar dados sobre terceiros; por exemplo, os médicos e os hospitais têm o dever legal de armazenar dados sobre o tratamento dos doentes durante vários anos, os empregadores têm de tratar dados sobre os seus funcionários para fins de segurança social e impostos e as empresas têm de tratar dados sobre os seus clientes para fins de impostos.

No contexto da transferência obrigatória de dados dos passageiros pelas companhias aéreas para autoridades estrangeiras de controlo da imigração, foi suscitada a questão da possibilidade de as obrigações legais estabelecidas no direito *estrangeiro* constituírem uma base legítima para o tratamento de dados nos termos do direito da UE (esta questão é analisada em maior detalhe na secção 6.2).

As obrigações legais do responsável pelo tratamento também constituem uma base para o tratamento legítimo de dados nos termos do **direito do CdE**. Tal como salientado anteriormente, as obrigações legais de um responsável pelo tratamento do setor privado restringemse ao caso específico dos interesses legítimos de terceiros, conforme mencionado no artigo 8.º, n.º 2, da CEDH. Por conseguinte, o exemplo acima apresentado também é relevante para o direito do CdE.

Interesses vitais do titular dos dados

No âmbito do **direito da UE**, o artigo 7.º, alínea d), da Diretiva de Proteção de Dados estabelece que o tratamento de dados pessoais é lícito se «for necessário para a proteção de interesses vitais da pessoa em causa». Estes interesses, que estão intimamente ligados à sobrevivência da pessoa em causa, poderiam constituir a base para a utilização legítima de dados sobre a saúde ou de dados sobre pessoas desaparecidas, por exemplo.

No âmbito do **direito do CdE**, os interesses vitais do titular dos dados não são mencionados no artigo 8.º da CEDH como fundamento da ingerência legítima no exercício do direito à proteção de dados. No entanto, algumas recomendações do CdE que complementam a Convenção 108 em domínios específicos mencionam expressamente os interesses vitais da pessoa em causa como base para o tratamento

legítimo de dados.[131] Evidentemente, os interesses vitais da pessoa em causa são considerados implicitamente incluídos no conjunto de razões que justificam o tratamento de dados: a proteção de direitos fundamentais nunca deve colocar em risco os interesses vitais da pessoa protegida.

Interesse público e exercício de autoridade pública

Uma vez que existem muitos sistemas de organização dos assuntos públicos, o artigo 7.º, alínea e), da Diretiva de Proteção de Dados estabelece que o tratamento de dados pessoais será lícito se «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 [...]».[132]

Exemplo: No processo que deu origem ao acórdão *Huber/Alemanha*,[133] H. Huber, um nacional austríaco residente na Alemanha, pediu ao Serviço Federal para as Migrações e os Refugiados que suprimisse do Registo Central de Estrangeiros («o AZR») os dados que lhe diziam respeito. Este registo, que contém dados pessoais sobre nacionais de outros países da UE que sejam residentes na Alemanha por um período superior a três meses, é utilizado para fins estatísticos e pelas autoridades policiais e judiciárias no âmbito da investigação e ação penal relativamente a atividades criminosas ou que constituam uma ameaça à segurança pública. O órgão jurisdicional de reenvio perguntou se o tratamento de dados pessoais realizado num registo como o Registo Central de Estrangeiros, a que também têm acesso outras autoridades públicas, é compatível com o direito da UE na medida em que não existe um registo semelhante para nacionais alemães.

O TJUE refere, em primeiro lugar, que, nos termos do artigo 7.º, alínea e), da Diretiva, o tratamento de dados pessoais só é lícito se for necessário para a execução de uma missão de interesse público ou o exercício de uma autoridade pública.

Segundo o Tribunal de Justiça, «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 [...] não pode ter um

131 Recomendação sobre a definição de perfis, artigo 3.4, al. b).

132 Ver também Diretiva Proteção de Dados, considerando 32.

133 TJUE, acórdão de 16 de dezembro de 2008 no processo C-524/06, *Huber/Alemanha*.

conteúdo variável consoante o Estado-Membro. Logo, tratase 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».[134]

O Tribunal de Justiça chama a atenção para o facto de o direito de livre circulação de um cidadão da União no território de um Estado-Membro de que não é nacional não é incondicional, podendo estar sujeito a restrições e condições previstas no Tratado e nas disposições adotadas em sua aplicação. Por isso, embora a utilização de um registo como o AZR com a finalidade de dar apoio às autoridades encarregues da aplicação da legislação sobre o direito de residência seja, em princípio, legítima, esse registo só pode conter as informações que forem necessárias para essa finalidade específica. O Tribunal de Justiça conclui que um tal sistema de tratamento de dados pessoais cumpre o direito da UE se contiver unicamente os dados necessários à aplicação dessa legislação e se o seu caráter centralizado permitir uma aplicação mais eficaz dessa legislação. Compete ao órgão jurisdicional nacional verificar se essas condições estão preenchidas no caso concreto. Se a resposta for negativa, a conservação e o tratamento de dados pessoais num registo como o AZR para fins estatísticos não podem, em qualquer caso, ser considerados necessários na aceção do artigo 7.º, alínea e), da Diretiva 95/46/CE.[135]

Por último, relativamente à questão da utilização dos dados contidos no registo para fins de combate à criminalidade, o Tribunal de Justiça entende que este objetivo envolve necessariamente «a repressão dos crimes e delitos cometidos, independentemente da nacionalidade dos seus autores». O registo em causa não contém dados pessoais de nacionais do Estado-Membro em questão e esta diferença de tratamento constitui uma discriminação proibida pelo artigo 18.º do TFUE. Consequentemente, esta disposição, tal como interpretada pelo Tribunal de Justiça, «[opõese] à instauração, por um Estado-Membro, de um sistema de tratamento de dados pessoais específico para os cidadãos da União que não são nacionais desse Estado-Membro, com o objetivo de combater a criminalidade»[136]

134 *Ibid.*, n.º 52.

135 *Ibid.*, n.ºs 54, 58, 59, 66-68.

136 *Ibid.*, n.ºs 78 e 81.

A utilização de dados pessoais por autoridades que atuam na esfera pública também está sujeita ao artigo 8.º da CEDH.

Interesses legítimos prosseguidos pelo responsável pelo tratamento ou por um terceiro

A pessoa em causa não é a única com interesses legítimos. O artigo 7.º, alínea f), da Diretiva de Proteção de Dados estabelece que o tratamento de dados pessoais é lícito 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 ou os direitos e liberdades fundamentais da pessoa em causa, protegidos [...]».

No acórdão que se segue, o TJUE pronunciou-se expressamente sobre o artigo 7.º, alínea f), da Diretiva.

Exemplo: No acórdão *ASNEF e FECEMD*,[137] o TJUE esclareceu que o direito nacional não pode prever outras condições de licitude do tratamento de dados pessoais para além das previstas no artigo 7.º, alínea f), da Diretiva. Naquele processo, estava em causa uma disposição da legislação espanhola sobre proteção de dados nos termos da qual outros particulares só poderiam invocar um interesse legítimo no tratamento de dados pessoais se as informações constassem já de fontes acessíveis ao público.

Em primeiro lugar, o Tribunal de Justiça salientou que a Diretiva 95/46 visa tornar equivalente em todos os Estados-Membros o nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais. A aproximação das legislações nacionais aplicáveis nesta matéria não deve fazer diminuir a proteção que asseguram, devendo, pelo contrário, ter por objetivo assegurar um elevado nível de proteção na União.[138] Consequentemente, o TJUE concluiu que «decorre do objetivo que consiste em assegurar um alto nível de proteção equivalente em todos os Estados-Membros que o artigo 7.º da Diretiva 95/46 prevê uma lista exaustiva e taxativa dos casos em que um tratamento de dados pessoais pode ser considerado lícito». Além disso, «os

137 TJUE, acórdão de 24 de novembro de 2011 nos processos apensos C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) Administración del Estado*.

138 *Ibid*., n.º 28. Ver Diretiva Proteção de Dados, considerandos 8 e 10.

Estados-Membros não podem acrescentar novos princípios relativos à legitimação dos tratamentos de dados pessoais ao artigo 7.º da Diretiva 95/46 nem prever exigências suplementares que venham alterar o alcance de um dos seis princípios previstos nesse artigo.»[139] O Tribunal de Justiça admitiu que, [n]o que se refere à ponderação necessária por força do artigo 7.º, alínea f), da Diretiva 95/46/CE, é possível tomar em consideração o facto de que a gravidade da violação dos direitos fundamentais da pessoa em causa pelo referido tratamento pode variar em função da questão de saber se os dados já constam, ou não, de fontes acessíveis ao público.»

Contudo, «o artigo 7.º, alínea f), desta diretiva opõese a que um Estado-Membro exclua de forma categórica e generalizada a possibilidade de algumas categorias de dados pessoais serem tratadas, sem permitir uma ponderação dos direitos e interesses opostos em causa num caso específico.»

À luz destas considerações, o Tribunal de Justiça concluiu que «o artigo 7.º, alínea f), da Diretiva 95/46 deve ser interpretado no sentido de que se opõe a uma legislação nacional que, na inexistência do consentimento da pessoa em causa e para autorizar o tratamento dos seus dados pessoais necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, exige, além do respeito dos direitos e liberdades fundamentais dessa pessoa, que os referidos dados constem de fontes acessíveis ao público, excluindo assim de forma categórica e generalizada todo e qualquer tratamento de dados que não constem dessas fontes.»[140]

É possível encontrar formulações semelhantes em recomendações do CdE. A Recomendação sobre a definição de perfis considera legítimo o tratamento de dados pessoais para fins de definição de perfis, se tal for necessário para prosseguir interesses legítimos de terceiros, desde que não prevaleçam os direitos e liberdades fundamentais das pessoas em causa.[141]

139 TJUE, acórdão de 24 de novembro de 2011 nos processos apensos C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) Administración del Estado,* n.ºs 30 e 32.

140 *Ibid.*, n.ºs 40, 44, 48 e 49.

141 Recomendação sobre a definição de perfis, artigo 3.4, al. b).

4.1.2. Tratamento lícito de dados sensíveis

O **direito do CdE** deixa a cargo do legislador nacional a definição das medidas de proteção adequadas para a utilização de dados sensíveis, enquanto o **direito da UE**, no artigo 8.º da Diretiva de Proteção de Dados, estabelece um regime pormenorizado para o tratamento de categorias de dados que revelem: a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como dados relativos à saúde e à vida sexual. O tratamento de dados sensíveis é, em princípio, proibido.[142] No entanto, o artigo 8.º, n.ºs 2 e 3, da Diretiva contém uma lista taxativa de derrogações a esta proibição. Entre estas derrogações contamse o consentimento explícito da pessoa em causa, os interesses vitais da pessoa em causa, os interesses legítimos de terceiros e o interesse público.

Contrariamente ao que acontece no caso do tratamento de dados não sensíveis, uma relação contratual com a pessoa em causa não é considerada uma base geral para o tratamento legítimo de dados sensíveis. Por conseguinte, se for necessário tratar dados sensíveis no contexto de um contrato com a pessoa em causa, esta deverá dar o seu consentimento explícito para a utilização destes dados, para além de manifestar a sua vontade em celebrar o próprio contrato. Porém, se a pessoa em causa pedir explicitamente bens ou serviços que revelem necessariamente dados sensíveis, esse pedido deve ser equiparado a um consentimento explícito.

Exemplo: Se um passageiro de uma companhia aérea, no contexto da reserva de um voo, solicitar a disponibilização de uma cadeira de rodas e comida kosher, a companhia aérea está autorizada a utilizar estes dados ainda que o passageiro não tenha assinado uma cláusula adicional declarando que consente na utilização de dados que revelam informações sobre a sua saúde e as suas convicções religiosas.

Consentimento explícito da pessoa em causa

O primeiro requisito de licitude do tratamento de quaisquer dados, sejam eles dados sensíveis ou não sensíveis, é o consentimento da pessoa em causa. No caso dos dados sensíveis, esse consentimento tem de ser explícito. O direito nacional pode, contudo, estabelecer que o consentimento para a utilização de dados sensíveis não constitui base legal suficiente para permitir o seu tratamento,[143] por exemplo,

142 Diretiva Proteção de Dados, artigo 8.º, n.º 1.

143 *Ibid.,* artigo 8.º, n.º 2, al. a).

quando, em casos excecionais, o tratamento envolve riscos extraordinários para a pessoa em causa.

Existe um caso especial em que até mesmo o consentimento implícito é reconhecido como base legal para o tratamento de dados sensíveis. O artigo 8.º, n.º 2, alínea e), da Diretiva estabelece que o tratamento não é proibido se disser respeito a dados manifestamente tornados públicos pela pessoa em causa. Esta disposição tem evidentemente subjacente o entendimento de que o ato de tornar públicos os seus dados deve ser interpretado como consentimento implícito para a utilização desses dados.

Interesses vitais da pessoa em causa

Tal como acontece no caso dos dados não sensíveis, os dados sensíveis podem ser objeto de tratamento devido aos interesses vitais da pessoa em causa.[144]

Para que o tratamento de dados sensíveis seja legítimo nestes casos, é necessário que fosse impossível submeter a questão à decisão da pessoa em causa, porque, por exemplo, esta estava inconsciente ou estava ausente e não tinha sido possível contactála.

Interesses legítimos de terceiros

Tal como acontece no caso dos dados não sensíveis, os interesses legítimos de terceiros poderão constituir a base para o tratamento de dados sensíveis. Porém, no que respeita aos dados sensíveis, e conforme estabelecido no artigo 8.º, n.º 2, da Diretiva de Proteção de Dados, só assim será nos seguintes casos:

- quando o tratamento for necessário para proteger interesses vitais de uma outra pessoa[145] se a pessoa em causa estiver física ou legalmente incapaz de dar o seu consentimento;

- quando os dados sensíveis forem relevantes no domínio da legislação do trabalho, tais como dados sobre a saúde no contexto de um local de trabalho

144 *Ibid.,* artigo 8.º, n.º 2, al. c).

145 *Ibid.*

especificamente perigoso, ou dados sobre as convicções religiosas no contexto de feriados;[146]

- quando fundações, associações ou outros organismos sem fins lucrativos de caráter político, filosófico, religioso ou sindical tratam dados sobre os seus membros, patrocinadores ou outras partes interessadas (esses dados são sensíveis porque revelarão provavelmente as convicções religiosas ou políticas das pessoas em questão);[147]

- quando os dados sensíveis forem utilizados no contexto de um processo judicial ou administrativo para declarar, exercer ou defender um direito.[148]

- Acresce que, de acordo com o artigo 8.º, n.º 3, da Diretiva de Proteção de Dados, sempre que forem utilizados dados sobre a saúde para fins de diagnóstico e tratamento médico por um profissional da saúde, a derrogação abrange a gestão destes serviços. A título de garantia especial, é estabelecido que apenas as pessoas sujeitas a obrigações profissionais específicas de confidencialidade serão consideradas «profissionais da saúde».

Interesse público

Segundo o artigo 8.º, n.º 4, da Diretiva de Proteção de Dados, os Estados-Membros podem prever outros casos em que é permitido o tratamento de dados sensíveis, desde que:

- o tratamento dos dados seja realizado por motivos de interesse público importante;

- esteja previsto em disposições legislativas nacionais ou numa decisão da autoridade de controlo; e

- as disposições legislativas nacionais ou a decisão da autoridade de controlo estabeleçam as garantias necessárias para proteger eficazmente os interesses das pessoas em causa.[149]

146 *Ibid.,* artigo 8.º, n.º 2, al. b).

147 *Ibid.,* artigo 8.º, n.º 2, al. d).

148 *Ibid.,* artigo 8.º, n.º 2, al. e).

149 *Ibid.,* artigo 8.º, n.º 4.

Um exemplo elucidativo são os sistemas eletrónicos de registos de saúde, que estão prestes a ser implementados em muitos Estados-Membros. Estes sistemas permitem que os dados de saúde recolhidos pelos profissionais de saúde durante o tratamento de um doente sejam disponibilizados a outros profissionais que prestam cuidados de saúde ao mesmo doente, geralmente a nível nacional.

O Grupo de Trabalho do artigo 29.º concluiu que as regras atualmente em vigor para o tratamento de dados sobre doentes não permitem a criação de tais sistemas, não sendo possível invocar, neste contexto, o artigo 8.º, n.º 3, da Diretiva de Proteção de Dados. Partindo do princípio de que a existência de tais sistemas eletrónicos de registos de saúde constitui um interesse público importante, poderia, contudo, ter por base o artigo 8.º, n.º 4, da Diretiva, exigindo uma base legal explícita para a sua criação que previsse também as garantias necessárias para assegurar o funcionamento do sistema em condições de segurança.[150]

4.2. Regras sobre a segurança do tratamento

Pontos-chave

- As regras sobre a segurança do tratamento impõem sobre o responsável pelo tratamento e o subcontratante a obrigação de colocarem em prática medidas técnicas e organizativas para evitar interferências não autorizadas nas operações de tratamento.
- O nível de segurança dos dados necessário é determinado:
  - pelas funcionalidades de segurança disponíveis no mercado para um determinado tipo de tratamento;
  - pelos custos; e
  - pela sensibilidade dos dados objeto de tratamento.
- A segurança do tratamento de dados é igualmente salvaguardada pelo dever geral imposto sobre todas as pessoas, sejam elas responsáveis pelo tratamento ou subcontratantes, de assegurar a confidencialidade dos dados.

Por conseguinte, tanto a **legislação do CdE sobre proteção de dados** como a **legislação da UE sobre proteção de dados** impõem sobre os responsáveis pelo tratamento

150 Grupo de Trabalho do artigo 29.º (2007), *Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde eletrónicos (RSE)*, WP 131, Bruxelas, 15 de fevereiro de 2007.

e os subcontratantes a obrigação de tomarem medidas adequadas para garantir a segurança dos dados.

4.2.1. Elementos da segurança dos dados

De acordo com as disposições relevantes do **direito da UE**:

> *«Os Estados-Membros estabelecerão que o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito».*[151]

O **direito do CdE** contém uma disposição semelhante:

> *«Para a proteção dos dados de caráter pessoal registados em ficheiros automatizados devem ser tomadas medidas de segurança apropriadas contra a destruição, acidental ou não autorizada, e a perda acidental e também contra o acesso, a modificação ou a difusão não autorizados.»*[152]

Em muitos casos, foram também definidas normas setoriais, nacionais e internacionais para o tratamento de dados. O *Rótulo Europeu de Proteção da Privacidade* (EuroPriSe), por exemplo, é um projeto eTEN (Redes Transeuropeias de Telecomunicações) da UE que explorou a possibilidade de certificar certos produtos, especialmente *software*, que cumpram a legislação europeia sobre proteção de dados. A Agência Europeia para a Segurança das Redes e da Informação (ENISA) foi criada com o objetivo de reforçar a capacidade da UE, dos Estados-Membros da UE e da comunidade empresarial para evitar, gerir e responder a problemas de segurança das redes e da informação.[153] A ENISA publica regularmente análises sobre as atuais ameaças à segurança e conselhos sobre a resposta a dar às mesmas.

Para garantir a segurança dos dados, não basta dispor do equipamento certo (*hardware* e *software*), sendo igualmente necessárias regras organizacionais internas

151 Diretiva Proteção de Dados, artigo 17.º, n.º 1.

152 Convenção 108, artigo 7.º.

153 Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação, JO 2004 L 77.

adequadas. Essas regras internas deveriam, de preferência, abranger as seguintes questões:

- fornecimento regular de informações a todos os funcionários sobre as regras relativas à segurança dos dados e as suas obrigações nos termos da legislação sobre proteção de dados, especialmente em matéria de confidencialidade;

- distribuição clara das responsabilidades e uma descrição clara das competências em matéria de tratamento de dados, especialmente no que diz respeito às decisões de tratamento de dados pessoais e de transferência de dados para terceiros;

- utilização de dados pessoais unicamente em conformidade com as instruções da pessoa competente ou com regras gerais;

- proteção contra o acesso a instalações e a *hardware* e *software* do responsável pelo tratamento ou do subcontratante, incluindo controlos sobre a autorização de acesso;

- certificação de que as autorizações de acesso a dados pessoais foram concedidas pela pessoa competente e exigem documentação adequada;

- protocolos automatizados sobre o acesso a dados pessoais por meios eletrónicos e controlo regular desses protocolos pelo serviço de controlo interno;

- documentação exaustiva para outras formas de divulgação diferentes do acesso automatizado a dados, a fim de demonstrar que não ocorreram quaisquer transmissões ilegais de dados.

A disponibilização de uma formação e educação adequada sobre segurança dos dados aos membros do pessoal também é uma medida preventiva de segurança importante e eficaz. É igualmente necessário instituir procedimentos de verificação, a fim de assegurar que as medidas adequadas estabelecidas no papel foram implementadas e funcionam na prática (por exemplo, auditorias internas ou externas).

Entre as medidas destinadas a melhorar o nível de segurança de um responsável pelo tratamento ou subcontratante contamse instrumentos como, por exemplo, os encarregados da proteção de dados pessoais, a educação dos funcionários

em matéria de segurança, auditorias regulares, testes de penetração e selos de qualidade.

Exemplo: No processo que deu origem ao acórdão *I. c. Finlândia*,[154] a requerente não conseguiu provar que outros funcionários do hospital onde ela trabalhava tinham tido ilegitimamente acesso aos seus registos de saúde. Por este motivo, os tribunais nacionais julgaram improcedente a ação por ela instaurada com fundamento na violação do seu direito à proteção de dados. O TEDH concluiu que tinha havido uma violação do artigo 8.º da CEDH, dado que o sistema de registo de processos clínicos do hospital não permitia obter retroativamente esclarecimentos sobre a utilização dos registos dos doentes, uma vez que revelava apenas as cinco consultas mais recentes e esta informação era eliminada assim que o processo regressasse aos arquivos. Segundo o TEDH, era decisivo o facto de o sistema de registo existente no hospital não cumprir claramente os requisitos legais estabelecidos no direito nacional, um aspeto ao qual os tribunais nacionais não tinham atribuído a devida importância.

Notificações de violação de dados pessoais

Vários países europeus introduziram na sua legislação sobre proteção de dados um novo instrumento para lidar com violações da segurança dos dados: a obrigação de os prestadores de serviços de comunicações eletrónicas notificarem violações de dados pessoais às prováveis vítimas e às autoridades de controlo. Nos termos do direito da UE, esta notificação é obrigatória para os prestadores de serviços de telecomunicações.[155] A notificação de violações de dados pessoais às pessoas em causa visa evitar a ocorrência de danos: a notificação de violações de dados pessoais e das suas possíveis consequências minimiza o risco de efeitos negativos para as pessoas em causa. Em casos de negligência grosseira, também deve ser aplicada uma coima aos prestadores de serviços.

154 TEDH, acórdão *I. c. Finlândia* de 17 de julho de 2008, petição n.º 20511/03.

155 Ver Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (*Diretiva relativa à privacidade e às comunicações eletrónicas*), JO 2002 L 201, art. 4.º, n.º 3, com a redação que lhe foi dada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor, JO 2009 L 337.

Será necessário implementar antecipadamente procedimentos internos para uma gestão e comunicação eficaz de violações de dados pessoais, uma vez que o prazo para cumprimento da obrigação de comunicação às pessoas em causa e/ou autoridade de controlo previsto no direito nacional é geralmente muito curto.

4.2.2. Confidencialidade

No âmbito do **direito da UE**, a segurança do tratamento de dados é igualmente salvaguardada pelo dever geral imposto sobre todas as pessoas, sejam elas responsáveis pelo tratamento ou subcontratantes, de assegurar a confidencialidade dos dados.

Exemplo: Uma funcionária de uma companhia de seguros recebe um telefonema no local de trabalho de alguém que afirma ser um cliente, solicitando informações sobre o seu contrato de seguro.

O dever de manter a confidencialidade dos dados dos clientes exige que a funcionária tome, pelo menos, medidas mínimas de segurança antes de divulgar dados pessoais. Neste sentido, poderia, por exemplo, oferecerse para telefonar, ela própria, para o número constante do processo do cliente.

O artigo 16.º da Diretiva de Proteção de Dados relativo à confidencialidade só é aplicável no contexto da relação entre o responsável pelo tratamento e o subcontratante. O facto de os responsáveis pelo tratamento estarem ou não sujeitos a um dever de confidencialidade, no sentido de que não podem divulgar os dados a terceiros, é tratado nos artigos 7.º e 8.º da Diretiva.

O dever de confidencialidade não abrange as situações em que uma pessoa toma conhecimento dos dados na qualidade de particular e não de funcionário do responsável pelo tratamento ou do subcontratante. Neste caso, o artigo 16.º da Diretiva de Proteção de Dados não é aplicável porque, com efeito, a utilização de dados pessoais por particulares está completamente fora do âmbito de aplicação da Diretiva quando tal utilização estiver abrangida pela chamada «exceção doméstica».[156] Esta exceção consiste na utilização de dados pessoais «por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas».[157] Porém, desde o acórdão

156 Diretiva Proteção de Dados, artigo 3.º, n.º 2, segundo travessão.

157 *Ibid*.

Bodil Lindqvist do TJUE,[158] esta exceção tem de ser objeto de uma interpretação restritiva, especialmente em relação à divulgação de dados. Em especial, a exceção doméstica não será aplicável à divulgação de dados pessoais a um número ilimitado de destinatários na Internet (para informações mais detalhadas sobre este processo, ver secções 2.1.2, 2.2, 2.3.1 e 6.1).

No âmbito do **direito do CdE**, a obrigação de confidencialidade está implícita no conceito de segurança dos dados no artigo 7.º da Convenção108, que trata da segurança dos dados.

Relativamente aos subcontratantes, a confidencialidade significa que estes só poderão utilizar os dados pessoais que lhes foram confiados pelo responsável pelo tratamento em conformidade com as instruções dadas por este. No que respeita aos funcionários do responsável pelo tratamento ou do subcontratante, a confidencialidade exige que estes utilizem os dados pessoais unicamente de acordo com as instruções dos respetivos superiores hierárquicos.

A obrigação de confidencialidade tem de ser incluída em qualquer contrato celebrado entre os responsáveis pelo tratamento e os seus subcontratantes. Além disso, os responsáveis pelo tratamento e os subcontratantes terão de tomar medidas específicas para impor sobre os seus funcionários um dever de confidencialidade, normalmente através da inclusão de cláusulas de confidencialidade no contrato de trabalho do funcionário.

Em muitos Estados-Membros da UE e Partes na Convenção 108, a violação de deveres profissionais de confidencialidade é punível nos termos da lei penal.

4.3. Regras sobre a transparência do tratamento

Pontos-chave

- Antes de dar início ao tratamento de dados pessoais, o responsável pelo tratamento deve, no mínimo, informar as pessoas em causa da sua própria identidade e da finalidade do tratamento, salvo se a pessoa em causa já possuir essas informações.

158 TJUE, acórdão de 6 de novembro de 2003 no processo C-101/01, *Bodil Lindqvist*.

- Sempre que os dados forem recolhidos junto de terceiros, a obrigação de fornecer informações não existe se:
  - o tratamento dos dados estiver previsto na lei; ou
  - o fornecimento das informações se revelar impossível ou implicar um esforço desproporcionado.
- Antes de dar início ao tratamento de dados pessoais, o responsável pelo tratamento deve ainda:
  - notificar a autoridade de controlo das operações de tratamento planeadas; ou
  - providenciar a documentação a nível interno das operações de tratamento por um encarregado da proteção de dados pessoais independente, caso a legislação nacional preveja este tipo de procedimento.

O princípio do tratamento leal exige a transparência do tratamento. Para este efeito, **o direito do CdE** estabelece que qualquer pessoa poderá tomar conhecimento da existência de ficheiros automatizados de dados, da sua finalidade e do responsável pelo ficheiro.[159] Os meios de concretização desta disposição são deixados ao critério do legislador nacional. O **direito da UE** é mais específico, assegurando a transparência perante a pessoa em causa através da obrigação de informação a que está sujeito o responsável pelo tratamento e perante o público em geral através da notificação.

Ambos os sistemas jurídicos permitem o estabelecimento de derrogações e restrições às obrigações do responsável pelo tratamento no direito nacional sempre que essas restrições constituam uma medida necessária à proteção de certos interesses públicos ou à proteção da pessoa em causa ou dos direitos e liberdades de outrem, desde que sejam necessárias numa sociedade democrática.[160] Estas derrogações poderão, por exemplo, ser necessárias no contexto de uma investigação criminal, mas também se poderão justificar noutras circunstâncias.

4.3.1. Informação

Nos termos do **direito do CdE** e do **direito da UE**, os responsáveis pelas operações de tratamento são obrigados a informar previamente a pessoa em causa do tratamento planeado.[161] Esta obrigação não depende de um pedido da pessoa em

159 Convenção 108, artigo 8.º, alínea a).

160 *Ibid.*, artigo 9.º, n.º 2; e Diretiva Proteção de Dados, artigo 13.º, n.º 1.

161 Convenção 108, artigo 8.º, al. a); Diretiva Proteção de Dados, artigos 10.º e 11.º.

causa, devendo o responsável pelo tratamento tomar a iniciativa de fornecer as informações, independentemente de a pessoa em causa ter ou não mostrado interesse nas mesmas.

Conteúdo da informação

As informações têm de incluir a finalidade do tratamento, bem como a identidade e o contacto do responsável pelo tratamento.[162] A Diretiva de Proteção de Dados exige o fornecimento de informações adicionais desde que «sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à pessoa em causa um tratamento leal dos mesmos». Os artigos 10.º e 11.º da Diretiva descrevem, entre outros aspetos, as categorias de dados tratados e os destinatários desses dados, bem como a existência do direito de acesso aos dados e de retificação dos mesmos. Sempre que forem recolhidos dados junto das pessoas em causa, as informações devem esclarecer se a resposta às perguntas tem caráter obrigatório ou facultativo, bem como as possíveis consequências de não responder.[163]

Do ponto de vista do **direito do CdE**, o fornecimento destas informações poderá ser considerado uma boa prática ao abrigo do princípio do tratamento leal dos dados e, nesse sentido, também faz parte do direito do CdE.

O princípio do tratamento leal exige que as informações sejam facilmente compreensíveis pelas pessoas em causa. Tem de ser utilizada uma linguagem adequada aos destinatários. O nível e o tipo de linguagem utilizados teriam de variar em função da audiência prevista (por exemplo, adultos ou crianças, público em geral ou académicos especializados).

Algumas pessoas em causa desejarão receber apenas informações resumidas sobre o modo e a finalidade do tratamento dos seus dados, enquanto outras exigirão uma explicação detalhada. A conciliação deste aspeto da informação leal é analisada num parecer do Grupo de Trabalho do artigo 29.º que promove a ideia dos chamados avisos com vários níveis,[164] dando à pessoa em causa a possibilidade de decidir que grau de pormenor prefere.

162 Convenção 108, artigo 8.º, al. a); Diretiva Proteção de Dados, artigo 10.º, al. a) e b).

163 Diretiva Proteção de Dados, artigo 10.º, al. c).

164 Grupo de Trabalho do artigo 29.º (2004), *Parecer 10/2004 sobre a prestação mais harmonizada da informação*, WP 100, Bruxelas, 25 de novembro de 2004.

Momento do fornecimento das informações

A Diretiva de Proteção de Dados contém disposições ligeiramente diferentes sobre o momento em que as informações têm de ser fornecidas, consoante os dados sejam recolhidos junto da pessoa em causa (artigo 10.º) ou de um terceiro (artigo 11.º). Quando os dados são recolhidos junto da pessoa em causa, as informações têm de ser fornecidas, o mais tardar, no momento da recolha. Quando os dados são recolhidos junto de terceiros, as informações têm de ser fornecidas, o mais tardar, ou no momento em que o responsável pelo tratamento regista os dados ou antes de os dados serem divulgados a um terceiro pela primeira vez.

Derrogações à obrigação de informar

O **direito da UE** prevê uma derrogação geral à obrigação de informar as pessoas em causa quando estas já tenham conhecimento dessas informações.[165] Esta derrogação é aplicável em situações em que a pessoa em causa já terá, de acordo com as circunstâncias do caso concreto, conhecimento de que os seus dados serão tratados para um determinado fim por um determinado responsável pelo tratamento.

O artigo 11.º da Diretiva, que diz respeito à obrigação de informar a pessoa em causa quando os dados não tenham sido recolhidos junto desta, estabelece ainda que essa obrigação não existirá, especialmente no caso do tratamento com finalidades estatísticas, históricas ou de investigação científica, se:

- o fornecimento dessas informações se revelar impossível;
- implicar esforços desproporcionados; ou
- o registo ou a divulgação dos dados estiver expressamente previsto na lei.[166]

Apenas o artigo 11.º, n.º 2, da Diretiva de Proteção de Dados estabelece que não é necessário informar as pessoas em causa das operações de tratamento se estas estiverem previstas na lei. Tendo em conta a presunção geral de que todos os cidadãos conhecem a lei, poderseia afirmar que, sempre que os dados forem recolhidos junto da pessoa em causa nos termos do artigo 10.º da Diretiva, esta tem conhecimento das informações. Porém, uma vez que o conhecimento da lei é apenas uma

165 Diretiva Proteção de Dados, artigo 10.º e 11.º, n.º 1.

166 *Ibid.*, considerando 40 e artigo 11.º, n.º 2.

presunção, o princípio do tratamento leal exigiria, nos termos do artigo 10.º, que a pessoa em causa fosse informada, ainda que o tratamento de dados esteja previsto na lei, sobretudo porque a informação da pessoa em causa não é uma tarefa particularmente difícil quando os dados são recolhidos diretamente junto desta.

Relativamente ao **direito do CdE**, a Convenção 108 prevê expressamente derrogações ao seu artigo 8.º. Mais uma vez, as derrogações estabelecidas nos artigos 10.º e 11.º da Diretiva de Proteção de Dados poderão ser encarados como exemplos de boas práticas para as derrogações estabelecidas no artigo 9.º da Convenção 108.

Diferentes formas de fornecer informações

De preferência, as informações deveriam ser comunicadas, verbalmente ou por escrito, a cada pessoa em causa. Se os dados forem recolhidos junto da pessoa em causa, as informações devem ser fornecidas no momento da recolha. Contudo, nos casos em que os dados sejam recolhidos junto de terceiros, tendo em conta as dificuldades práticas que evidentemente se colocam ao contacto direto com as pessoas em causa, as informações também podem ser fornecidas através da sua publicação por meios adequados.

Uma das formas mais eficientes de fornecer informações será a inclusão de avisos adequados na página inicial do responsável pelo tratamento (por exemplo, a política de privacidade de um sítio Web). No entanto, uma parte considerável da população não utiliza a Internet e este facto deve ser tomado em consideração na política de informação de uma empresa ou de uma autoridade pública.

4.3.2. Notificação

O legislador nacional pode impor sobre os responsáveis pelo tratamento a obrigação de notificar as autoridades de controlo competentes das suas operações de tratamento para que estas possam ser publicadas. Em alternativa, o legislador nacional pode estabelecer que os responsáveis pelo tratamento poderão nomear um encarregado da proteção dos dados pessoais, que será responsável, em especial, por manter um registo das operações de tratamento efetuadas pelo responsável pelo tratamento.[167] Este registo interno tem de ser colocado à disposição dos membros do público que o solicitem.

167 *Ibid.,* artigo 18.º, n.º 2, segundo travessão.

Exemplo: As notificações efetuadas por um encarregado interno da proteção dos dados pessoais, bem como a documentação por ele elaborada, têm de descrever as principais características do tratamento de dados em questão. Esta descrição incluirá informações sobre o responsável pelo tratamento, a finalidade do tratamento, a base legal do tratamento, as categorias de dados tratados, os prováveis terceiros destinatários, se estão ou não previstos fluxos transfronteiriços de dados e, em caso afirmativo, que dados seriam abrangidos.

A publicação das notificações pela autoridade de controlo tem de assumir a forma de um registo especial. Para cumprir o seu objetivo, o acesso a este registo tem de ser fácil e gratuito. O mesmo é aplicável à documentação mantida pelo encarregado da proteção dos dados pessoais do responsável pelo tratamento.

O legislador nacional poderá estabelecer isenções à obrigação de notificar a autoridade de controlo competente ou de nomear um encarregado interno de proteção dos dados pessoais relativamente a operações de tratamento que não sejam suscetíveis de representar um risco específico para as pessoas em causa, conforme estipulado no artigo 18.º, n.º 2, da Diretiva de Proteção de Dados.[168]

4.4. Regras sobre a promoção do cumprimento

Pontos-chave

- Desenvolvendo o princípio da responsabilidade, a Diretiva de Proteção de Dados menciona vários instrumentos de promoção do cumprimento:
  - controlo prévio das operações de tratamento planeadas por parte da autoridade de controlo nacional;
  - encarregados da proteção dos dados pessoais que prestarão ao responsável pelo tratamento um apoio especializado na área da proteção de dados;
  - códigos de conduta que especificam as regras sobre proteção de dados aplicáveis num segmento da sociedade, especialmente no mundo empresarial.
- No âmbito do direito do CdE, são propostos instrumentos semelhantes de promoção do cumprimento na Recomendação sobre a definição de perfis.

168 *Ibid.,* artigo 18.º, n.º 2, primeiro travessão.

4.4.1. Controlo prévio

Nos termos do artigo 20.º da Diretiva de Proteção de Dados, a autoridade de controlo deve verificar se existem operações de tratamento que possam representar riscos específicos para os direitos e liberdades das pessoas em causa – quer devido à finalidade do tratamento quer às circunstâncias em que tem lugar – antes do início do tratamento. O legislador nacional tem de determinar as operações de tratamento sujeitas a controlo prévio. Este controlo poderá resultar na proibição das operações de tratamento ou numa ordem de alteração de determinadas características das operações propostas. O artigo 20.º da Diretiva pretende evitar que operações de tratamento que representem riscos desnecessários tenham sequer início, dado que a autoridade de controlo tem competência para proibir estas operações. Para que este mecanismo seja eficaz, é indispensável que a autoridade de controlo seja efetivamente notificada. A fim de assegurar que os responsáveis pelo tratamento cumprem a sua obrigação de notificação, será necessário atribuir poderes coercivos às autoridades de controlo, nomeadamente o poder de aplicar coimas aos responsáveis pelo tratamento.

Exemplo: Se uma empresa efetuar operações de tratamento que, nos termos da legislação nacional, estejam sujeitas a controlo prévio, esta empresa terá de apresentar documentação sobre as operações de tratamento planeadas à autoridade de controlo. A empresa não poderá dar início às operações de tratamento antes de receber uma resposta positiva da autoridade de controlo.

Em alguns Estados-Membros, a legislação nacional estabelece que é possível dar início às operações de tratamento se a autoridade de controlo não se pronunciar dentro de um certo prazo, por exemplo, três meses.

4.4.2. Encarregados da proteção dos dados pessoais

A Diretiva de Proteção de Dados prevê a possibilidade de o legislador nacional estabelecer que os responsáveis pelo tratamento podem nomear uma pessoa para exercer as funções de encarregado da proteção dos dados pessoais.[169] Este encarregado será responsável por assegurar que os direitos e liberdades das pessoas em causa não são suscetíveis de serem prejudicados pelas operações de tratamento.[170]

169 *Ibid.,* artigo 18.º, n.º 2, segundo travessão.

170 *Ibid.*

Exemplo: Nos termos do artigo 4f, n.º 1, da Lei Federal da Proteção de Dados alemã (*Bundesdatenschutzgesetz*), as empresas privadas que tenham 10 ou mais funcionários afetos, a título permanente, ao tratamento automatizado de dados pessoais são obrigadas a nomear um encarregado interno da proteção dos dados pessoais.

A fim de concretizar este objetivo, é fundamental que o titular deste cargo disponha de um certo grau de independência no seio da organização do responsável pelo tratamento, tal como expressamente referido na Diretiva. Seria igualmente necessário estabelecer, no contexto dos direitos no trabalho, mecanismos de proteção contra vicissitudes como o despedimento sem justa causa, a fim de apoiar o exercício eficaz deste cargo.

Com vista a promover o cumprimento da legislação nacional sobre proteção de dados, algumas recomendações do CdE também adotaram o conceito de encarregado interno da proteção dos dados pessoais.[171]

4.4.3. Códigos de conduta

A fim de promoverem o cumprimento, o setor empresarial e outros setores podem formular regras detalhadas para regular as suas atividades normais de tratamento de dados. Graças aos seus conhecimentos especializados, os membros do setor estarão em melhor posição para encontrar soluções práticas e que, consequentemente, terão maior probabilidade de serem adotadas. Nesta conformidade, os Estados-Membros – assim como a Comissão Europeia são incentivados a promover a elaboração de códigos de conduta destinados a contribuir, em função das características dos diferentes setores, para a boa execução das disposições nacionais tomadas pelos Estados-Membros nos termos da Diretiva.[172]

A fim de assegurar a conformidade destes códigos de conduta com as disposições nacionais adotadas nos termos da Diretiva de Proteção de Dados, os Estados-Membros têm de estabelecer um procedimento para a apreciação dos códigos. Este procedimento exigiria normalmente a participação da autoridade nacional, de associações profissionais e de outras organizações representativas de outras categorias de responsáveis pelo tratamento.[173]

171 Ver, por exemplo, Recomendação sobre a definição de perfis, artigo 8.3.

172 Ver a Diretiva Proteção de Dados, artigo 27.º, n.º 1.

173 *Ibid.,* artigo 27.º, n.º 2.

Os projetos de códigos comunitários, assim como as alterações ou prorrogações de códigos comunitários existentes, podem ser submetidos à apreciação do Grupo de Trabalho do artigo 29.º. Após aprovação por este Grupo de Trabalho, a Comissão Europeia pode garantir uma publicidade adequada desses códigos.[174]

Exemplo: A Federação Europeia de Marketing Direto e Interativo (FEDMA) elaborou um Código de Conduta Europeu relativo ao uso de dados pessoais em operações de marketing direto, que foi aprovado pelo Grupo de Trabalho do artigo 29.º. Em 2010, foi aditado ao código um anexo relativo às comunicações de marketing eletrónicas.[175]

174 *Ibid.,* artigo 27.º, n.º 3.

175 Grupo de Trabalho do artigo 29.º (2010), *Parecer 4/2010 sobre o código de conduta europeu relativo ao uso de dados pessoais em operações de marketing direto*, WP 174, Bruxelas, 13 de julho de 2010.

5

Os direitos das pessoas em causa e a tutela do seu exercício

UE	Questões abrangidas	CdE
Direito de acesso		
Diretiva de Proteção de Dados, artigo 12.º TJUE, acórdão de 7 de maio de 2009 no processo C-553/07, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*	**Direito de acesso aos próprios dados**	Convenção 108, artigo 8.º, al. b)
	Direito de retificação, apagamento (eliminação) ou bloqueio	Convenção 108, artigo 8.º, al. c) TEDH, acórdão *Cemalettin Canli c. Turquia* de 18 de novembro de 2008, petição n.º 22427/04 TEDH, acórdão *Segerstedt-Wiberg e outros c. Suécia* de 6 de junho de 2006, petição n.º 62332/00 TEDH, acórdão *Ciubotaru c. Moldávia* de 27 de abril de 2010, petição n.º 27138/04
Direito de oposição		
Diretiva de Proteção de Dados, artigo 14.º, n.º 1, al. a)	**Direito de oposição devido à situação particular da pessoa em causa**	Recomendação sobre a definição de perfis, artigo 5.3

UE	Questões abrangidas	CdE
Diretiva de Proteção de Dados, artigo 14.º, n.º 1, al. b)	Direito de oposição à utilização posterior dos dados para fins de marketing	Recomendação sobre marketing direto, artigo 4.1
Diretiva de Proteção de Dados, artigo 15.º	Direito de oposição a decisões automatizadas	Recomendação sobre a definição de perfis, artigo 5.5
Controlo independente		
Carta, artigo 8.º, n.º 3 Diretiva de Proteção de Dados, artigo 28.º Regulamento Proteção de Dados (Instituições da UE),capítulo V Regulamento Proteção de Dados TJUE, acórdão de 9 de março de 2010 no processo C-518/07, *Comissão Europeia/ República Federal da Alemanha* TJUE, acórdão de 16 de outubro de 2012 no processo C-614/10, *Comissão Europeia/ República da Áustria* TJUE, acórdão de 8 de abril de 2014 no processo C-288/12, *Comissão Europeia/ Hungria*	Autoridades nacionais de controlo	Convenção 108, Protocolo Adicional, artigo 1.º
Recursos e sanções		
Diretiva de Proteção de Dados, artigo 12.º	Pedido ao responsável pelo tratamento	Convenção 108, artigo 8.º, al. b)
Diretiva de Proteção de Dados, artigo 28.º, n.º 4 Regulamento Proteção de Dados (Instituições da UE), artigo 32.º, n.º 2	Pedidos deduzidos perante a autoridade de controlo	Convenção 108, Protocolo Adicional, artigo 1.º, n.º 2, al. b)
Carta, artigo 47.º	Tribunais (em geral)	CEDH, artigo 13.º
Diretiva de Proteção de Dados, artigo 28.º, n.º 3	Tribunais nacionais	Convenção 108, Protocolo Adicional, artigo 1.º, n.º 4
TFUE, artigo 263.º, n.º 4 Regulamento Proteção de Dados (Instituições da UE), artigo 32.º, n.º 1 TFUE, artigo 267.º	TJUE	
	TEDH	CEDH, artigo 34.º

UE	Questões abrangidas	CdE
Recursos e sanções		
Carta, artigo 47.º Diretiva de Proteção de Dados, artigos 22.º e 23.º TJUE, acórdão de 10 de abril de 1984 no processo C-14/83, *Sabine von Colson e Elisabeth Kamann/Land Nordrhein-Westfalen* TJUE, acórdão de 26 de fevereiro de 1986 no processo C-152/84, *M.H. Marshall Southampton and South-West Hampshire Area Health Authority*	**Por infrações à legislação nacional sobre proteção de dados**	CEDH, artigo 13.º (apenas para Estados membros do CdE) Convenção 108, artigo 10.º TEDH, acórdão *K.U. c. Finlândia* de 2 de março de 2008, petição n.º 2872/02 TEDH, acórdão *Biriuk c. Lituânia* de 25 de novembro de 2008, petição n.º 23373/03
Regulamento Proteção de Dados (Instituições da UE), artigos 34.º e 49.º TJUE, acórdão de 29 de junho de 2010 no processo C28/08 P, *Comissão Europeia/The Bavarian Lager Co. Ltd*	**Por violações da legislação da UE por instituições e órgãos da UE**	

A eficácia das regras jurídicas, em geral, e dos direitos das pessoas em causa, em especial, depende, em grande parte, da existência de mecanismos adequados de fiscalização do seu cumprimento e de tutela do seu exercício, respetivamente. Nos termos da legislação europeia sobre proteção dos dados, o direito nacional tem de atribuir à pessoa em causa os poderes necessários para proteger os seus dados. O direito nacional deve igualmente criar autoridades de controlo independentes para ajudar as pessoas em causa a exercerem os seus direitos e para controlar o tratamento de dados pessoais. Além disso, o direito a uma tutela jurisdicional efetiva, tal como garantido pela CEDH e pela Carta, exige que todas as pessoas tenham acesso aos tribunais.

5.1. Os direitos dos titulares dos dados

Pontos-chave

- Qualquer pessoa terá o direito, nos termos da legislação nacional, de pedir a qualquer responsável pelo tratamento informações sobre se este está a tratar dados que lhe digam respeito.
- Os titulares dos dados terão o direito, nos termos da legislação nacional, de obterem junto do responsável pelo tratamento dos seus dados:

- acesso aos seus próprios dados;
- a retificação (ou bloqueio, consoante os casos) dos seus dados, caso estes estejam incorretos;
- o apagamento ou o bloqueio dos seus dados, consoante os casos, se o tratamento dos dados for ilícito.

- As pessoas em causa terão ainda o direito de manifestar ao responsável pelo tratamento a sua oposição:
  - a decisões automatizadas (tomadas com base em dados pessoais tratados exclusivamente por meios automatizados);
  - ao tratamento dos seus dados se essa atividade produzir resultados desproporcionados;
  - à utilização dos seus dados para fins de marketing direto.

5.1.1. Direito de acesso

No **direito da UE**, o artigo 12.º da Diretiva de Proteção de Dados contém os elementos do direito de acesso das pessoas em causa, incluindo o direito de obter do responsável pelo tratamento «confirmação de terem ou não sido tratados dados que lhes digam respeito, e informações pelo menos sobre os fins a que se destina esse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados», bem como «a retificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na presente diretiva, nomeadamente devido ao caráter incompleto ou inexato desses dados».

No **direito do CdE**, estes direitos também existem e têm de estar previstos no direito nacional (artigo 8.º da Convenção 108). Em várias recomendações do CdE, é utilizado o termo «acesso» e os diferentes aspetos do direito de acesso são descritos e a sua implementação no direito interno é proposta nos moldes referidos no parágrafo anterior.

Nos termos do artigo 9.º da Convenção 108 e do artigo 13.º da Diretiva de Proteção de Dados, a obrigação dos responsáveis pelo tratamento de responder a um pedido de acesso das pessoas em causa poderá ser objeto de restrições devido a interesses jurídicos superiores de outrem. Estes interesses jurídicos superiores poderão envolver interesses públicos, tais como a segurança nacional, a segurança pública e a repressão de infrações penais, bem como interesses privados que prevaleçam

sobre os interesses de proteção dos dados. As derrogações e restrições têm de ser necessárias numa sociedade democrática e proporcionais ao objetivo prosseguido. Em casos muito excecionais, por exemplo por indicação médica, a própria proteção da pessoa em causa poderá exigir a restrição da transparência, especialmente no que respeita à restrição do direito de acesso de todas as pessoas em causa.

Sempre que os dados sejam tratados exclusivamente para fins de investigação científica ou para fins estatísticos, a Diretiva de Proteção de Dados permite que o legislador nacional restrinja os direitos de acesso; porém, terão de ser implementadas garantias jurídicas adequadas. Em especial, é necessário assegurar que não serão tomadas quaisquer medidas ou decisões em relação a pessoas determinadas no contexto desse tratamento de dados e que «manifestamente não exista qualquer perigo de violação do direito à vida privada da pessoa em causa».[176] O artigo 9.º, n.º 3, da Convenção 108 contém disposições semelhantes.

O direito de acesso aos próprios dados

No **direito do CdE**, o direito de acesso aos próprios dados é expressamente reconhecido pelo artigo 8.º da Convenção 108. O TEDH tem afirmado repetidamente que todas as pessoas têm o direito de acesso a informações sobre os seus próprios dados pessoais detidos ou utilizados por terceiros e que este direito resulta da necessidade de respeitar a vida privada.[177] No acórdão *Leander*,[178] o TEDH concluiu que o direito de acesso a dados pessoais armazenados por autoridades públicas poderia, no entanto, ser objeto de restrições em certas situações.

No **direito da UE**, o direito de acesso aos próprios dados é expressamente reconhecido pelo artigo 12.º da Diretiva de Proteção de Dados e, como direito fundamental, no artigo 8.º, n.º 2, da Carta.

O artigo 12.º, alínea a), da Diretiva estabelece que os Estados-Membros deverão garantir a todas as pessoas em causa o direito de acesso aos seus dados pessoais e a informações. Em especial, todas as pessoas em causa têm o direito de obter do

176 Diretiva Proteção de Dados, artigo 13.º, n.º 2.

177 TEDH, acórdão *Gaskin c. Reino Unido* de 7 de julho de 1989, petição n.º 10454/83; TEDH, acórdão *Odièvre c. França* [GS] de 13 de fevereiro de 2003, petição n.º 42326/98; TEDH, acórdão *K.H. e outros c. Eslováquia* de 28 de abril de 2009, petição n.º 32881/04; TEDH, acórdão *Godelli c. Itália* de 25 de setembro de 2012, petição n.º 33783/09.

178 TEDH, acórdão *Leander c. Suécia* de 11 de julho de 1985, petição n.º 9248/81.

responsável pelo tratamento a confirmação de terem ou não sido tratados dados que lhes digam respeito e informações que abranjam, pelo menos, o seguinte:

- os fins a que se destina o tratamento;
- as categorias de dados sobre que incide;
- os dados sujeitos a tratamento;
- os destinatários ou as categorias de destinatários a quem são comunicados os dados;
- quaisquer informações disponíveis sobre a origem dos dados sujeitos a tratamento;
- no caso de decisões automatizadas, a lógica subjacente ao tratamento automatizado dos dados.

O legislador nacional pode alargar o leque de informações a prestar pelo responsável pelo tratamento, nele incluindo, por exemplo, a indicação da base legal para o tratamento de dados.

Exemplo: O acesso da pessoa em causa aos seus próprios dados pessoais permitelhe determinar se esses dados são ou não exatos. Por conseguinte, é indispensável que a pessoa em causa seja informada sobre as categorias de dados objeto de tratamento, bem como sobre o conteúdo desses dados. Assim sendo, não basta que o responsável pelo tratamento informe a pessoa em causa de que o tratamento incide sobre o seu nome, morada, data de nascimento e esfera de interesse. O responsável pelo tratamento tem igualmente de informar a pessoa em causa de que está a tratar «o nome: N.N.; uma morada: 1040 Viena, Schwarzenbergplatz 11, Áustria; a data de nascimento: 10.10.1974; e a esfera de interesse (de acordo com a declaração da pessoa em causa): música clássica.» O último elemento contém também informações sobre a origem dos dados.

A comunicação dos dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem dos dados à pessoa em causa tem de ser efetuada de forma inteligível, o que significa que o responsável pelo tratamento poderá ter de dar uma explicação mais pormenorizada sobre o que é o tratamento. Por exemplo, a mera

indicação de abreviaturas técnicas ou de termos médicos em resposta a um pedido de acesso não será, em princípio, suficiente, ainda que só estejam armazenadas essas abreviaturas ou esses termos.

Na resposta a um pedido de acesso, o responsável pelo tratamento tem de fornecer informações sobre a origem dos dados por ele tratados, na medida em que tais informações estejam disponíveis. Esta obrigação tem de ser entendida à luz dos princípios do tratamento leal e da responsabilidade. O responsável pelo tratamento não pode destruir informações sobre a origem dos dados para se eximir à sua comunicação, nem pode ignorar as normas aplicáveis e as necessidades reconhecidas na sua área de atividade em matéria de documentação. Se o responsável pelo tratamento não conservar nenhuma documentação sobre a origem dos dados tratados, não estará, em princípio, a cumprir as suas obrigações ao abrigo do direito de acesso.

Sempre que sejam realizadas avaliações automatizadas, será necessário explicar a lógica geral da avaliação, incluindo os critérios específicos que foram aplicados à avaliação da pessoa em causa.

A Diretiva não esclarece se o direito de acesso às informações abrange o passado e, em caso afirmativo, que período no passado. A este propósito, tal como sublinhado na jurisprudência do TJUE, o direito de acesso aos próprios dados não pode ser injustificadamente restringido mediante a fixação de prazos para o seu exercício. As pessoas em causa também devem ter uma oportunidade razoável de obter informações sobre operações de tratamento de dados realizadas anteriormente.

Exemplo: No processo que deu origem ao acórdão *Rijkeboer*,[179] foi perguntado ao TJUE se a restrição do direito de acesso a informações sobre os destinatários ou categorias de destinatários de dados pessoais e sobre o conteúdo dos dados comunicados ao ano anterior à data do pedido de acesso era compatível com o artigo 12.º, alínea a), da Diretiva.

Com vista a determinar se o artigo 12.º, alínea a), da Diretiva permite a imposição de tal restrição no tempo, o Tribunal de Justiça decidiu interpretar o artigo à luz dos objetivos da Diretiva. Em primeiro lugar, afirmou que o direito de acesso era necessário para que a pessoa em causa pudesse exercer o direito

179 TJUE, acórdão de 7 de maio de 2009 no processo C-553/07, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer.*

a obter do responsável pelo tratamento a retificação, apagamento ou bloqueio dos seus dados (artigo 12.º, alínea b)), ou a notificação aos terceiros a quem os dados tivesses sido comunicados dessa retificação, apagamento ou bloqueio (artigo 12.º, alínea c)). O direito de acesso também era necessário para que a pessoa em causa pudesse exercer o seu direito de oposição ao tratamento dos seus dados pessoais (artigo 14.º), ou o direito de recurso quando sofresse um prejuízo (artigos 22.º e 23.º).

A fim de garantir o efeito útil das disposições supramencionadas, o Tribunal de Justiça considerou que «esse direito deve necessariamente abranger o passado. Com efeito, se assim não fosse, a pessoa interessada não estaria em condições de eficazmente exercer o seu direito de obter a retificação, supressão ou bloqueio dos dados que se presume serem ilícitos ou incorretos ou de intentar uma ação em justiça e de ser ressarcida pelo prejuízo sofrido».

O direito de retificação, apagamento e bloqueio dos dados

«Todas as pessoas devem poder beneficiar do direito de acesso aos dados que lhes dizem respeito e que estão em fase de tratamento, a fim de assegurarem, nomeadamente, a sua exatidão e a licitude do tratamento.»[180] Em conformidade com estes princípios, as pessoas em causa devem ter o direito, nos termos da legislação nacional, de obterem do responsável pelo tratamento a retificação, o apagamento ou o bloqueio dos seus dados se considerarem que o seu tratamento não cumpre o disposto na Diretiva, nomeadamente devido ao caráter incompleto ou inexato desses dados.[181]

Exemplo: No processo que deu origem ao acórdão *Cemalettin Canli c. Turquia*,[182] o TEDH considerou que as incorreções existentes num relatório policial elaborado no contexto de um processo penal constituíam uma violação do artigo 8.º da CEDH.

O requerente tinha estado envolvido, por duas vezes, em processos penais devido à sua alegada participação em organizações ilegais, mas nunca tinha sido condenado. Quando o requerente foi novamente detido e formalmente

180 Diretiva Proteção de Dados, considerando 41.

181 *Ibid.,* artigo 12.º, al. b).

182 TEDH, acórdão *Cemalettin Canli c. Turquia* de 18 de novembro de 2008, petição n.º 22427/04, n.ºs 33, 42 e 43; TEDH, acórdão *Dalea c. França* de 2 de fevereiro de 2010, petição n.º 964/07.

acusado de outro crime, a polícia apresentou ao tribunal criminal um relatório intitulado «*Formulário de informações sobre outros crimes*», em que o requerente era identificado como membro de duas organizações ilegais. O requerente pediu que o relatório e os registos policiais fossem alterados, mas o seu pedido foi indeferido. O TEDH entendeu que as informações constantes do relatório policial estavam abrangidas pelo âmbito do artigo 8.º da CEDH, uma vez que as informações públicas sistematicamente recolhidas e armazenadas em arquivos detidos pelas autoridades também poderiam estar abrangidas pelo conceito de «vida privada». Além disso, o relatório policial estava incorreto e não tinha sido elaborado e apresentado ao tribunal criminal de acordo com a lei. O TEDH concluiu que tinha havido uma violação do artigo 8.º.

Exemplo: No processo que deu origem ao acórdão *Segerstedt-Wiberg e outros c. Suécia*,[183] os requerentes tinham sido membros de certos partidos políticos liberais e comunistas e suspeitavam que as autoridades policiais mantinham informações sobre eles nos seus registos de segurança. O TEDH deu como provado que o armazenamento dos dados em questão tinha base legal e prosseguia um objetivo legítimo. Relativamente a alguns dos requerentes, o TEDH considerou que a conservação dos dados durante todo aquele tempo constituía uma ingerência desproporcionada nas suas vidas privadas. Por exemplo, no caso de H. Schmid, as autoridades tinham conservado a informação de que, em 1969, ele tinha alegadamente defendido o uso de violência na resistência ao controlo policial durante as manifestações. O TEDH entendeu que esta informação não poderia ter prosseguido qualquer interesse de segurança nacional relevante, sobretudo dada a sua natureza histórica. O TEDH concluiu que tinha havido uma violação do artigo 8.º da CEDH em relação a quatro dos cinco requerentes.

Em alguns casos, bastará que a pessoa em causa se limite a pedir a retificação, por exemplo, de erros ortográficos no nome, de uma nova morada ou número de telefone. No entanto, se esses pedidos estiverem relacionados com questões jurídicas, tais como a identidade jurídica da pessoa em causa ou a morada correta para efeitos de entrega de documentos legais, os pedidos de retificação poderão não ser suficientes e o responsável pelo tratamento poderá ter o direito de exigir provas da alegada inexatidão. Essas exigências não poderão impor sobre a pessoa em causa um ónus de prova desrazoável, impedindoa, assim, de obter a retificação dos seus

183 TEDH, acórdão *Segerstedt-Wiberg e outros c. Suécia* de 6 de junho de 2006, petição n.º 62332/00, n.ºs 89 e 90; ver também, por exemplo, TEDH, acórdão *M.K. c. França* de 18 de abril de 2013, petição n.º 19522/09.

dados. O TEDH concluiu pela existência de violações do artigo 8.º da CEDH em vários casos em que o requerente tinha sido impedido de contestar a exatidão das informações mantidas em registos secretos.[184]

Exemplo: No processo que deu origem ao acórdão *Ciubotaru c. Moldávia*,[185] o requerente solicitou a alteração da sua origem étnica de moldava para romena, pedido esse que foi indeferido alegadamente por falta de provas. O TEDH considerou que era aceitável que os Estados exigissem provas objetivas da identidade étnica de uma pessoa no momento do seu registo. Quando o pedido se baseasse em factos puramente subjetivos e infundados, as autoridades poderiam recusar esse registo. Contudo, o pedido do requerente não se baseara apenas na perceção subjetiva da sua própria etnicidade, tendo aquele apresentado ligações objetivamente comprováveis ao grupo étnico romeno, tais como a língua, o nome, empatia e outras. No entanto, a legislação nacional exigia que o requerente apresentasse provas de que os seus pais pertenciam a esse grupo étnico. Tendo em conta a realidade histórica da Moldávia, esta exigência tinha criado um obstáculo inultrapassável ao registo de uma identidade étnica diferente daquela que as autoridades soviéticas tinham registado em relação aos pais. Ao recusar a apreciação do pedido apresentado pelo requerente à luz de provas objetivas, o Estado não tinha cumprido a obrigação positiva de assegurar o efetivo respeito pela sua vida privada. O TEDH concluiu que tinha havido uma violação do artigo 8.º da CEDH.

Na pendência de uma ação cível ou de um procedimento instaurado perante uma autoridade pública para decidir se determinados dados estão ou não corretos, a pessoa em causa pode solicitar que seja inserida uma anotação no seu ficheiro de dados indicando que a exatidão dos dados foi contestada e que se aguarda uma decisão oficial sobre a questão. Durante este período, o responsável pelo tratamento não pode apresentar estes dados como informações certas ou definitivas, especialmente a terceiros.

Os pedidos de apagamento ou eliminação dos dados baseiamse muitas vezes na alegação de que o tratamento de dados não tem uma base legítima. Essas alegações surgem geralmente quando o consentimento foi revogado ou quando certos dados já não necessários à prossecução da finalidade para que foram recolhidos. O ónus da prova de que o tratamento dos dados é legítimo recairá sobre o responsável

184 TEDH, acórdão *Rotaru c. Roménia* de 4 de maio de 2000, petição n.º 28341/95.

185 TEDH, acórdão *Ciubotaru c. Moldávia* de 27 de abril de 2010, petição n.º 27138/04, n.ºs 51 e 59.

pelo tratamento, uma vez que é ele o responsável pela legitimidade do tratamento. O princípio da responsabilidade exige que o responsável pelo tratamento esteja em condições de demonstrar, a todo o tempo, que as suas operações de tratamento de dados têm uma base legal legítima; caso contrário terá de interromper esse tratamento.

Se o tratamento dos dados for contestado com fundamento na inexatidão dos dados ou na ilicitude do tratamento, a pessoa em causa pode exigir, nos termos do princípio do tratamento leal, que os dados em causa sejam bloqueados. Isto significa que os dados não serão eliminados, mas que o responsável pelo tratamento deverá abster-se de os utilizar durante o período de bloqueio. Este bloqueio será particularmente necessário nos casos em que a continuação da utilização de dados inexatos ou detidos ilegitimamente seja suscetível de prejudicar a pessoa em causa. O legislador nacional deve regular, em maior pormenor, as condições da constituição e do cumprimento da obrigação de bloquear a utilização dos dados.

As pessoas em causa têm ainda o direito de obter do responsável pelo tratamento a notificação a terceiros de qualquer bloqueio, retificação ou apagamento, caso estes tenham recebido dados antes destas operações de tratamento. Uma vez que o responsável pelo tratamento deve documentar a comunicação de dados a terceiros, deverá ser possível identificar os destinatários dos dados e pedir a eliminação dos mesmos. Porém, se os dados tiverem sido entretanto publicados, por exemplo, na Internet, poderá ser impossível obter totalmente o apagamento dos dados, uma vez que não será possível encontrar os destinatários dos mesmos. Nos termos da Diretiva de Proteção de Dados, é obrigatório contactar os destinatários dos dados para os informar da retificação, apagamento ou bloqueio dos dados, «salvo se isso for comprovadamente impossível ou implicar um esforço desproporcionado».[186]

5.1.2. Direito de oposição

O direito de oposição abrange o direito de oposição a decisões individuais automatizadas, o direito de oposição devido à situação particular da pessoa em causa e o direito de oposição à utilização posterior dos dados para efeitos de marketing direto.

186 Diretiva Proteção de Dados, artigo 12.º, al. c), última parte do período.

O direito de oposição a decisões individuais automatizadas

As decisões automatizadas são decisões tomadas com base em dados pessoais tratados exclusivamente por meios automatizados. Se essas decisões forem suscetíveis de afetar consideravelmente as vidas das pessoas a que dizem respeito, dado incidirem, por exemplo, sobre a sua solvabilidade, capacidade profissional, comportamento ou a confiança de que são merecedoras, é necessária uma proteção especial para evitar consequências indesejadas. A Diretiva de Proteção de Dados estabelece que não devem ficar sujeitas a decisões automatizadas questões que sejam importantes para as pessoas e que estas devem ter o direito de analisar a decisão automatizada.[187]

Exemplo: Um exemplo prático importante de tomada de decisões automatizadas é a classificação do risco de crédito. Para tomar uma decisão rápida sobre a solvabilidade de um futuro cliente, são recolhidos junto deste certos dados, como a profissão e a situação familiar, que são depois combinados com dados sobre essa pessoa provenientes de outras fontes, como os sistemas de informação de crédito. Estes dados são introduzidos automaticamente num algoritmo de classificação, que calcula um valor global que representa a solvabilidade do potencial cliente. Deste modo, o funcionário da empresa pode decidir, numa questão de segundos, se a pessoa em causa é ou não aceitável como cliente.

Não obstante, nos termos da Diretiva, os Estados-Membros deverão estabelecer que uma pessoa poderá ficar sujeita a uma decisão individual automatizada se os interesses da pessoa em causa não estiverem em risco, por a decisão lhe ter sido favorável, ou se estiverem salvaguardados por outros meios adequados.[188] O direito de oposição a decisões automatizadas também está previsto no **direito do CdE**, nomeadamente na Recomendação sobre a definição de perfis.[189]

187 *Ibid.,* artigo 15.º, n.º 1.

188 *Ibid.,* artigo 15.º, n.º 2.

189 Recomendação sobre a definição de perfis, artigo 5.5.

O direito de oposição devido à situação particular da pessoa em causa

Não existe um direito geral de oposição das pessoas em causa ao tratamento dos seus dados.[190] O artigo 14.º, n.º 4, da Diretiva de Proteção de Dados, porém, atribui à pessoa em causa o direito de se opor por razões preponderantes e legítimas relacionadas com a sua situação particular. Foi reconhecido um direito semelhante na Recomendação sobre a definição de perfis do CdE.[191] Estas disposições visam a conciliação entre os direitos à proteção de dados das pessoas em causa e os interesses legítimos de terceiros no tratamento dos dados das pessoas em causa.

Exemplo: Um banco conserva dados sobre os clientes em situação de incumprimento. Um cliente cujos dados constam desta base de dados pede outro empréstimo. A base de dados é consultada, é efetuada uma avaliação da situação financeira do cliente e o empréstimo é recusado. No entanto, o cliente pode opor-se ao registo dos seus dados pessoais na base de dados e pedir a sua eliminação se conseguir provar que o incumprimento resultara simplesmente de um erro que tinha sido corrigido imediatamente após o cliente se ter apercebido do mesmo.

Se a pessoa em causa exercer fundamentadamente o seu direito de oposição, o responsável pelo tratamento deixará de poder tratar os dados em questão. Porém, a legitimidade das operações de tratamento dos dados da pessoa em causa efetuadas antes da oposição não será afetada.

O direito de oposição à utilização posterior dos dados para fins de marketing direto

O artigo 14.º, alínea b), da Diretiva de Proteção de Dados prevê o direito específico de oposição à utilização dos próprios dados para fins de marketing direto («mala direta» na terminologia da Diretiva). A Recomendação do CdE sobre marketing direto

190 Ver também TEDH, acórdão *M.S. c. Suécia* de 27 de agosto de 1997, petição n.º 20837/92, em que foram comunicados dados médicos sem consentimento e sem a possibilidade de oposição; TEDH, acórdão *Leander c. Suécia* de 26 de março de 1987, petição n.º 9248/81; ou TEDH, acórdão *Mosley c. Reino Unido* de 10 de maio de 2011, petição n.º 48009/08.

191 Recomendação sobre a definição de perfis, artigo 5.3.

também estabelece este direito.[192] Este tipo de oposição deve ser manifestado antes de os dados serem disponibilizados a terceiros para fins de marketing direto. Por conseguinte, deve ser dada à pessoa em causa a oportunidade de se opor antes de os dados serem transferidos.

5.2. Controlo independente

Pontos-chave

- A fim de assegurar uma proteção de dados eficaz, é necessário criar autoridades de controlo independentes ao abrigo do direito nacional.
- As autoridades de controlo nacionais devem agir com total independência, devendo essa independência ser garantida pela lei que as criou e estar refletida na sua estrutura orgânica.
- As autoridades de controlo desempenham funções específicas, entre as quais:
  - fiscalizar e promover a proteção de dados a nível nacional;
  - aconselhar as pessoas em causa e os responsáveis pelo tratamento, bem como o Governo e o público em geral;
  - apreciar queixas e auxiliar as pessoas em causa que aleguem violações dos seus direitos à proteção de dados;
  - supervisionar os responsáveis pelo tratamento e os subcontratantes;
  - intervir, se necessário
    - dirigindo advertências ou censuras aos responsáveis pelo tratamento e subcontratantes ou aplicandolhes uma multa,
    - ordenando a retificação, bloqueio ou apagamento dos dados,
    - proibindo o tratamento;
  - reencaminhar casos para o tribunal.

192 CdE, Comité de Ministros (1985), *Recommendation Rec(85)20 to member states on the protection of personal data used for the purposes of direct marketing* (Recomendação Rec(85)20 aos Estados membros sobre a proteção de dados de caráter pessoal utilizados para fins de marketing direto), de 25 de outubro de 1985, artigo 4.º, n.º 1.

Ao exigir um controlo independente, a Diretiva de Proteção de Dados institui um importante mecanismo para garantir uma proteção de dados eficaz. A Diretiva criou um instrumento de fiscalização do cumprimento da legislação sobre proteção de dados que não constava inicialmente da Convenção 108 ou das Diretrizes da OCDE sobre a privacidade.

Uma vez que a existência de um mecanismo de controlo independente se revelou indispensável para o desenvolvimento de uma proteção de dados eficaz, as Diretrizes da OCDE sobre a privacidade foram revistas em 2013 e uma nova disposição apela aos Estados membros para criarem e manterem autoridades de fiscalização do cumprimento da legislação sobre privacidade com a estrutura de governação, os recursos e os conhecimentos técnicos necessários para exercerem eficazmente as suas competências e tomarem decisões objetivas, imparciais e coerentes.[193]

No âmbito do **direito do CdE**, o Protocolo Adicional à Convenção 108 estabeleceu a obrigatoriedade da criação de autoridades de controlo. Este instrumento define, no artigo 1.º, o quadro jurídico das autoridades de controlo independentes que as Partes Contratantes têm de implementar no direito interno. Na descrição das funções e competências destas autoridades, utiliza uma fórmula semelhante à da Diretiva de Proteção de Dados. Em princípio, o funcionamento das autoridades de controlo deveria, assim, ser idêntico no âmbito do direito da UE e do CdE.

No âmbito do **direito da UE**, as competências e a estrutura orgânica das autoridades de controlo foram inicialmente descritas no artigo 28.º, n.º 1, da Diretiva de Proteção de Dados. O Regulamento Proteção de Dados (Instituições da UE)[194] cria a AEPD, a autoridade de controlo do tratamento de dados pelos órgãos e instituições da UE. Ao descrever as funções e responsabilidades da autoridade de controlo, este Regulamento tira partido da experiência adquirida desde a promulgação da Diretiva de Proteção de Dados.

A independência das autoridades de proteção de dados é garantida pelo artigo 16.º, n.º 2, do TFUE e pelo artigo 8.º, n.º 3, da Carta. Esta última disposição considera expressamente que o controlo por uma autoridade independente é um elemento

193 OCDE (2013), *Guidelines governing the protection of privacy and transborder flows of personal data*, artigo 19.º., al. c).

194 Regulamento (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 2001 L 8, artigos 41.º a 48.º.

essencial do direito fundamental à proteção de dados. Por seu lado, a Diretiva de Proteção de Dados exige que os Estados-Membros criem autoridades de controlo para fiscalizar a aplicação das suas disposições, atuando com total independência.[195] Não só a lei que cria a autoridade de controlo tem de conter disposições que garantam expressamente a sua independência, como a estrutura orgânica específica dessa autoridade tem de demonstrar essa independência.

Em 2010, o TJUE pronunciou-se pela primeira vez sobre o âmbito da exigência de independência das autoridades de controlo no domínio da proteção de dados.[196] Os exemplos que se seguem ilustram o seu raciocínio.

Exemplo: No processo que deu origem ao acórdão *Comissão/Alemanha*,[197] a Comissão Europeia tinha pedido ao TJUE que declarasse que a Alemanha tinha transposto incorretamente a exigência de «total independência» das autoridades de controlo responsáveis pela proteção de dados e, como tal, não tinha cumprido as obrigações que lhe incumbiam por força do artigo 28.º, n.º 1, da Diretiva de Proteção de Dados. No entender da Comissão, o problema residia no facto de a Alemanha ter submetido à tutela do Estado as autoridades responsáveis pela fiscalização do tratamento de dados pessoais fora do setor público nos diferentes Estados federados (*Länder*).

A apreciação do mérito da ação dependia, segundo o Tribunal de Justiça, do alcance da exigência de independência prevista naquela disposição e, consequentemente, da sua interpretação.

O Tribunal de Justiça sublinhou que a expressão «com total independência» constante do artigo 28.º, n.º 1, da Diretiva tinha de ser interpretada com base na própria redação da disposição, bem com nos objetivos e na sistemática da Diretiva de Proteção de Dados.[198] O Tribunal de Justiça salientou que as autoridades

195 Diretiva Proteção de Dados, artigo 28.º, n.º 1, último período; Convenção 108, Protocolo Adicional, artigo 1.º, n.º 3.

196 Ver FRA (2010), *Fundamental rights: challenges and achievements in 2010* (Direitos Fundamentais: desafios e progressos em 2010), Relatório anual 2010, p. 59. A FRA abordou esta questão em maior detalhe no seu relatório *Data protection in the European Union: the role of National Data Protection Authorities* (Proteção de dados na União Europeia: o papel das autoridades nacionais de proteção de dados), que foi publicado em maio de 2010.

197 TJUE, acórdão de 9 de março de 2010 no processo C-518/07, *Comissão Europeia/República Federal da Alemanha*, n.º 27.

198 *Ibid.*, n.ºs 17 e 29.

de controlo eram «as guardiãs» dos direitos relacionados com o tratamento de dados pessoais garantidos pela Diretiva e que a sua instituição nos Estados-Membros era, portanto, considerada «um elemento essencial da proteção das pessoas no que diz respeito ao tratamento de dados pessoais».[199] O Tribunal de Justiça concluiu que «no exercício das suas funções, as autoridades de controlo devem agir de forma objetiva e imparcial. Para tal, devem estar ao abrigo de qualquer influência externa, incluindo a influência, direta ou indireta, do Estado ou dos *Länder*, e não apenas da influência dos organismos controlados».[200]

O TJUE também concluiu que a expressão «total independência» devia ser interpretada à luz da independência da AEPD, tal como definida no Regulamento Proteção de Dados (Instituições da UE). Conforme sublinhou o Tribunal de Justiça, o artigo 44.º, n.º 2, deste Regulamento explicita o conceito de independência, acrescentado que, «no exercício das suas funções, a AEPD não solicita nem aceita instruções seja de quem for.» Fica assim excluída a tutela estatal de uma autoridade de controlo independente.[201]

Nesta conformidade, o TJUE entendeu que as instituições alemãs de proteção de dados ao nível dos Estados federados responsáveis pela fiscalização do tratamento de dados pessoais por organismos não públicos não eram suficientemente independentes porque estavam sujeitas à tutela do Estado.

Exemplo: No acórdão *Comissão/Áustria*,[202] o TJUE chamou a atenção para problemas semelhantes relativos à posição de certos membros do pessoal da autoridade austríaca para a proteção de dados (Comissão para a Proteção de Dados, DSK). O Tribunal de Justiça concluiu que, neste caso, a legislação austríaca impedia a Autoridade Austríaca para a Proteção de Dados de exercer as suas funções com total independência na aceção da Diretiva de Proteção de Dados. A independência da DSK não estava suficientemente garantida porque o seu pessoal era constituído por funcionários da Chancelaria Federal, que tinha poderes de supervisão sobre a DSK e o direito de ser informada, a todo o tempo, sobre o seu trabalho.

199 *Ibid*., n.º 23.

200 *Ibid*. n.º 25.

201 *Ibid*. n.º 27.

202 TJUE, acórdão de 16 de outubro de 2012 no processo C-614/10, *Comissão Europeia/República da Áustria,* n.ºs 59 e 63.

Exemplo: No acórdão *Comissão/Hungria*, o TJUE salientou que «a exigência [...], de que importa garantir que cada autoridade de fiscalização exerce com total independência as funções que lhe estão atribuídas, implica a obrigação do Estado-Membro em causa de respeitar a duração do mandato dessa autoridade até ao termo inicialmente previsto para o mesmo». O Tribunal de Justiça concluiu que a «Hungria, ao fazer cessar antecipadamente o mandato da autoridade de fiscalização da proteção de dados pessoais, não cumpriu as obrigações que lhe incumbem por força da Diretiva 95/46/CE [...].[203]

As autoridades de controlo dispõem, nos termos do direito nacional, de poderes, designadamente, para:[204]

- aconselhar os responsáveis pelo tratamento e as pessoas em causa sobre todas as questões relacionadas com proteção de dados;
- investigar operações de tratamento e intervir em conformidade;
- dirigir uma advertência ou uma censura ao responsável pelo tratamento;
- ordenar a retificação, o bloqueio, o apagamento ou a destruição dos dados;
- impor uma proibição temporária ou definitiva sobre o tratamento;
- reencaminhar o caso para o tribunal.

A fim de exercer as suas funções, a autoridade de controlo tem de ter acesso a todos os dados pessoais e informações necessários à realização de um inquérito, bem como a quaisquer instalações onde o responsável pelo tratamento guarde informações relevantes.

Os procedimentos e o efeito jurídico das conclusões da autoridade de controlo variam consideravelmente entre os diferentes ordenamentos jurídicos internos. Estas conclusões podem assumir diversas formas, que vão desde recomendações semelhantes às recomendações do Provedor de Justiça a decisões imediatamente executórias. Por conseguinte, quando for analisada a eficiência dos recursos disponíveis num ordenamento jurídico, é necessário ter também em conta o seu contexto.

203 TJUE, acórdão de 8 de abril de 2014, processo C-288/12, *Comissão Europeia c. Hungria*, n.ºs 50 e 67.

204 Diretiva Proteção de Dados, artigo 28.º; ver também Convenção 108, Protocolo Adicional, artigo 1.º.

5.3. Recursos e sanções

Pontos-chave

- Nos termos da Convenção 108 e da Diretiva de Proteção de Dados, o direito nacional tem de estabelecer recursos e sanções adequados contra violações do direito à proteção de dados.
  - O direito a uma tutela jurisdicional efetiva exige, nos termos do direito da UE, que o direito nacional preveja recursos judiciais em caso de violação dos direitos à proteção de dados, independentemente da possibilidade de recorrer a uma autoridade de controlo.
  - O direito nacional deve estabelecer sanções eficazes, equivalentes, proporcionais e dissuasoras.
- Antes de recorrer aos tribunais, é necessário contactar primeiro o responsável pelo tratamento. A obrigatoriedade de contactar a autoridade de controlo antes de recorrer aos tribunais é uma matéria que deverá ser regulada pelo direito nacional.
- As pessoas em causa podem, em último recurso e sob determinadas condições, submeter casos de violação da legislação sobre proteção de dados à apreciação do TEDH.
- As pessoas em causa também podem recorrer ao TJUE, mas apenas em casos muito excecionais.

Os direitos garantidos pela legislação sobre proteção de dados só podem ser exercidos pela pessoa cujos direitos estão em jogo, ou seja, alguém que seja, ou pelo menos alegue ser, a pessoa em causa. Essas pessoas podem fazer-se representar no exercício dos seus direitos por pessoas que preencham os requisitos estabelecidos no direito nacional. Os menores têm de ser representados pelos progenitores ou tutores. As pessoas também se podem fazer representar junto das autoridades de controlo por associações que tenham por objetivo lícito promover os direitos à proteção de dados.

5.3.1. Pedidos ao responsável pelo tratamento

Os direitos mencionados na secção 3.2 têm de ser exercidos, em primeira instância, junto do responsável pelo tratamento. Seria inútil recorrer diretamente à autoridade nacional de controlo ou a um tribunal nacional, uma vez que a autoridade se limitaria a informar que seria necessário contactar primeiro o responsável pelo tratamento e o tribunal indeferiria liminarmente a petição. Os requisitos formais de um pedido

juridicamente relevante ao responsável pelo tratamento, especialmente se é ou não exigida a forma escrita, deveriam ser regulados pelo direito nacional.

A entidade a quem o pedido foi dirigido na qualidade de responsável pelo tratamento deve responder ao pedido, ainda que não seja efetivamente o responsável pelo tratamento. Em qualquer caso, a pessoa em causa deve receber uma resposta no prazo estipulado no direito nacional, ainda que consista apenas na informação de que não estão a ser tratados quaisquer dados sobre o autor do pedido. Em conformidade com as disposições do artigo 12.º, alínea a), da Diretiva de Proteção de Dados e do artigo 8.º, alínea b), da Convenção 108, esse pedido deve ser tratado sem demora excessiva. Consequentemente, o legislador nacional deve estipular um prazo de resposta que seja suficientemente curto, mas que, ainda assim, permita ao responsável pelo tratamento lidar adequadamente com o pedido.

Antes de responder ao pedido, a entidade contactada na qualidade de responsável pelo tratamento tem de confirmar a identidade do autor do pedido para determinar se este é efetivamente quem afirma ser e, deste modo, evitar uma grave violação do dever de confidencialidade. Quando os requisitos relativos à confirmação da identidade não estiverem especificamente regulados no direito nacional, terão de ser estabelecidos pelo responsável pelo tratamento. No entanto, o princípio do tratamento leal oporseia a que os responsáveis pelo tratamento estabelecessem condições demasiado onerosas para comprovar a identidade (e a autenticidade do pedido, tal como discutido na secção 2.1.1).

O direito nacional deve igualmente estabelecer se os responsáveis pelo tratamento podem ou não exigir do autor do pedido o pagamento de uma determinada taxa antes de responderem ao pedido: o artigo 12.º, alínea a), da Diretiva e o artigo 8.º, alínea b), da Convenção 108 estabelecem que a resposta aos pedidos de acesso deve ser dada «sem [...] custos excessivos». Em muitos países europeus, a legislação nacional estabelece que a resposta aos pedidos apresentados ao abrigo da legislação sobre proteção de dados não deve comportar quaisquer custos, desde que não implique um esforço excessivo e extraordinário; por seu lado, os responsáveis pelo tratamento estão geralmente protegidos, pela legislação nacional, contra o abuso do direito de obter resposta.

Se a pessoa, instituição ou órgão contactado na qualidade de responsável pelo tratamento não negar que possui essa qualidade, está obrigado, dentro do prazo estipulado no direito nacional, a:

- satisfazer o pedido e informar o autor do pedido do modo como este foi satisfeito; ou

- comunicar ao autor do pedido os motivos pelos quais o seu pedido não foi satisfeito.

5.3.2. Pedidos deduzidos perante a autoridade de controlo

Se uma pessoa tiver apresentado um pedido de acesso ou deduzido oposição junto do responsável pelo tratamento e não receber uma resposta oportuna e satisfatória, pode apresentar um pedido de assistência à autoridade nacional de controlo. Durante o procedimento perante a autoridade de controlo, importa esclarecer se a pessoa, instituição ou órgão a quem o autor do pedido se dirigiu estava efetivamente obrigado a responder ao pedido e se essa resposta foi correta e suficiente. O interessado tem de ser informado pela autoridade de controlo do seguimento dado ao seu pedido.[205] Os efeitos jurídicos das decisões das autoridades nacionais de controlo são estabelecidos pelo direito nacional: essas decisões podem ter força executiva, ou seja, podem ser executadas coercivamente, ou poderá ser necessário recorrer aos tribunais se o responsável pelo tratamento não der cumprimento às decisões (parecer, censura, etc.) da autoridade de controlo.

Se os direitos à proteção de dados garantidos pelo artigo 16.º do TFUE forem alegadamente violados por instituições ou órgãos da UE, a pessoa em causa pode apresentar uma reclamação junto da AEPD,[206] a autoridade independente de controlo responsável pela proteção de dados nos termos do Regulamento Proteção de Dados (Instituições da UE) que estabelece as funções e as competências desta autoridade. A falta de resposta da AEPD no prazo de seis meses equivale a uma decisão de indeferimento da reclamação.

As decisões da autoridade nacional de controlo devem ser suscetíveis de recurso judicial, tendo legitimidade para interpor recurso tanto a pessoa em causa como os responsáveis pelo tratamento, dado terem sido partes no procedimento perante a autoridade de controlo.

205 Diretiva Proteção de Dados, artigo 28.º, n.º 4.

206 Regulamento (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 2001 L 8.

Exemplo: A autoridade de proteção de dados do Reino Unido proferiu uma decisão em 24 de julho de 2013 na qual pedia à polícia de Hertfordshire que cessasse a utilização de um sistema de vigilância de chapas de matrícula que considerava contrário à lei. Os dados recolhidos pelas câmaras eram armazenados em bases de dados locais das autoridades policiais e numa base de dados centralizada. As fotografias das chapas de matrícula eram conservadas durante dois anos e as fotografias dos veículos durante 90 dias. O Comissário para Informação entendeu que uma utilização tão alargada de câmaras e outras formas de vigilância não era proporcional ao problema que se pretendia resolver.

5.3.3. Pedido deduzido perante o tribunal

Nos termos da Diretiva de Proteção de Dados, se uma pessoa apresentar um pedido a um responsável pelo tratamento ao abrigo da legislação sobre proteção de dados e não ficar satisfeita com a sua resposta, deverá ter o direito de recorrer para um tribunal nacional.[207]

A obrigatoriedade de contactar a autoridade de controlo antes de recorrer aos tribunais é uma matéria que deverá ser regulada pelo direito nacional. Porém, na maioria dos casos, as pessoas que pretendem exercer os seus direitos à proteção de dados terão toda a vantagem em contactar primeiro a autoridade de controlo, uma vez que o procedimento aplicável aos pedidos de assistência deverá ser gratuito e sem burocracias. As informações especializadas documentadas na decisão da autoridade de controlo (parecer, censura, etc.) também poderão ajudar a pessoa em causa a fazer valer os seus direitos perante os tribunais.

No âmbito do **direito do CdE**, as violações dos direitos à proteção de dados, alegadamente cometidas a nível nacional por uma Parte Contratante da CEDH e que constituam simultaneamente uma violação do artigo 8.º da CEDH, poderão ser também submetidas ao TEDH após esgotadas todas as vias de recurso internas. As petições relativas a violações do artigo 8.º da CEDH apresentadas ao TEDH terão de preencher ainda outras condições de admissibilidade (artigos 34.º a 37.º da CEDH).[208]

Embora as petições ao TEDH só possam ter por objeto violações das Partes Contratantes, também podem abordar indiretamente atos ou omissões de particulares, na

207 Diretiva Proteção de Dados, artigo 22.º.

208 CEDH, artigos 34.º a 37.º, disponível em: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

medida em que uma Parte Contratante não tenha cumprido as obrigações positivas que lhe incumbem por força da CEDH e não tenha assegurado uma proteção suficiente contra violações dos direitos à proteção de dados no direito nacional.

Exemplo: No processo que deu origem ao acórdão *K.U. c. Finlândia*,[209] o requerente, menor, alegou que tinha sido publicado um anúncio de natureza sexual sobre ele num sítio de encontros na Internet. O prestador de serviços não revelou a identidade da pessoa que tinha publicado a informação devido às obrigações de confidencialidade estabelecidas no direito finlandês. O requerente alegou que o direito finlandês não assegurava um nível de proteção suficiente contra este tipo de atos praticados por particulares, nomeadamente a colocação de dados incriminadores sobre o requerente na Internet. O TEDH entendeu que os Estados estavam não só obrigados a absterse de ingerências arbitrárias na vida privada das pessoas, como estavam também sujeitos a obrigações positivas que envolviam a adoção de medidas destinadas a garantir o respeito pela vida privada, mesmo no âmbito das relações entre particulares. No caso do requerente, uma proteção efetiva e prática exigiria a adoção de medidas eficazes para identificar e levar à justiça o autor da infração. Contudo, o Estado não tinha assegurado essa proteção, tendo o TEDH concluído que tinha havido uma violação do artigo 8.º da CEDH.

Exemplo: No processo que deu origem ao acórdão *Köpke c. Alemanha*,[210] a requerente tinha sido submetida, sem o seu conhecimento, a videovigilância, na sequência de suspeitas de que tinha cometido furto no local de trabalho. O TEDH concluiu que nada indicava que as autoridades nacionais não tinham conseguido encontrar um equilíbrio justo, no âmbito da sua margem de apreciação, entre o direito da requerente ao respeito pela sua vida privada ao abrigo do artigo 8.º, por um lado, e o interesse do empregador na proteção dos seus direitos de propriedade e o interesse público numa boa administração da justiça. Consequentemente, a petição foi declarada inadmissível.

Se o TEDH concluir que um Estado Parte violou algum dos direitos protegidos pela CEDH, esse Estado é obrigado a executar a sentença daquele Tribunal. As medidas de execução da sentença devem, em primeiro lugar, pôr termo à violação e reparar, tanto quanto possível, as consequências negativas que dela tenham resultado

209 TEDH, acórdão *K.U. c. Finlândia* de 2 de março de 2009, petição n.º 2872/02.

210 TEDH, acórdão *Köpke c. Alemanha* (decisão sobre a admissibilidade) de 5 de outubro de 2010, petição n.º 420/07.

para o requerente. A execução das sentenças poderá também exigir a adoção de medidas de caráter geral para prevenir violações semelhantes àquelas que o TEDH deu como provadas, quer através de alterações à legislação, jurisprudência ou outras medidas.

Sempre que o TEDH concluir pela existência de uma violação da CEDH, o artigo 41.º da CEDH estabelece que o Tribunal poderá atribuir uma reparação razoável ao requerente, a expensas do Estado Parte.

No âmbito do **direito da UE**,[211] as vítimas de infrações da legislação nacional sobre proteção de dados que implementa a legislação da UE neste domínio podem, em certos casos, recorrer ao TJUE. Há dois cenários em que a pessoa em causa poderá recorrer ao TJUE com fundamento na violação dos seus direitos à proteção de dados.

No primeiro cenário, a pessoa em causa deverá ter sido vítima direta de um ato administrativo ou regulamentar da UE que viole o seu direito à proteção de dados. Nos termos do artigo 263.º, n.º 4, do TFUE:

> *«Qualquer pessoa singular ou coletiva pode interpor [...] recursos contra os atos de que seja destinatária ou que lhe digam direta e individualmente respeito, bem como contra os atos regulamentares que lhe digam diretamente respeito e não necessitem de medidas de execução.»*

Deste modo, as vítimas de tratamento ilícito de dados pessoais por um órgão da UE podem recorrer diretamente para o Tribunal Geral do TJUE, que é o órgão competente para conhecer de litígios relacionados com o Regulamento Proteção de Dados (Instituições da UE). Também existe a possibilidade de recorrer diretamente para o TJUE se a situação jurídica de uma pessoa for diretamente afetada por uma disposição legal da UE.

O segundo cenário diz respeito à competência do TJUE (Tribunal de Justiça) para proferir decisões a título prejudicial nos termos do artigo 267.º do TFUE.

No decurso de um processo nacional, as pessoas em causa podem requerer ao órgão jurisdicional nacional que peça esclarecimentos ao Tribunal de Justiça sobre a interpretação dos Tratados da UE e sobre a interpretação e validade de atos das

211 UE (2007), Tratado de Lisboa que altera o Tratado da União Europeia e o Tratado que institui a Comunidade Europeia, assinado em Lisboa em 13 de dezembro de 2007, JO 2007 C 306. Ver também as versões consolidadas do Tratado da União Europeia, JO 2012 C 326 e do TFUE, JO 2012 C 326.

instituições, órgãos ou organismos da UE. Esses esclarecimentos designamse decisões prejudiciais. Embora não satisfaçam diretamente a pretensão do autor da queixa, estas decisões permitem aos órgãos jurisdicionais nacionais assegurarse de que estão a aplicar a interpretação correta do direito da UE.

Se uma parte no processo nacional pedir o reenvio de uma questão para o TJUE, apenas os tribunais nacionais que atuam em última instância, cujas decisões já não são suscetíveis de recurso, são obrigados a dar cumprimento a esse pedido.

Exemplo: No processo que deu origem ao acórdão *Kärntner Landesregierung e o.*,[212] o Tribunal Constitucional austríaco pediu ao TJUE para se pronunciar sobre a validade dos artigos 3.º a 9.º da Diretiva 2006/24/CE (*Diretiva Conservação de Dados*) à luz dos artigos 7.º, 9.º e 11.º da Carta e sobre a compatibilidade de certas disposições da Lei Federal Austríaca sobre Telecomunicações que transpõe a Diretiva Conservação de Dados com determinados aspetos da Diretiva de Proteção de Dados e do Regulamento Proteção de Dados (Instituições da UE).

M. Seitlinger, um dos demandantes no processo perante o Tribunal Constitucional, afirmou que utilizava o telefone, a Internet e o correio eletrónico para fins profissionais e na sua vida privada. Consequentemente, a informação que enviava e recebia passava por redes públicas de telecomunicações. Nos termos da Lei das Telecomunicações austríaca, de 2003, o seu prestador de serviços de telecomunicações é obrigado a recolher e a armazenar dados sobre a sua utilização da rede. M. Seitlinger apercebeuse de que esta recolha e este armazenamento dos seus dados pessoais não eram, de modo algum, tecnicamente necessários para levar a informação do ponto A para o ponto B na rede. A recolha e o armazenamento desses dados também não eram remotamente necessários para fins de faturação. M. Seitlinger não tinha certamente dado o seu consentimento para esta utilização dos seus dados pessoais. O único motivo para a recolha e o armazenamento de todos estes dados adicionais era a Lei das Telecomunicações austríaca, de 2003.

Por conseguinte, M. Seitlinger propôs uma ação no Tribunal Constitucional austríaco, alegando que as obrigações impostas por lei sobre o seu prestador de serviços de telecomunicações violavam os seus direitos fundamentais ao abrigo do artigo 8.º da Carta da UE.

212 TJUE, acórdão de 8 de abril de 2014, processos apensos C-293/12 e C-594/12, *Digital Rights Ireland e Seitling e Outros*.

O TJUE só se pronuncia sobre os elementos constitutivos do pedido de decisão prejudicial que lhe foi apresentado. O órgão jurisdicional nacional continua a ser competente para decidir o litígio no processo principal.

Em princípio, o Tribunal de Justiça tem de responder às questões que lhe são colocadas. Não se pode recusar a proferir uma decisão prejudicial alegando que a sua resposta não seria relevante nem oportuna face ao processo original. No entanto, pode fazêlo se a questão não estiver abrangida pela sua esfera de competência.

Por último, se uma instituição ou órgão da UE alegadamente violar direitos à proteção de dados que sejam garantidos pelo artigo 16.º do TFUE no decurso de operações de tratamento de dados, a pessoa em causa pode recorrer ao Tribunal Geral do TJUE (artigo 32.º, n.ºs 1 e 4, do Regulamento Proteção de Dados relativamente às Instituições da UE). O mesmo acontece com as decisões da AEPD sobre essas violações (artigo 32.º, n.º 3, do Regulamento Proteção de Dados [Instituições da UE]).

Embora o Tribunal Geral do TJUE seja competente para decidir litígios relacionados com o Regulamento Proteção de Dados (Instituições da UE), se o demandante for uma pessoa que atue na qualidade de funcionário de uma instituição ou órgão da UE, terá de recorrer para o Tribunal da Função Pública da UE.

Exemplo: O processo que deu origem ao acórdão *Comissão Europeia/The Bavarian Lager Co. Ltd*[213] ilustra os meios de recurso disponíveis contra atividades ou decisões das instituições e órgãos da UE relevantes para a proteção de dados.

A Bavarian Lager solicitou à Comissão Europeia o acesso à ata completa de uma reunião realizada pela Comissão, alegadamente relacionada com questões jurídicas relevantes para a empresa. A Comissão tinha indeferido o pedido de acesso da empresa com fundamento em interesses superiores de proteção de dados.[214] A Bavarian Lager tinha recorrido desta decisão para o TJUE, mais concretamente para o Tribunal de Primeira Instância (o antecessor do Tribunal Geral) ao abrigo do artigo 32.º do Regulamento Proteção de Dados (Instituições da UE). No acórdão de 8 de novembro de 2007 proferido no processo T194/04,

213 TJUE, acórdão de 29 de junho de 2010 no processo C28/08 P, *Comissão Europeia/The Bavarian Lager Co. Ltd*.

214 Para uma análise do argumento, ver: AEPD (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Bruxelas, AEPD, disponível em: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

Bavarian Lager/Comissão, o Tribunal de Primeira Instância anulou a decisão da Comissão de indeferir o pedido de acesso. A Comissão Europeia recorreu desta decisão para o Tribunal de Justiça, que, em Grande Secção, decidiu anular o acórdão do Tribunal de Primeira Instância e confirmar o indeferimento do pedido de acesso.

5.3.4. Sanções

No âmbito do **direito do CdE**, o artigo 10.º da Convenção 108 dispõe que as Partes devem estabelecer sanções e vias de recurso apropriadas em face de violações das disposições do direito interno que confiram eficácia aos princípios básicos da proteção de dados consagrados na Convenção.[215] No âmbito do **direito da UE**, o artigo 24.º da Diretiva de Proteção de Dados estabelece que os Estados-Membros «tomarão as medidas adequadas para assegurar a plena aplicação das disposições da presente diretiva e determinarão, nomeadamente, as sanções a aplicar em caso de violação das disposições adotadas [...]».

Ambos os instrumentos conferem aos Estados-Membros uma ampla margem de discricionariedade na escolha das sanções e das vias de recurso adequadas. Nenhum destes instrumentos jurídicos contém orientações específicas sobre a natureza ou o tipo de sanções consideradas adequadas, nem dá exemplos de sanções.

No entanto,

> *embora os Estados-Membros da UE gozem de uma certa margem de discricionariedade na determinação das medidas mais adequadas para salvaguardar os direitos que o direito da UE atribui às pessoas, tendo em conta o princípio da cooperação leal estabelecido no artigo 4.º, n.º 3, do Tratado UE, devem ser respeitados os requisitos mínimos da eficácia, equivalência, proporcionalidade e dissuasão.*[216]

O TJUE tem entendido repetidamente que a liberdade conferida ao legislador nacional para determinar as sanções aplicáveis não é absoluta.

215 TEDH, acórdão *I. c. Finlândia* de 17 de julho de 2008, petição n.º 20511/03; TEDH, acórdão *K.U. c. Finlândia* de 2 de dezembro de 2008, petição n.º 2872/02.

216 Ver FRA (2012), *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package* (Parecer da Agência dos Direitos Fundamentais da União Europeia sobre a proposta do pacote de reforma legislativa sobre proteção de dados), 2/2012, Viena, 1 de outubro de 2012, p. 27.

Exemplo: No acórdão *Von Colson e Kamann/Land Nordrhein-Westfalen,*[217] o TJUE salientou que todos Estados-Membros destinatários de uma diretiva são obrigados a adotar, no seu ordenamento jurídico interno, todas as medidas necessárias para assegurar a sua eficácia plena, em conformidade com o objetivo por ela prosseguido. O Tribunal de Justiça considerou que, apesar de caber aos Estados Membros a escolha das formas e meios de assegurar a implementação de uma diretiva, essa liberdade não afeta as obrigações a que estão sujeitos. Em especial, uma tutela jurídica eficaz terá de proporcionar ao titular as condições para exercer e fazer valer o direito em questão em toda a sua extensão material. Para proporcionarem uma proteção genuína e eficaz, os recursos jurídicos têm de desencadear processos penais e/ou indemnizatórios que resultem em sanções com um efeito dissuasor.

Relativamente às sanções por violações do direito da UE por instituições ou órgãos da União, dado o âmbito de aplicação especial do Regulamento Proteção de Dados (Instituições da UE), apenas estão previstas sanções de natureza disciplinar. Nos termos do artigo 49.º do Regulamento, «[q]ualquer incumprimento, intencional ou por negligência, das obrigações decorrentes do presente regulamento, por um funcionário ou outro agente das Comunidades Europeias, é passível de sanção disciplinar [...]».

217 TJUE, acórdão de 10 de abril de 1984, processo C-14/83, *Sabine von Kolson and Elisabeth Kamann c. Land Nordrhein-Westfalen.*

6

Fluxos transfronteiriços de dados

UE	Questões abrangidas	CdE
Fluxos transfronteiriços de dados		
Diretiva de Proteção de Dados, artigo 25.º, n.º 1 TJUE, acórdão de 6 de novembro de 2003 no processo C-101/01, *Bodil Lindqvist*	**Definição**	Convenção 108, Protocolo Adicional, artigo 2.º, n.º 1
Livre fluxo de dados		
Diretiva de Proteção de Dados, artigo 1.º, n.º 2	**Entre Estados-Membros da UE**	
	Entre Partes Contratantes da Convenção 108	Convenção 108, artigo 12.º, n.º 2
Diretiva de Proteção de Dados, artigo 25.º	**Para países terceiros com um nível de proteção adequado**	Convenção 108, Protocolo Adicional, artigo 2.º, n.º 1
Diretiva de Proteção de Dados, artigo 26.º, n.º 1	**Para países terceiros em casos específicos**	Convenção 108, Protocolo Adicional, artigo 2.º, n.º 2, al. a)
Restrições ao fluxo de dados para países terceiros		
Diretiva de Proteção de Dados, artigo 26.º, n.º 2 Diretiva de Proteção de Dados, artigo 26.º, n.º 4	**Cláusulas contratuais**	Convenção 108, Protocolo Adicional, artigo 2.º, n.º 2, al. b) Guia da elaboração de cláusulas contratuais
Diretiva de Proteção de Dados, artigo 26.º, n.º 2	**Regras vinculativas para as empresas**	

UE	Questões abrangidas	CdE
Exemplos: Acordo PNR UE-EUA Acordo SWIFT UE-EUA	Acordos internacionais especiais	

Para além de prever o livre fluxo de dados entre os Estados-Membros, a Diretiva de Proteção de Dados também contém disposições sobre os requisitos da transferência de dados pessoais para países terceiros fora da UE. O CdE também reconheceu a importância de estabelecer regras aplicáveis aos fluxos transfronteiriços de dados para países terceiros e adotou o Protocolo Adicional à Convenção 108 em 2001. Este Protocolo reúne as principais disposições regulamentares adotadas pelas Partes na Convenção e pelos Estados-Membros da UE em matéria de fluxo transfronteiriço de dados.

6.1. Natureza dos fluxos transfronteiriços de dados

Pontos-chave

- Uma transferência transfronteiriça de dados é uma transferência de dados pessoais para um destinatário que está sujeito a uma jurisdição estrangeira.

O artigo 2.º, n.º 1, do Protocolo Adicional à Convenção 108 descreve o fluxo transfronteiriço de dados como a transferência de dados pessoais para um destinatário que está sujeito a uma jurisdição estrangeira. O artigo 25.º, n.º 1, da Diretiva de Proteção de Dados regula a «transferência para um país terceiro de dados pessoais objeto de tratamento, ou que se destinem a ser objeto de tratamento após a sua transferência [...]». Essa transferência de dados só é permitida se forem observadas as regras estabelecidas no artigo 2.º do Protocolo Adicional à Convenção 108, devendo os Estados-Membros da UE cumprir também os artigos 25.º e 26.º da Diretiva de Proteção de Dados.

Exemplo: No acórdão *Bodil Lindqvist*,[218] o TJUE considerou que «a referência, feita numa página da Internet, a várias pessoas e a sua identificação pelo nome

218 TJUE, acórdão de 6 de novembro de 2003 no processo C-101/01, *Bodil Lindqvist*, n.ºs 27, 68 e 69.

ou por outros meios, por exemplo, o número de telefone ou informações relativas às suas condições de trabalho e aos seus passatempos constitui um "tratamento de dados pessoais por meios total ou parcialmente automatizados" na aceção do artigo 3.º, n.º 1, da Diretiva 95/46.».

O Tribunal de Justiça sublinhou então que a Diretiva também estabelece regras específicas que visam assegurar o controlo, pelos Estados-Membros, das transferências de dados de caráter pessoal para países terceiros.

Porém, tendo em conta, por um lado, o estádio de evolução da Internet à data da elaboração da diretiva e, por outro, a ausência, na Diretiva, de critérios aplicáveis à utilização da Internet, «não se pode presumir que o legislador comunitário tinha a intenção de incluir prospetivamente no conceito de "transferência para um país terceiro de dados" a inserção [...] de dados numa página Internet, mesmo que estes se tornem deste modo acessíveis às pessoas de países terceiros que possuam os meios técnicos para acederem a esses dados.»

Caso contrário, se a Diretiva fosse «interpretada no sentido de que existe uma "transferência para um país terceiro de dados" cada vez que são carregados dados de caráter pessoal numa página Internet, essa transferência seria necessariamente uma transferência para todos os países terceiros onde existem os meios técnicos necessários para aceder à Internet. O regime especial previsto [na Diretiva] tornarseia, necessariamente, no que respeita às operações na Internet, um regime de aplicação geral. Com efeito, desde que a Comissão verificasse [...] que um país terceiro não assegura um nível de proteção adequado, os Estados-Membros seriam obrigados a impedir qualquer colocação na Internet de dados de caráter pessoal.»

O princípio segundo o qual a mera publicação de dados (pessoais) não deve ser considerada um fluxo transfronteiriço de dados também é aplicável aos registos públicos e aos meios de comunicação social *online*, tais como os jornais (eletrónicos) e a televisão. Apenas a comunicação dirigida a destinatários específicos está abrangida pelo conceito de «fluxo transfronteiriço de dados».

6.2. Livre fluxo de dados entre os Estados-Membros ou entre as Partes Contratantes

Pontos-chave

- A transferência de dados pessoais para outro país membro do Espaço Económico Europeu ou para outra Parte Contratante da Convenção 108 não pode ser objeto de restrições.

No âmbito do **direito do CdE,** o fluxo de dados pessoais entre as Partes da Convenção deverá ser livre, nos termos do artigo 12.º, n.º 2, da Convenção 108. O legislador nacional não poderá restringir a exportação de dados pessoais para uma Parte Contratante, salvo se:

- a natureza especial dos dados assim o exigir;[219] ou
- A restrição for necessária para evitar que a transferência se subtraia às disposições legais internas em matéria de fluxo transfronteiriço de dados para países terceiros.[220]

No âmbito do **direito da UE**, as restrições e proibições ao livre fluxo de dados entre os Estados-Membros por razões relativas à proteção de dados são proibidas pelo artigo 1.º, n.º 2, da Diretiva de Proteção de Dados. A área do livre fluxo de dados foi alargada pelo Acordo sobre o Espaço Económico Europeu (EEE),[221] que integra a Islândia, o Listenstaine e a Noruega no mercado interno.

Exemplo: Se uma filial de um grupo internacional de empresas, estabelecido em vários Estados-Membros da UE, entre os quais a Eslovénia e a França, transferir dados pessoais da Eslovénia para a França, a legislação eslovena não pode restringir ou proibir esse fluxo de dados.

219 Convenção 108, artigo 12.º, n.º 3, al. a).

220 *Ibid.,* artigo 12.º, n.º 3, al. b).

221 Decisão do Conselho e da Comissão de 13 de dezembro de 1993 relativa à celebração do Acordo sobre o Espaço Económico Europeu entre as Comunidades Europeias, os seus Estadosmembros e a República da Áustria, a República da Finlândia, a República da Islândia, o Principado do Liechtenstein, o Reino da Noruega, o Reino da Suécia e a Confederação Suíça, JO 1994 L 1.

No entanto, se essa filial eslovena desejar transferir os mesmos dados pessoais para a empresamãe nos Estados Unidos, o exportador de dados esloveno terá de se submeter ao procedimento estabelecido na legislação eslovena para o fluxo transfronteiriço de dados para países terceiros sem um nível adequado de proteção de dados, a menos que a empresamãe tenha aderido aos princípios de «porto seguro», um código de conduta voluntário sobre a garantia de um nível adequado de proteção de dados (ver secção 6.3.1).

Os fluxos transfronteiriços de dados para países membros do EEE para fins não relacionados com o mercado interno, tais como a investigação criminal, não estão, porém, sujeitos às disposições da Diretiva de Proteção de Dados e, como tal, não estão abrangidos pelo princípio do livre fluxo de dados. No que respeita ao direito do CdE, todas as áreas estão incluídas no âmbito de aplicação da Convenção 108 e do Protocolo Adicional à Convenção 108, embora as Partes Contratantes possam estabelecer derrogações. Todos os países membros do EEE também são Partes na Convenção 108.

6.3. Livre fluxo de dados para países terceiros

Pontos-chave

- A transferência de dados pessoais para países terceiros não estará sujeita a restrições nos termos da legislação nacional sobre proteção de dados se:
  - tiver sido apurado que o destinatário possui um nível adequado de proteção de dados; ou
  - for necessária tendo em conta os interesses específicos da pessoa em causa ou os interesses superiores legítimos de terceiros, especialmente interesses públicos importantes.
- Para que a proteção de dados num país terceiro seja considerada adequada, os princípios fundamentais da proteção de dados deverão ter sido efetivamente implementados no direito nacional desse país.
- Nos termos do direito da UE, a adequação da proteção de dados num país terceiro é apreciada pela Comissão Europeia. Nos termos do direito do CdE, o modo de apreciação dessa adequação é deixado ao critério do legislador nacional.

6.3.1. Livre fluxo de dados devido a uma proteção adequada

O **direito do CdE** permite que o direito interno preveja o livre fluxo de dados para Estados não contratantes se o Estado ou organização destinatário assegurar um nível de proteção adequado para a transferência de dados pretendida.[222] Compete ao legislador nacional determinar de que modo o nível de proteção num país estrangeiro deverá ser apreciado e quem deverá realizar essa apreciação.

No **direito da UE**, o livre fluxo de dados para países terceiros com um nível adequado de proteção de dados está previsto no artigo 25.º, n.º 1, da Diretiva de Proteção de Dados. A exigência de adequação e não de equivalência permite o reconhecimento de vários sistemas de proteção dos dados. Segundo o artigo 25.º, n.º 6, da Diretiva, a Comissão Europeia é competente para apreciar o nível de proteção de dados em países estrangeiros e, para este efeito, consulta o Grupo de Trabalho do artigo 29.º, que tem dado um contributo substancial para a interpretação dos artigos 25.º e 26.º.[223]

A constatação de um nível adequado de proteção pela Comissão Europeia tem efeito vinculativo. Se a Comissão Europeia publicar uma constatação de um nível adequado de proteção relativamente a um determinado país no *Jornal Oficial da União Europeia*, todos os países membros do EEE e os respetivos órgãos estão vinculados por essa decisão, o que significa que o fluxo de dados para esse país não está sujeito a procedimentos de controlo ou autorização perante as autoridades nacionais.[224]

A Comissão Europeia também pode apreciar partes do sistema jurídico de um país ou limitar a sua apreciação a temas específicos. Por exemplo, a Comissão adotou uma constatação de um nível adequado de proteção apenas relativa à legislação

222 Convenção 108, Protocolo Adicional, artigo 2.º, n.º 1.

223 Ver, por exemplo, Grupo de Trabalho do artigo 29.º (2003), *Working document on transfers of personal data to third countries: applying Article 26 (2) of the EU Data Protection Directive to binding corporate rules for international data transfers* (Documento de trabalho sobre as transferências de dados pessoais para países terceiros: a aplicação do artigo 26.º, n.º 2, da Diretiva Proteção de Dados da UE a regras vinculativas para as empresas em matéria de transferências internacionais de dados), WP 74, Bruxelas, 3 de junho de 2003; e Grupo de Trabalho do artigo 29.º (2005), *Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995*, WP 114, Bruxelas, 25 de novembro de 2005.

224 Para uma lista continuamente atualizada de países que foram objeto de uma constatação de um nível de proteção adequado, consultar a página inicial da Comissão Europeia, DireçãoGeral da Justiça, disponível em: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

comercial canadiana.[225] Existem também várias constatações de um nível adequado de proteção para transferências baseadas em acordos entre a UE e países estrangeiros. Estas decisões referemse exclusivamente a um único tipo de transferência de dados, tal como a transmissão dos registos de identificação dos passageiros pelas companhias aéreas para autoridades estrangeiras de controlo fronteiriço quando voam da UE para certos destinos no estrangeiro (ver secção 6.4.3). Mais recentemente, as transferências de dados baseadas em acordos especiais entre a UE e países terceiros dispensam geralmente a constatação de um nível adequado de proteção, presumindose que o próprio acordo assegura esse nível de proteção.[226]

Uma das mais importantes decisões sobre a adequação da proteção não diz respeito a um conjunto de disposições legais,[227] mas sim a regras, semelhantes a um código de conduta, conhecidas como os princípios de «porto seguro». Estes princípios foram definidos pela UE e pelos Estados Unidos da América para as empresas norteamericanas. A adesão aos princípios de «porto seguro» tem lugar através de um compromisso assumido voluntariamente perante o Departamento do Comércio norteamericano e documentado numa lista publicada por este. Uma vez que um dos elementos mais importantes da adequação é a eficácia da implementação da proteção de dados, o acordo de «porto seguro» também prevê um certo grau de supervisão estatal: apenas podem aderir ao sistema «porto seguro» as empresas que estejam sujeitas à supervisão da Comissão Federal do Comércio norteamericana.

6.3.2. Livre fluxo de dados em casos específicos

No âmbito do **direito do CdE**, o artigo 2.º, n.º 2, do Protocolo Adicional à Convenção 108 permite a transferência de dados pessoais para países terceiros onde não exista

225 Comissão Europeia (2002), Decisão 2002/2/CE de 20 de dezembro de 2001 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção proporcionado pela lei canadiana sobre dados pessoais e documentos eletrónicos (Personal Information and Eletronic Documents Act), JO 2002 L 2.

226 Por exemplo, o Acordo entre os Estados Unidos da América e a União Europeia sobre a utilização e a transferência dos registos de identificação dos passageiros para o Departamento da Segurança Interna dos Estados Unidos (JO 2012 L 215, pp. 5–14) ou o Acordo entre a União Europeia e os Estados Unidos da América sobre o tratamento de dados de mensagens de pagamentos financeiros e a sua transferência da União Europeia para os Estados Unidos, para efeitos do Programa de Deteção do Financiamento do Terrorismo, JO 2010 L 8, pp. 11-16.

227 Comissão Europeia (2000), Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ) emitidos pelo Departamento do Comércio dos Estados Unidos da América, JO 2000 L 215.

um nível adequado de proteção de dados, desde que a transferência esteja prevista no direito interno e seja necessária para:

- os interesses específicos da pessoa em causa; ou
- os interesses legítimos prevalecentes de terceiros, em especial interesses públicos importantes.

No âmbito do **direito da UE**, o artigo 26.º, n.º 1, da Diretiva de Proteção de Dados contém disposições semelhantes às do Protocolo Adicional à Convenção 108.

Nos termos da Diretiva, os interesses da pessoa em causa poderão justificar o livre fluxo de dados para um país terceiro se:

- a pessoa em causa tiver dado, de forma inequívoca, o seu consentimento à exportação dos dados;
- A pessoa em causa celebrar – ou se preparar para celebrar – um contrato que exija claramente a transferência dos dados para um destinatário no estrangeiro;
- tiver sido celebrado, no interesse da pessoa em causa, um contrato entre o responsável pelo tratamento e um terceiro; ou
- a transferência for necessária para proteger os interesses vitais da pessoa em causa.
- para a transferência de dados de um registo público; tratase de um exemplo de interesse prevalecente na possibilidade de o público em geral ter acesso a informações armazenadas em registos públicos.

Os interesses legítimos de terceiros poderão justificar o livre fluxo transfronteiriço de dados:[228]

- devido a um interesse público importante não relacionado com a segurança nacional ou pública, uma vez que não estão abrangidos pela Diretiva de Proteção de Dados; ou

228 Diretiva Proteção de Dados, artigo 26.º, n.º 1, al. d).

- para a declaração, o exercício ou a defesa de um direito num processo judicial.

Os casos supramencionados devem ser entendidos como derrogações à regra de que a livre transferência de dados para outros países exige um nível adequado de proteção de dados no país destinatário. As derrogações têm de ser sempre interpretadas restritivamente. Este entendimento tem sido reiterado pelo Grupo de Trabalho do artigo 29.º no contexto do artigo 26.º, n.º 1, da Diretiva de Proteção de Dados, especialmente se a suposta base legal da transferência de dados for o consentimento.[229] O Grupo de Trabalho do artigo 29.º concluiu que as regras gerais sobre a relevância jurídica do consentimento também são aplicáveis ao artigo 26.º, n.º 1, da Diretiva. Se, por exemplo, no contexto das relações laborais, existirem dúvidas sobre se o consentimento prestado pelos funcionários é, de facto, um consentimento livre, as transferências de dados não podem ter por base o artigo 26.º, n.º 1, alínea a), da Diretiva. Nestes casos, será aplicável o artigo 26.º, n.º 2, que exige que as autoridades nacionais responsáveis pela proteção de dados autorizem as transferências de dados.

6.4. Restrições ao fluxo de dados para países terceiros

Pontos-chave

- Antes de exportar dados para países terceiros que não assegurem um nível adequado de proteção de dados, o responsável pelo tratamento pode ter de submeter o fluxo de dados pretendido à apreciação da autoridade de controlo.
- O responsável pelo tratamento que pretende exportar dados tem de demonstrar duas coisas durante esta apreciação:
  - que existe uma base legal para a transferência de dados para o destinatário; e
  - que foram adotadas medidas para garantir um nível adequado de proteção dos dados no destinatário.
- As medidas que visam garantir um nível adequado de proteção de dados no destinatário poderão incluir:

229 Ver, em especial, Grupo de Trabalho do artigo 29.º (2005), *Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995*, WP 114, Bruxelas, 25 de novembro de 2005.

  - cláusulas contratuais entre o responsável pelo tratamento que exporta os dados e o destinatário dos dados no estrangeiro; ou
  - regras vinculativas para as empresas, geralmente aplicáveis a transferências de dados no seio de um grupo multinacional de empresas.
- As transferências de dados para autoridades estrangeiras também podem ser reguladas por um acordo internacional especial.

A Diretiva de Proteção de Dados e o Protocolo Adicional à Convenção 108 permitem que o direito interno estabeleça regimes jurídicos aplicáveis aos fluxos transfronteiriços de dados para países terceiros que não assegurem um nível adequado de proteção de dados, desde que o responsável pelo tratamento tenha adotado medidas especiais para assegurar a existência de garantias adequadas em matéria de proteção de dados no destinatário e possa provar este facto à autoridade competente. Este requisito só é expressamente mencionado no Protocolo Adicional à Convenção 108; no entanto, também é considerado um procedimento corrente no quadro da Diretiva de Proteção de Dados.

6.4.1. Cláusulas contratuais

Tanto o **direito do CdE** como o **direito da UE** mencionam as cláusulas contratuais entre o responsável pelo tratamento que exporta os dados e o destinatário no país terceiro como possíveis meios de garantir um nível suficiente de proteção de dados no destinatário.

Ao **nível da UE**, a Comissão Europeia, com o auxílio do Grupo de Trabalho do artigo 29.º, definiu cláusulas contratuaistipo que foram oficialmente certificadas por uma decisão da Comissão como prova de um nível adequado de proteção de dados.[230] Uma vez que as decisões da Comissão são obrigatórias, em todos os seus elementos, para os Estados-Membros, as autoridades nacionais responsáveis pelo controlo dos fluxos transfronteiriços de dados devem ter em conta estas cláusulas contratuaistipo nos seus procedimentos.[231] Deste modo, se o responsável pelo tratamento que exporta os dados e o destinatário no país terceiro estabelecerem e assinarem as referidas cláusulas, esta medida deverá ser suficiente para demonstrar à autoridade de controlo que foram implementadas garantias adequadas.

230 Diretiva Proteção de Dados, artigo 26.º, n.º 4.

231 TFUE, artigo 288.º.

A existência de cláusulas contratuaistipo no quadro jurídico da UE não obsta a que os responsáveis pelo tratamento formulem outras cláusulas contratuais *ad hoc*. Porém, destas teria de resultar o mesmo nível de proteção que é assegurado pelas cláusulas contratuaistipo. Os elementos mais importantes das cláusulas contratuais-tipo são os seguintes:

- uma cláusula de terceiro beneficiário que permite às pessoas em causa exercer direitos contratuais embora não sejam parte no contrato;

- a concordância do destinatário ou importador dos dados em se submeter ao procedimento da autoridade nacional de controlo e/ou tribunais do responsável pelo tratamento que exporta os dados.

Existem atualmente dois conjuntos de cláusulastipo para transferências entre responsáveis pelo tratamento entre as quais o responsável pelo tratamento que exporta os dados poderá escolher.[232] Para as transferências de responsáveis pelo tratamento para subcontratantes, existe apenas um conjunto de cláusulas contratuaistipo.[233]

No contexto do **direito do CdE**, o Comité Consultivo da Convenção 108 elaborou um guia sobre a elaboração de cláusulas contratuais.[234]

232 O conjunto I consta do anexo à Decisão 2001/497/CE da Comissão, de 15 de junho de 2001, relativa às cláusulas contratuaistipo aplicáveis a transferências de dados pessoais para países terceiros, nos termos da Diretiva 95/46/CE, JO 2001 L 181; o conjunto II consta do anexo à Decisão 2004/915/CE da Comissão, de 27 de dezembro de 2004, que altera a Decisão 2001/497/CE no que se refere à introdução de um conjunto alternativo de cláusulas contratuais típicas aplicáveis à transferência de dados pessoais para países terceiros, JO 2004 L 385.

233 Comissão Europeia (2010), Decisão 2010/87 da Comissão, de 5 de fevereiro de 2010, relativa a cláusulas contratuaistipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, JO 2010 L 39.

234 CdE, Comité Consultivo da Convenção 108 (2002), *Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data* (Guia da elaboração de cláusulas contratuais sobre a proteção de dados durante a transferência de dados pessoais para terceiros não sujeitos a um nível adequado de proteção de dados).

6.4.2. Regras vinculativas para as empresas

As regras vinculativas para as empresas (RVE) multilaterais envolvem geralmente várias autoridades europeias de proteção de dados ao mesmo tempo.[235] Para que as RVE sejam aprovadas, o respetivo projeto tem de ser enviado, juntamente com o formulário normalizado do pedido de aprovação, para a autoridade principal,[236] que é identificável com base no formulário. Seguidamente, esta autoridade informa todas as autoridades de controlo dos países membros do EEE onde se encontrem estabelecidas filiais do grupo, embora a sua participação no processo de avaliação das RVE seja voluntária. Embora não seja obrigatório, todas as autoridades de proteção de dados envolvidas devem incorporar o resultado da avaliação nos seus procedimentos formais de autorização.

6.4.3. Acordos internacionais especiais

A UE celebrou acordos especiais para dois tipos de transferências de dados:

Registos de identificação dos passageiros

As companhias aéreas recolhem dados sobre os registos de identificação dos passageiros (PNR) durante o processo de reserva, nomeadamente o nome, morada, dados do cartão de crédito e número do lugar dos passageiros. Nos termos do direito norteamericano, as companhias aéreas são obrigadas a disponibilizar estes dados ao Departamento de Segurança Interna antes da partida. Esta obrigação é aplicável a voos com origem ou destino aos Estados Unidos.

235 O teor e a estrutura adequados das regras vinculativas para as empresas são explicados em Grupo de Trabalho do artigo 29.º (2008), *Working document setting up a framework for the structure of Binding Corporate Rules* (Documento de trabalho que estabelece um quadro para a estrutura das regras vinculativas para as empresas), WP 154, Bruxelas, 24 de junho de 2008; e em Grupo de Trabalho do artigo 29.º (2008), *Working document setting up a table with the elements and principles to be found in Binding Corporate Rules* (Documento de trabalho que estabelece um quadro com os elementos e os princípios das regras vinculativas para as empresas), WP 153, Bruxelas, 24 de junho de 2008.

236 Grupo de Trabalho do artigo 29.º (2007), *Recommendation 1/2007 on the standard application for approval of binding corporate rules for the transfer of personal data* (Recomendação 1/2007 sobre o formulário do pedido de aprovação das regras vinculativas para as empresas em matéria de transferência de dados pessoais), WP 133, Bruxelas, 10 de janeiro de 2007.

Para garantir uma proteção adequada dos dados PNR, nos termos da Diretiva 95/46/CE, foi adotado em 2004 um pacote legislativo sobre PNR[237]. Este pacote incluiu uma decisão de adequação do tratamento de dados efetuado pelo Departamento de Segurança Interna norte-americano.

Em consequência da anulação pelo TJUE do pacote PNR[238], a UE e os Estados Unidos assinaram dois acordos separados com dois objetivos: em primeiro lugar, proporcionar uma base legal para a divulgação de dados PNR às autoridades dos Estados Unidos; em segundo, assegurar um nível adequado de proteção de dados no país destinatário.

O primeiro acordo entre os países da UE e os Estados Unidos sobre o modo como os dados são partilhados e geridos, assinado em 2012, apresentava várias falhas, pelo que foi substituído no mesmo ano por um novo acordo a fim de reforçar a segurança jurídica.[239] O novo acordo oferece melhorias significativas. Restringe e clarifica as finalidades para que as informações podem ser utilizadas, tais como a prevenção e o combate ao terrorismo e à criminalidade transnacional grave, e fixa o período de conservação dos dados: após seis meses, os dados devem ser anonimizados. . Se os seus dados forem utilizados abusivamente, qualquer pessoa tem o direito de recurso administrativo e judicial nos termos da legislação dos EUA. Têm igualmente o direito de acesso aos seus próprios dados PNR e de solicitar a sua retificação pelo Departamento da Segurança Interna, incluindo a possibilidade de supressão, se as informações estiverem incorretas.

O Acordo, que entrou em vigor em 1 de julho de 2012, manterseá em vigor durante um período de sete anos, até 2019.

237 Decisão do Conselho 2004/496/CE, de 17 de maio de 2004, relativa à celebração de um acordo entre a Comunidade Europeia e os Estados Unidos da América sobre o tratamento e transferência de dados contidos no registo de identificação de passageiros (PNR) por parte das transportadoras aéreas para o Serviço das Alfândegas e Proteção das Fronteiras do Departamento de Segurança Interna dos Estados Unidos, JO 2004 L 183, p. 83, e Decisão da Comissão 2004/535/CE, de 14 de maio de 2004, sobre o nível de proteção adequado dos dados pessoais contidos nos Passenger Name Record transferidos para o *Bureau of Customs and Border Protection* dos Estados Unidos, JO 2004 L 235, p. 11-22.

238 TJUE, acórdão de 30 de maio de 2006, nos processos apensos C-317/04 e C-318/04, *Parlamento Europeu c.Conselho da União Europeia*, pontos 57, 58 e 59, no qual o Tribunal considerou que tanto a decisão de adequação como o cordo relativo ao tratamento de dados estavam excluídos do âmbito de aplicação da Diretiva.

239 Decisão 2012/472/UE do Conselho, de 26 de abril de 2012, relativa à celebração do Acordo entre os Estados Unidos da América e a União Europeia sobre a utilização e a transferência dos registos de identificação dos passageiros para o Departamento da Segurança Interna dos Estados Unidos. JO 2012 L 215/4. O texto do Acordo encontrase reproduzido em anexo a esta Decisão, JO 2012 L 215, p. 514.

Em dezembro de 2011, o Conselho da União Europeia aprovou a celebração de um Acordo atualizado entre a UE e a Austrália sobre o tratamento e a transferência de dados PNR.[240] Este acordo representa mais um passo na agenda da UE, que inclui diretrizes globais sobre PNR,[241] o estabelecimento de um sistema PNR da UE[242] e a negociação de acordos com países terceiros.[243]

Dados de mensagens de pagamentos financeiros

A *Sociedade das Telecomunicações Financeiras Interbancárias no Mundo (Society for Worldwide Interbank Financial Telecommunication SWIFT)* sedeada na Bélgica, que é o subcontratante para a maioria das transferências monetárias globais provenientes de bancos europeus, possuía um centro 'espelho' nos Estados Unidos e foi confrontada com um pedido de divulgação de dados ao Departamento do Tesouro norteamericano para fins de investigação do terrorismo.[244]

Da perspetiva da UE, não existia base legal suficiente para divulgar estes dados essencialmente europeus, aos quais era possível aceder nos Estados Unidos apenas

240 Decisão 2012/381/UE do Conselho, de 13 de dezembro de 2011, relativa à celebração do Acordo entre a União Europeia e a Austrália sobre o tratamento e a transferência de dados do registo de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Serviço Aduaneiro e de Proteção das Fronteiras australiano, JO 2012 L 186/3. O texto do Acordo, que substituiu um acordo anterior de 2008, encontrase reproduzido em anexo a esta Decisão, JO 2012 L 186, p. 4-16.

241 Ver, em especial, a Comunicação da Comissão, de 21 de setembro de 2010, sobre a abordagem global relativa à transferência de dados do registo de identificação dos passageiros (PNR) para países terceiros, COM(2010) 492 final, Bruxelas, 21 de Setembro de 2010. Ver também o Parecer 7/2010, do Grupo de Trabalho do Artigo 29, sobre esta Comunicação da Comissão.

242 Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, COM(2011) 32 final, Bruxelas, 2 de fevereiro de 2011. Em abril de 2011, o Parlamento Europeu solicitou à FRA um parecer sobre esta Proposta e a sua conformidade com a Carta dos Direitos Fundamentais da União Europeia. Ver: FRA (2011), *Opinion 1/2011 – Passenger Name Record* (Parecer 1/2011 – Registo de identificação dos passageiros), Viena, 14 de junho de 2011.

243 A UE está atualmente a negociar um novo acordo PNR com o Canadá, que susbtituirá o acordo de 2006 atualmente em vigor.

244 Ver, neste contexto, Grupo de Trabalho do artigo 29.º (2011), *Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing* (Parecer 14/2011 sobre questões de proteção de dados relacionadas com a prevenção do branqueamento de capitais e do financiamento do terrorismo), WP 186, Bruxelas, 13 de junho de 2011; Grupo de Trabalho do artigo 29.º (2006), *Parecer 10/2006 sobre o tratamento de dados pessoais pela Sociedade das Telecomunicações Financeiras Interbancárias no Mundo (Society for Worldwide Interbank Financial Telecommunication SWIFT)*, WP 128, Bruxelas, 22 de novembro de 2006; Comissão para a Proteção da Vida Privada belga (Commission de la protection de la vie privée) (2008), «Control and recommendation procedure initiated with respect to the company SWIFT scrl», Decisão de 9 de dezembro de 2008.

porque um dos centros de tratamento de dados da SWIFT estava localizado nesse país.

Em 2010, foi celebrado um acordo especial entre a UE e os Estados Unidos, conhecido como o Acordo SWIFT, a fim de proporcionar a necessária base legal e assegurar a proteção dos dados.[245]

Nos termos deste acordo, os dados financeiros armazenados pela SWIFT continuam a ser fornecidos ao Departamento do Tesouro norteamericano para efeitos de prevenção, investigação, deteção ou repressão do terrorismo ou do seu financiamento. O Departamento do Tesouro norteamericano pode solicitar dados financeiros à SWIFT, devendo o pedido:

- identificar o mais claramente possível os dados financeiros;
- fundamentar claramente a necessidade dos dados;
- ser formulado de modo a reduzir ao mínimo o volume de dados requerido;
- absterse de solicitar dados relacionados com o Espaço Único de Pagamentos em Euros (SEPA).

O Departamento do Tesouro norteamericano deve enviar à Europol uma cópia de cada pedido e esta verifica se o pedido está ou não conforme com os princípios do Acordo SWIFT[246]. Se esta conformidade for confirmada, a SWIFT tem de fornecer os dados financeiros diretamente ao Departamento do Tesouro norteamericano. O departamento tem de manter os dados financeiros num ambiente físico seguro ao qual apenas tenham acesso os analistas encarregados da investigação do terrorismo ou do seu financiamento e os dados financeiros não podem estar interligados com qualquer outra base de dados. Em regra, os dados financeiros fornecidos pela SWIFT deverão ser eliminados no prazo máximo de cinco anos a contar da receção. Os dados financeiros relevantes para investigações ou ações penais específicas

245 Decisão 2010/412/UE do Conselho, de 13 de julho de 2010, relativa à celebração do Acordo entre a União Europeia e os Estados Unidos da América sobre o tratamento de dados de mensagens de pagamentos financeiros e a sua transferência da União Europeia para os Estados Unidos para efeitos do Programa de Deteção do Financiamento do Terrorismo, JO 2010 L 195, p. 3 e 4. O texto do Acordo encontrase reproduzido em anexo a esta Decisão, JO 2010 L 195, p. 5-14.

246 A Instância Comum de Controlo (ICC) da Europol realizou inspeções às atividades da Europol nesta área, cujos resultados estão disponíveis em http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

poderão ser conservados pelo período de tempo necessário a essas investigações ou ações penais.

O Departamento do Tesouro norteamericano pode transferir informações extraídas de dados recebidos pela SWIFT para autoridades específicas de aplicação da lei, de segurança pública ou de combate ao terrorismo, dentro ou fora dos Estados Unidos, exclusivamente para fins de investigação, deteção, prevenção ou repressão do terrorismo e do seu financiamento. Sempre que a transferência ulterior de dados financeiros envolva um cidadão ou residente de um Estado-Membro da UE, qualquer partilha dos dados com as autoridades de um país terceiro carece do consentimento prévio das autoridades competentes do Estado-Membro interessado. Podem ser estabelecidas exceções quando a partilha dos dados for essencial para a prevenção de uma ameaça imediata e grave contra a segurança pública.

O respeito pelos princípios do Acordo SWIFT é acompanhado por supervisores independentes, incluindo uma pessoa designada pela Comissão Europeia.

As pessoas em causa têm o direito de obter a confirmação, através da autoridade de proteção de dados da UE competente para o efeito, de que os direitos relativos à proteção dos seus dados foram respeitados. As pessoas em causa têm também o direito de retificação, apagamento ou bloqueio dos seus dados recolhidos e armazenados pelo Departamento do Tesouro norteamericano ao abrigo do Acordo SWIFT. No entanto, os direitos de acesso das pessoas em causa poderão estar sujeitos a certas limitações legais. Se o acesso for recusado, a pessoa em causa deve ser informada, por escrito, da recusa e do seu direito de interpor recurso administrativo e judicial nos Estados Unidos.

O Acordo SWIFT vigora por um período de cinco anos, até agosto de 2015 e é renovado automaticamente por períodos sucessivos de um ano, salvo se uma das Partes notificar a outra, com pelo menos seis meses de antecedência, da sua intenção de não prorrogar o Acordo.

7

Proteção de dados no contexto da atividade policial e da justiça penal

UE	Questões abrangidas	CdE
	Em geral	Convenção 108
	Atividade policial	Recomendação sobre a atividade policial
		TEDH, acórdão *B.B. c. França* de 17 de dezembro de 2009, petição n.º 5335/06
		TEDH, acórdão *S. e Marper c. Reino Unido* de 4 de dezembro de 2008, petições n.ºs 30562/04 e 30566/04
		TEDH, acórdão *Vetter c. França* de 31 de maio de 2005, petição n.º 59842/00
	Cibercrime	Convenção sobre o cibercrime
Proteção de dados no contexto da cooperação transfronteiriça entre as autoridades policiais e judiciárias		
Decisão-Quadro relativa à proteção de dados	Em geral	Convenção 108
		Recomendação sobre a atividade policial
Decisão Prüm	Para dados especiais: impressões digitais, ADN, hooliganismo, etc.	Convenção 108
		Recomendação sobre a atividade policial
Decisão Europol	Por agências especiais	Convenção 108
Decisão Eurojust		Recomendação sobre a atividade policial
Regulamento Frontex		

UE	Questões abrangidas	CdE
Decisão Schengen II Regulamento VIS Regulamento Eurodac Decisão SIA	Por sistema de informação comum especial	Convenção 108 Recomendação sobre a atividade policial TEDH, acórdão *Dalea c. França* de 2 de fevereiro de 2010, petição n.º 964/07

O CdE e a UE aprovaram instrumentos legais específicos para conciliar o interesse das pessoas singulares na proteção de dados e o interesse da sociedade na recolha de dados para fins de combate à criminalidade e de garantia da segurança nacional e pública.

7.1. Legislação do CdE sobre proteção de dados no domínio policial e da justiça penal

Pontos-chave

- A Convenção 108 e a Recomendação sobre a atividade policial do CdE abrangem a proteção de dados em todas as áreas da atividade policial.
- A Convenção sobre o Cibercrime (*Convenção de Budapeste*) é um instrumento jurídico internacional vinculativo que diz respeito a crimes cometidos contra e através de redes eletrónicas.

Ao nível europeu, a Convenção 108 abrange todos os domínios do tratamento de dados pessoais e as suas disposições visam regular o tratamento de dados pessoais em geral. Consequentemente, a Convenção 108 é aplicável à proteção de dados no domínio policial e da justiça penal, embora as Partes Contratantes possam limitar a sua aplicação.

As funções que a lei atribui às autoridades policiais e judiciárias implicam muitas vezes o tratamento de dados pessoais, o que poderá ter sérias consequências para as pessoas em questão. A Recomendação sobre a atividade policial, adotada pelo CdE em 1987, fornece orientações às Partes Contratantes sobre a concretização dos

princípios consagrados na Convenção 108 no contexto dos dados pessoais tratados pelas autoridades policiais.[247]

7.1.1. A Recomendação sobre a atividade policial

O TEDH tem afirmado sistematicamente que o armazenamento e a conservação de dados pessoais pelas autoridades policiais ou de segurança nacional constituem uma ingerência nos direitos protegidos pelo artigo 8.º, n.º 1, da CEDH. Muitos acórdãos do TEDH respeitam à justificação destas ingerências.[248]

Exemplo: No processo que deu origem ao acórdão *B.B. c. França*,[249] o TEDH considerou que a inclusão de uma pessoa condenada pela prática de crimes sexuais numa base de dados judicial estava abrangida pelo artigo 8.º da CEDH. No entanto, uma vez que tinham sido implementadas garantias suficientes em matéria de proteção de dados, tais como o direito da pessoa em causa requerer o apagamento dos dados, o período limitado de conservação dos dados e o acesso limitado a tais dados, tinha sido encontrado um equilíbrio justo entre os interesses privados e públicos concorrentes em jogo. O TEDH concluiu que não tinha havido uma violação do artigo 8.º da CEDH.

Exemplo: No processo que deu origem ao acórdão *S. e Marper c. Reino Unido*,[250] ambos os requerentes tinham sido acusados da prática de certos crimes, mas não tinham sido condenados. Não obstante, a polícia tinha conservado e armazenado as suas impressões digitais, perfis de ADN e amostras de células. A lei permitia a conservação de dados biométricos por tempo indeterminado nos casos em que uma pessoa fosse suspeita da prática de um crime, ainda que esta fosse posteriormente absolvida ou o processo fosse arquivado. O TEDH entendeu que a conservação generalizada e indiscriminada de dados pessoais sem qualquer limitação temporal e em que os casos em que as pessoas absolvidas podiam requerer a eliminação eram muito limitados constituía uma inge-

247 CdE, Comité de Ministros (1987), *Recommendation Rec(87)15 to member states regulating the use of personal data in the police sector* (Recomendação Rec(87)15 aos Estados membros sobre a utilização de dados pessoais no setor policial), 17 de setembro de 1987.

248 Ver, por exemplo, TEDH, acórdão *Leander c. Suécia* de 26 de março de 1987, petição n.º 9248/81; TEDH, acórdão *M.M. c. Reino Unido* de 13 de novembro de 2012, petição n.º 24029/07; TEDH, acórdão *M.K. c. França* de 18 de abril de 2013, petição n.º 19522/09.

249 TEDH, acórdão *B.B. c. França* de 17 de dezembro de 2009, petição n.º 5335/06.

250 TEDH, acórdão *S. e Marper c. Reino Unido* de 4 de dezembro de 2008, petições n.ºs 30562/04 e 30566/04, n.ºs 119 e 125.

rência desproporcional no exercício do direito dos requerentes ao respeito pela vida privada. O TEDH concluiu que tinha havido uma violação do artigo 8.º da CEDH.

Muitos outros acórdãos do TEDH respeitam à justificação da ingerência no exercício do direito à proteção de dados sob a forma de vigilância.

Exemplo: No processo que deu origem ao acórdão *Allan c. Reino Unido*,[251] as conversas privadas de um recluso com uma amiga na sala de visitas da prisão e com um coarguido numa cela tinham sido gravadas pelas autoridades sem o seu conhecimento. O TEDH considerou que a utilização de dispositivos de gravação áudio e vídeo na cela do requerente, na sala de visitas da prisão e na pessoa de um outro recluso correspondia a uma ingerência no seu direito ao respeito pela vida privada. Uma vez que não existia um regime jurídico que regulasse a utilização de dispositivos de gravação oculta pela polícia à data relevante, a referida ingerência não estava de acordo com a lei. O TEDH concluiu que tinha havido uma violação do artigo 8.º da CEDH.

Exemplo: No processo que deu origem ao acórdão *Klass e outros c. Alemanha*,[252] os requerentes alegaram que vários atos legislativos alemães que permitiam a vigilância secreta da correspondência e das telecomunicações violavam o artigo 8.º da CEDH, especialmente porque a pessoa em causa não era informada das medidas de vigilância adotadas e não podiam recorrer aos tribunais após a cessação dessas medidas. O TEDH entendeu que uma ameaça de vigilância constituía necessariamente uma ingerência na liberdade de comunicação entre os utentes dos serviços postais e de telecomunicações. Porém, considerou que tinham sido implementadas garantias suficientes contra abusos. O legislador alemão tinha motivos para considerar tais medidas necessárias numa sociedade democrática no interesse da segurança nacional e para fins de prevenção de distúrbios ou da criminalidade. O TEDH concluiu que não tinha havido uma violação do artigo 8.º da CEDH.

Uma vez que o tratamento de dados pelas autoridades policiais pode ter um impacto significativo sobre as pessoas em questão, existe uma necessidade ainda maior de definir regras detalhadas sobre proteção de dados para a manutenção de bases de dados nesta área. A Recomendação sobre a atividade policial do CdE

251 TEDH, acórdão *Allan c. Reino Unido* de 5 de novembro de 2002, petição n.º 48539/99.

252 TEDH, acórdão *Klass e outros c. Alemanha* de 6 de setembro de 1978, petição n.º 5029/71.

procurou responder a esta questão fornecendo orientações sobre o modo de recolha dos dados para fins relacionados com o trabalho da polícia; o modo de conservação dos ficheiros de dados nesta área; as pessoas que deverão ter acesso a estes ficheiros, incluindo as condições da transferência de dados para autoridades policiais estrangeiras; o modo como as pessoas em causa deverão poder exercer os seus direitos à proteção de dados; e o modo de implementação do controlo por autoridades independentes. Também é considerada a obrigação de garantir uma segurança adequada dos dados.

A Recomendação não prevê uma recolha ilimitada, indiscriminada de dados por parte das autoridades policiais, limitandoa ao que for necessário para prevenir um perigo real ou pôr termo a um crime específico. A recolha de outros dados teria de se basear em legislação nacional específica. O tratamento de dados sensíveis deverá limitarse ao que for absolutamente necessário no contexto de um determinado inquérito.

Sempre que forem recolhidos dados pessoais sem o conhecimento da pessoa em causa, esta deverá ser informada da recolha de dados assim que essa divulgação já não comprometer a investigação. A recolha de dados através de meios técnicos de vigilância ou de outros meios automatizados também se deverá basear em disposições legais específicas.

Exemplo: No processo que deu origem ao acórdão *Vetter c. França*,[253] o requerente tinha sido acusado de homicídio por testemunhas anónimas. Uma vez que o requerente visitava regularmente a casa de um amigo, a polícia instalou aí dispositivos de escuta com a autorização do juiz de instrução. Com base nas conversas gravadas, o requerente foi detido e julgado por homicídio. Requereu ao tribunal que a gravação fosse declarada inadmissível como meio probatório, alegando, em especial, que não estava prevista na lei. Segundo o TEDH, o que importava determinar era se a utilização de dispositivos de escuta estava «de acordo com a lei». A colocação de dispositivos de escuta em espaços privados estava manifestamente fora do âmbito de aplicação do artigo 100.º e segs. do Código de Processo Penal, dado que estas disposições respeitavam à interceção de linhas telefónicas. O artigo 81.º do Código não estabelecia, com uma clareza razoável, o âmbito ou o modo de exercício da discricionariedade das autoridades na autorização da monitorização de conversas privadas. Nesta

253 TEDH, acórdão *Vetter c. França* de 31 de maio de 2005, petição n.º 59842/00.

conformidade, o requerente não tinha usufruído do grau mínimo de proteção a que os cidadãos tinham direito ao abrigo do princípio do Estado de direito numa sociedade democrática. O TEDH concluiu que tinha havido uma violação do artigo 8.º da CEDH.

A Recomendação conclui que, no armazenamento de dados pessoais, deveria ser feita uma distinção clara entre: dados administrativos e dados policiais; diferentes tipos de pessoas em causa, tais como arguidos, condenados, vítimas e testemunhas; e dados considerados factos objetivos e dados baseados em suspeitas ou especulação.

A finalidade dos dados policiais deveria ser rigorosamente limitada. Isto tem consequências para a comunicação de dados policiais a terceiros: a legitimidade da transferência ou comunicação desses dados dentro do setor policial deveria depender da existência ou não de um interesse legítimo em partilhar a informação. A transferência ou comunicação desses dados fora do setor policial só deveria ser permitida quando existisse uma autorização ou obrigação legal clara nesse sentido. A transferência ou comunicação internacional deveria restringirse às autoridades policiais estrangeiras e basearse em disposições legais especiais, possivelmente acordos internacionais, salvo se fosse necessária para a prevenção de um perigo grave e iminente.

O tratamento de dados pela polícia deve estar sujeito a um controlo independente para assegurar o cumprimento da legislação interna sobre proteção de dados. As pessoas em causa devem ter todos os direitos de acesso previstos na Convenção 108. Nos casos em que os direitos de acesso das pessoas em causa tenham sido restringidos em conformidade com o artigo 9.º da Convenção 108 no interesse de uma investigação policial eficaz, o direito nacional deve atribuir à pessoa em causa o direito de recorrer para a autoridade nacional de controlo responsável pela proteção de dados ou para outro órgão independente.

7.1.2. Convenção de Budapeste sobre o Cibercrime

Uma vez que as atividades criminais utilizam e afetam cada vez mais sistemas eletrónicos de tratamento de dados, são necessárias novas disposições legais na área do direito penal para responder a este desafio. Por conseguinte, o CdE adotou um instrumento jurídico internacional – a Convenção sobre o Cibercrime (também conhecida como a Convenção de Budapeste) – para responder à questão dos crimes

cometidos contra e através de redes eletrónicas.[254] Esta Convenção também está aberta à adesão de países que não sejam membros do CdE e, em meados de 2013, quatro Estados não pertencentes ao CdE – Austrália, República Dominicana, Japão e Estados Unidos – eram partes na Convenção e 12 outros países não membros tinham assinado a Convenção ou tinham sido convidados a aderir.

A Convenção sobre o Cibercrime continua a ser o tratado internacional mais influente em matéria de violações da lei através da Internet ou de outras redes de informação. Exige que as Partes atualizem e harmonizem o seu direito penal contra a pirataria informática e outras violações de segurança, incluindo violação de direitos de autor, burla informática, pornografia infantil e outras ciberatividades ilícitas. A Convenção também prevê poderes processuais que abrangem buscas em redes informáticas e a interceção de comunicações no contexto da luta contra o cibercrime. Por último, viabiliza uma cooperação internacional eficaz. Foi adotado um protocolo adicional à Convenção relativo à incriminação de atos de natureza racista e xenófoba praticados através de sistemas informáticos.

Embora a Convenção não seja, *per se*, um instrumento de promoção da proteção de dados, incrimina atos suscetíveis de violar o direito das pessoas à proteção dos seus dados. Estabelece ainda sobre as Partes Contratantes a obrigação de, ao implementarem a Convenção, preverem uma proteção adequada dos direitos humanos e das liberdades garantidos pela CEDH, nomeadamente o direito à proteção de dados.[255]

7.2. Legislação da UE sobre proteção de dados em matéria policial e penal

Pontos-chave

- Ao nível da UE, a proteção de dados no setor policial e da justiça penal só está regulada no contexto da cooperação transfronteiriça entre as autoridades policiais e judiciárias.
- Foram estabelecidos regimes especiais de proteção de dados para o Serviço Europeu de Polícia (Europol) e a Unidade Europeia de Cooperação Judiciária (Eurojust), dois órgãos da UE que apoiam e promovem a aplicação efetiva da lei transfronteiras.

254 Conselho da Europa, Comité de Ministros (2001), Convenção sobre o Cibercrime, STCE n.º 185, Budapeste, 23 de novembro de 2001, que entrou em vigor em 1 de julho de 2004.

255 *Ibid.,* artigo 15.º, n.º 1.

- Existem também regimes especiais de proteção de dados para os sistemas de informação comuns que foram estabelecidos ao nível da UE para fins de intercâmbio transfronteiriço de informações entre as autoridades policiais e judiciárias competentes. São exemplos importantes o Schengen II, o Sistema de Informação sobre Vistos (VIS) e o Eurodac, um sistema centralizado que contém os dados dactiloscópicos de nacionais de países terceiros que apresentem um pedido de asilo num dos Estados-Membros da UE.

A Diretiva de Proteção de Dados não é aplicável no domínio policial e da justiça penal. A secção 7.2.1 descreve os instrumentos jurídicos mais importantes nesta área.

7.2.1. A Decisão-Quadro relativa à proteção de dados

A Decisão-Quadro 2008/977/JAI do Conselho relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (*Decisão-Quadro relativa à proteção de dados*)[256] visa assegurar a proteção dos dados pessoais das pessoas singulares quando estes são tratados para efeitos de prevenção, investigação ou repressão de infrações penais ou de execução de sanções penais. Os Estados-Membros e a UE são representados por autoridades competentes que trabalham no setor policial ou da justiça penal. Estas autoridades são agências ou organismos da UE, bem como autoridades dos Estados-Membros.[257] A aplicabilidade da Decisão-Quadro está limitada à garantia da proteção dos dados no âmbito da cooperação transfronteiriça entre estas autoridades e não abrange a segurança nacional.

A Decisão-Quadro relativa à Proteção de Dados baseiase, em grande parte, nos princípios e definições constantes da Convenção 108 e da Diretiva de Proteção de Dados.

Os dados só podem ser utilizados por uma autoridade competente e exclusivamente para a finalidade para que foram transmitidos ou disponibilizados. O Estado-Membro destinatário é obrigado a respeitar as restrições ao intercâmbio de dados eventualmente impostas pela legislação do Estado-Membro transmitente. Porém, em certos casos, o Estado destinatário pode utilizar os dados para uma finalidade diferente. As autoridades competentes têm o dever específico de registar e documentar as transmissões, com vista a ajudar a identificar claramente as responsabilidades

256 Conselho da União Europeia (2008), Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais no âmbito da cooperação policial e judiciária em matéria penal (*Decisão-Quadro relativa à proteção de dados*), JO 2008 L 350.

257 *Ibid.,* artigo 2.º, al. h)

emergentes de queixas. A transferência ulterior de dados recebidos no âmbito da cooperação transfronteira para terceiros exige o consentimento do Estado-Membro de onde os dados provêm, embora estejam previstas exceções para casos urgentes.

As autoridades competentes devem tomar as medidas de segurança necessárias para proteger os dados pessoais contra qualquer forma ilícita de tratamento.

Cada Estado-Membro deve assegurar a designação de uma ou várias autoridades nacionais de controlo responsáveis pelo aconselhamento e pela fiscalização da aplicação das disposições adotadas nos termos da Decisão-Quadro relativa à proteção de dados. Qualquer pessoa pode apresentar à autoridade de controlo um pedido de proteção dos seus direitos e liberdades no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes.

A pessoa em causa tem o direito de ser informada sobre o tratamento dos seus dados pessoais, bem como o direito de acesso, retificação, apagamento ou bloqueio. Quando o exercício destes direitos for recusado por razões preponderantes, a pessoa em causa deve ter o direito de recorrer para a autoridade nacional de controlo competente e/ou para um tribunal. Qualquer pessoa que sofra um prejuízo devido a violações das disposições nacionais de execução da Decisão-Quadro relativa à proteção de dados tem o direito de obter uma indemnização do responsável pelo tratamento.[258] De um modo geral, as pessoas em causa devem poder recorrer judicialmente em caso de violação dos direitos garantidos pela legislação nacional de execução da Decisão-Quadro relativa à proteção de dados.[259]

A Comissão Europeia propôs uma reforma legislativa, que consiste num Regulamento geral sobre a proteção de dados,[260] e numa Diretiva geral sobre a proteção de dados.[261] Esta nova diretiva irá substituir a atual Diretiva de Proteção de Dados e aplicar princípios e regras gerais à cooperação policial e judiciária em matéria penal.

258 *Ibid.,* artigo 19.º.

259 *Ibid.,* artigo 20.º.

260 Comissão Europeia (2012), *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) 11 final, Bruxelas, 25 de janeiro de 2012.

261 Comissão Europeia (2012), *Proposta de Diretiva do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados (Diretiva geral sobre a proteção de dados)*, COM(2012) 10 final, Bruxelas, 25 de janeiro de 2012.

7.2.2. Instrumentos jurídicos mais específicos sobre a proteção de dados no âmbito da cooperação transfronteiriça entre autoridades policiais e judiciárias

Para além da Decisão-Quadro relativa à proteção de dados, existem outros instrumentos jurídicos que regulam o intercâmbio de informações detidas pelos Estados-Membros em áreas específicas, tais como a Decisão-Quadro 2009/315/JAI do Conselho relativa à organização e ao conteúdo do intercâmbio de informações extraídas do registo criminal entre os Estados-Membros e a Decisão do Conselho relativa a disposições de cooperação entre as unidades de informação financeira dos Estados-Membros em matéria de troca de informações.[262]

Importa salientar que a cooperação transfronteiriça[263] entre as autoridades competentes envolve, cada vez mais, o intercâmbio de dados sobre imigração. Esta área do direito não se enquadra no domínio policial e da justiça penal, mas é, em muitos aspetos, relevante para o trabalho das autoridades policiais e judiciárias. O mesmo é válido em relação aos dados sobre mercadorias importadas para a UE ou exportadas da UE. A eliminação dos controlos fronteiriços internos dentro da UE exacerbou o risco de fraude, obrigando os Estados-Membros a intensificar a cooperação, sobretudo através do reforço do intercâmbio transfronteiriço de informações, a fim de detetar e reprimir mais eficazmente atos que violem a legislação aduaneira nacional e da UE.

A Decisão Prüm

Um exemplo importante da cooperação transfronteiras institucionalizada através do intercâmbio de dados detidos por autoridades nacionais é a Decisão 2008/615/JAI do Conselho relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras (*Decisão*

262 Conselho da União Europeia (2009), Decisão-Quadro 2009/315/JAI do Conselho, de 26 de fevereiro de 2009, relativa à organização e ao conteúdo do intercâmbio de informações extraídas do registo criminal entre os Estados-Membros, JO 2009 L 93; Conselho da União Europeia (2000), Decisão 2000/642/JAI do Conselho, de 17 de outubro de 2000, relativa a disposições de cooperação entre as unidades de informação financeira dos Estados-Membros em matéria de troca de informações, JO 2000 L 271.

263 Comissão Europeia (2012), Comunicação da Comissão ao Parlamento Europeu e ao Conselho – Reforçar a cooperação em matéria de aplicação da lei na UE: o modelo europeu de intercâmbio de informações (EIXM), COM(2012) 735 final, Bruxelas, 7 de dezembro de 2012.

Prüm), que incorporou o Tratado de Prüm no direito da UE em 2008.[264] O Tratado de Prüm era um acordo internacional sobre cooperação policial assinado em 2005 pela Áustria, Bélgica, França, Alemanha, Luxemburgo, Países Baixos e Espanha.[265]

A Decisão Prüm visa ajudar os Estados-Membros a melhorar a partilha de informações para fins de prevenção e de luta contra a criminalidade em três domínios: terrorismo, criminalidade transfronteiras e migração ilegal. Para esse efeito, a Decisão estabelece disposições relativas:

- ao acesso automatizado a perfis de ADN, a dados dactiloscópicos e a certos dados do registo nacional de veículos;
- ao fornecimento de dados relacionados com eventos importantes de alcance transfronteiriço;
- ao fornecimento de informações para a prevenção de atentados terroristas;
- a outras medidas de aprofundamento da cooperação policial transfronteiras.

As bases de dados disponibilizadas ao abrigo da Decisão Prüm são inteiramente reguladas pelo direito nacional, mas o intercâmbio de dados é simultaneamente regulado pela Decisão e, mais recentemente, pela Decisão-Quadro relativa à proteção de dados. Os órgãos competentes para fiscalizar estes fluxos de dados são as autoridades nacionais de controlo responsáveis pela proteção de dados.

7.2.3. Proteção de dados na Europol e na Eurojust

Europol

A Europol, o serviço de polícia da UE, tem a sua sede na Haia, existindo uma Unidade Nacional Europol (UNE) em cada Estado-Membro. A Europol foi criada em 1998; o seu atual estatuto jurídico como instituição da UE tem por base a Decisão do

264 Conselho da União Europeia (2008), Decisão 2008/615/JAI do Conselho, de 23 de junho de 2008, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras, JO 2008 L 210.

265 Convenção entre o Reino da Bélgica, a República Federal da Alemanha, o Reino de Espanha, a República Francesa, o GrãoDucado do Luxemburgo, o Reino dos Países Baixos e a República da Áustria relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras, disponível em: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

Conselho que cria o Serviço Europeu de Polícia (*Decisão Europol*).[266] A Europol tem por objetivo apoiar a prevenção e a investigação da criminalidade organizada, do terrorismo e de outras formas graves de criminalidade, enumeradas no anexo à Decisão Europol, que afetem dois ou mais Estados-Membros.

A fim de atingir os seus objetivos, a Europol criou o Sistema de Informações Europol, que proporciona uma base de dados para os Estados-Membros trocarem dados e informações de natureza penal através das respetivas UNE. O Sistema de Informações Europol apenas pode ser utilizado para disponibilizar dados relativos a: pessoas que sejam suspeitas da prática de uma infração penal da competência da Europol ou que tinham sido condenadas por alguma dessas infrações; ou pessoas relativamente às quais haja indícios factuais de que tenham praticado essas infrações. A Europol e as UNE podem introduzir diretamente dados no Sistema de Informações Europol e consultálos. Apenas a parte que introduziu os dados no sistema pode proceder à sua alteração, retificação ou apagamento.

Quando tal seja necessário para o desempenho das suas funções, a Europol pode conservar, alterar e utilizar dados relativos a infrações penais em ficheiros de análise. Os ficheiros de análise são criados para efeitos de compilação, tratamento ou utilização de dados com o objetivo de apoiar investigações criminais concretas conduzidas pela Europol em conjunto com os Estados-Membros da UE.

Em resposta aos novos desenvolvimentos, foi criado o Centro Europeu da Cibercriminalidade no seio da Europol em 1 de janeiro de 2013.[267] O centro serve de ponto de convergência europeu das informações sobre cibercriminalidade, contribuindo para reações mais rápidas no caso dos crimes em linha, desenvolvendo e implementando funcionalidades forenses digitais e aplicando as melhores práticas no domínio da investigação de cibercrimes. O centro dedica especial atenção aos cibercrimes que:

266 Conselho da Europa (2009), Decisão do Conselho, de 6 de abril de 2009, que cria o Serviço Europeu de Polícia (Europol), JO 2009 L 121. Ver também a Proposta da Comissão para um regulamento que prevê, por conseguinte, um quadro jurídico para uma nova Europol, que substitui e sucede à Europol criada pela Decisão 2009/371/JAI do Conselho, de 6 de abril de 2009, que cria o Serviço Europeu de Polícia (Europol) , bem como à CEPOL criada pela Decisão 2005/681/JAI do Conselho, que cria a Academia Europeia de Polícia (CEPOL), COM(2013) 173 final.

267 Ver também AEPD (2012), *Parecer da Autoridade Europeia para a Proteção de Dados sobre a Comunicação da Comissão Europeia ao Conselho e ao Parlamento Europeu relativa à criação de um Centro Europeu da Cibercriminalidade*, Bruxelas, 29 de junho de 2012 [apenas está disponível em PT a síntese do parecer].

- são praticados por grupos criminosos organizados para gerar grandes lucros, como a fraude em linha;
- causam danos graves às vítimas, como a exploração sexual de crianças em linha;
- afetam infraestruturas e sistemas de informação críticos da UE.

O regime de proteção de dados aplicável às atividades da Europol é reforçado. No seu artigo 27.º, a Decisão Europol estabelece a aplicabilidade dos princípios consagrados na Convenção 108 e na Recomendação sobre a atividade policial em matéria de tratamento de dados automatizados e não automatizados. A transmissão de dados entre a Europol e os Estados-Membros também tem de respeitar as regras previstas na Decisão-Quadro relativa à proteção de dados.

A fim de assegurar o cumprimento da legislação sobre proteção de dados aplicável e, em especial, que o tratamento de dados pessoais não viola os direitos das pessoas, a Instância Comum de Controlo (ICC) fiscaliza e controla as atividades da Europol.[268] Todas as pessoas têm o direito de acesso a quaisquer dados pessoais que a Europol mantenha a seu respeito, bem como o direito de requerer a verificação, retificação ou apagamento dos mesmos. Se uma pessoa não ficar satisfeita com a decisão da Europol sobre o exercício destes direitos, poderá recorrer para o Comité de Recursos da ICC.

Se ocorrerem danos devido à existência de erros de facto ou de direito nos dados conservados ou tratados pela Europol, a parte lesada só poderá recorrer ao tribunal competente do Estado-Membro onde ocorreu o facto gerador do dano.[269] A Europol reembolsará o Estado-Membro se os danos resultarem do incumprimento das suas obrigações legais.

Eurojust

Criada em 2002, a Eurojust é um órgão da UE com sede na Haia, que promove a cooperação judiciária no âmbito de investigações e procedimentos penais relacionados

268 Decisão Europol, artigo 34.º

269 *Ibid.*, artigo 52.º

com formas graves de criminalidade que impliquem dois ou mais Estados-Membros.[270] A Eurojust é competente para:

- incentivar e melhorar a coordenação das investigações e procedimentos penais entre as autoridades dos vários Estados-Membros;

- facilitar a execução de pedidos e decisões relacionados com cooperação judiciária.

As funções da Eurojust são desempenhadas por membros nacionais. Cada Estado-Membro destaca um juiz ou procurador para a Eurojust, cujo estatuto está sujeito ao direito nacional e a quem são atribuídas as competências exigidas para o desempenho das funções necessárias ao incentivo e melhoria da cooperação judiciária. Além disso, os membros nacionais atuam colegialmente para desempenhar funções especiais da Europol.

A Eurojust pode tratar dados pessoais, desde que tal seja necessário para alcançar os seus objetivos. Porém, este tratamento está limitado a informações específicas sobre pessoas suspeitas da prática ou da participação em infrações penais da competência da Eurojust ou condenadas por tais infrações. A Eurojust também pode tratar certas informações sobre testemunhas ou vítimas de infrações penais abrangidas pela sua esfera de competência.[271] Em casos excecionais, a Eurojust pode tratar, durante um período de tempo limitado, outros dados pessoais relativos às circunstâncias em que foi cometida uma infração quando os mesmos seja de interesse imediato para uma investigação em curso. No âmbito da sua competência, a Eurojust pode cooperar e trocar dados pessoais com outras instituições, órgãos e agências da UE. A Eurojust pode igualmente cooperar e trocar dados pessoais com organizações e países terceiros.

Relativamente à proteção de dados, a Eurojust deve garantir um nível de proteção pelo menos equivalente aos princípios consagrados na Convenção 108 do Conselho

270 Conselho da União Europeia (2002), Decisão 2002/187/JAI do Conselho, de 28 de fevereiro de 2002, relativa à criação da Eurojust a fim de reforçar a luta contra as formas graves de criminalidade, JO 2002 L 63; Conselho da União Europeia (2003), Decisão 2003/659/JAI do Conselho, de 18 de junho de 2003, que altera a Decisão 2002/187/JAI do Conselho relativa à criação da Eurojust a fim de reforçar a luta contra as formas graves de criminalidade, JO 2003 L 245; Conselho da União Europeia (2009), Decisão 2009/426/JAI do Conselho, de 16 de dezembro de 2008, relativa ao reforço da Eurojust e que altera a Decisão 2002/187/JAI do Conselho relativa à criação da Eurojust a fim de reforçar a luta contra as formas graves de criminalidade, JO 2009 L 138 (*Decisões Eurojust*).

271 Versão consolidada da Decisão 2002/187/JAI do Conselho, na redação que lhe foi dada pela Decisão 2003/659/JAI do Conselho e pela Decisão 2009/426/JAI do Conselho, artigo 15.º, n.º 2.

da Europa na redação em vigor. Em casos de intercâmbio de dados, devem ser respeitadas regras e limitações específicas, que são estabelecidas em acordos ou mecanismos de cooperação em conformidade com as Decisões Eurojust do Conselho e as Regras da Eurojust relativas à proteção dados.[272]

Foi criada uma ICC independente da Eurojust, que é responsável pelo controlo do tratamento de dados pessoais efetuado por esta. As pessoas que não estiverem satisfeitas com a resposta dada pela Eurojust a um pedido de acesso, retificação, bloqueio ou apagamento de dados pessoais podem recorrer para a ICC. Se a Eurojust tratar ilicitamente dados pessoais, será responsável, em conformidade com a legislação nacional do Estado-Membro onde se situa a sua sede, os Países Baixos, por quaisquer danos causados à pessoa em causa.

7.2.4. Proteção de dados nos sistemas de informação comuns ao nível da UE

Para além do intercâmbio de dados entre os Estados-Membros e a criação de autoridades da UE especializadas com o objetivo de combater a criminalidade transfronteiriça, foram estabelecidos vários sistemas de informação comuns ao nível da UE para servir de plataforma ao intercâmbio de dados entre as autoridades nacionais e da UE competentes para determinados fins de aplicação da lei, nomeadamente no domínio aduaneiro e da imigração. Alguns destes sistemas resultaram de acordos multilaterais que foram posteriormente complementados por sistemas e instrumentos jurídicos da UE, tais como o Sistema de Informação de Schengen, o Sistema de Informação sobre Vistos, o Eurodac, o Eurosur ou o Sistema de Informação Aduaneiro.

A Agência Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala (eu-LISA),[273] criada em 2012, é responsável pela gestão operacional a longo prazo do Sistema de Informação de Schengen de segunda geração (SIS II), do Sistema de Informação sobre Vistos (VIS) e do Eurodac. A principal função da euLISA consiste em assegurar o funcionamento eficaz, seguro e ininterrupto dos sistemas informáticos. É igualmente responsável pela adoção das medidas necessárias para garantir a segurança dos sistemas e dos dados.

272 Disposições do Regulamento Interno da Eurojust relativas ao Tratamento e à Proteção de Dados Pessoais, JO 2005 C 68/01, 19 de março de 2005, p. 1.

273 Regulamento (UE) n.º 1077/2011 do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, que cria uma Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça, JO 2011 L 286.

O Sistema de Informação de Schengen

Em 1985, vários Estados-Membros das antigas Comunidades Europeias celebraram o Acordo entre os Estados da União Económica Benelux, a Alemanha e a França relativo à supressão gradual dos controlos nas suas fronteiras comuns (*Acordo de Schengen*), com o objetivo de criar um espaço de livre circulação de pessoas, sem controlos fronteiriços, dentro do território Schengen.[274] A fim de neutralizar a ameaça para a segurança pública suscetível de resultar da abertura das fronteiras, foram reforçados os controlos nas fronteiras externas do espaço Schengen e estabelecida uma estreita cooperação entre as autoridades policiais e judiciárias nacionais.

Em virtude da adesão de outros Estados ao Acordo de Schengen, o sistema Schengen foi finalmente integrado no quadro jurídico da UE pelo Tratado de Amesterdão.[275] Esta decisão foi implementada em 1999. A mais recente versão do Sistema de Informação de Schengen, o chamado SIS II, entrou em funcionamento em 9 de abril de 2013. Este sistema serve agora todos os Estados-Membros da UE e ainda a Islândia, o Listenstaine, a Noruega e a Suíça.[276] A Europol e a Eurojust também têm acesso ao SIS II.

O SIS II é composto por um sistema central (CSIS), um sistema nacional (NSIS) em cada Estado-Membro e uma infraestrutura de comunicação ente o sistema central e os sistemas nacionais. O CSIS contém certos dados introduzidos pelos Estados-Membros sobre pessoas e objetos. O CSIS é utilizado pelas autoridades nacionais responsáveis pelo controlo fronteiriço e pela emissão de vistos, bem como pelas autoridades policiais, aduaneiras e judiciárias nacionais em todo o espaço Schengen. Cada um dos Estados-Membros gere uma cópia nacional do CSIS os Sistemas Nacionais de Informação de Schengen (NSIS) que é constantemente atualizada, atualizando assim o CSIS. O NSIS é consultado e emitirá uma indicação quando:

274 Acordo entre os Governos dos Estados da União Económica Benelux, da República Federal da Alemanha e da República Francesa relativo à supressão gradual dos controlos nas fronteiras comuns, JO 2000 L 239.

275 Comunidades Europeias (1997), Tratado de Amesterdão que altera o Tratado da União Europeia, os Tratados que instituem as Comunidades Europeias e alguns atos relativos a esses Tratados, JO 1997 C 340.

276 Regulamento (CE) n.º 1987/2006 do Parlamento Europeu e do Conselho, de 20 de dezembro de 2006, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen de segunda geração, JO 2006 L 381 (*SIS II*) e Conselho da União Europeia (2007), Decisão 2007/533/JAI do Conselho, de 12 de junho de 2007, relativa ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação Schengen de segunda geração (*SIS II*), JO 2007 L 205.

- a pessoa não tiver o direito de entrar ou permanecer no território Schengen;
- a pessoa ou objeto for procurado por autoridades policiais ou judiciárias;
- tiver sido participado o desaparecimento da pessoa; ou
- tiver sido participado o furto ou extravio das mercadorias, nomeadamente notas de banco, automóveis, carrinhas, armas de fogo e documentos de identificação.

Caso seja emitida uma indicação, devem ser iniciadas atividades de seguimento através dos Sistemas Nacionais de Informação de Schengen.

O SIS II possui novas funcionalidades, nomeadamente a possibilidade de introduzir: dados biométricos, tais como impressões digitais e fotografias; ou novas categorias de indicações, tais como embarcações, aeronaves, contentores ou meios de pagamento furtados; e melhores indicações sobre pessoas e objetos; cópias dos mandados de detenção europeus (MDE) emitidos contra pessoas procuradas para efeitos de detenção, entrega ou extradição.

A Decisão 2007/533/JAI do Conselho relativa ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação Schengen de segunda geração (Decisão Schengen II) incorpora a Convenção 108: «Os dados pessoais tratados em aplicação da presente decisão são protegidos nos termos da Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal».[277] Sempre que as autoridades policiais nacionais utilizem dados pessoais em aplicação da Decisão Schengen II, as disposições da Convenção 108, bem como da Recomendação sobre a atividade policial, têm de ser implementadas no direito nacional.

A autoridade nacional de controlo competente em cada Estado-Membro é responsável pela supervisão do NSIS interno. Deve, em especial, verificar a qualidade dos dados que o Estado-Membro introduz no CSIS através do NSIS. A autoridade nacional de controlo deve assegurar a realização de uma auditoria às operações de tratamento de dados no NSIS interno pelo menos de quatro em quatro anos. As autoridades nacionais de controlo e a AEPD cooperam e asseguram a supervisão coordenada do SIS, sendo a AEPD responsável pela supervisão do C-SIS. Por uma questão

277 Conselho da União Europeia (2007), Decisão 2007/533/JAI do Conselho, de 12 de junho de 2007, relativa ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação Schengen de segunda geração, JO 2007 L 205, artigo 57.º

de transparência, é enviado um relatório conjunto de atividades para o Parlamento Europeu, o Conselho e a euLISA de dois em dois anos.

As pessoas podem exercer os seus direitos de acesso relativos ao SIS II em qualquer Estado-Membro, dado que cada N-SIS é uma cópia exata do CSIS.

> Exemplo: No processo que deu origem ao acórdão *Dalea c. França*,[278] foi recusado ao requerente um visto para visitar França, dado que as autoridades francesas tinham comunicado ao Sistema de Informação Schengen que a entrada dessa pessoa deveria ser recusada. O requerente procurou exercer, sem êxito, os seus direitos de acesso e retificação ou apagamento dos dados perante a Comissão para a Proteção de Dados francesa e, em última instância, perante o Conselho de Estado. O TEDH considerou que a inclusão do requerente no Sistema de Informação de Schengen tinha sido efetuada de acordo com a lei e tinha prosseguido o objetivo legítimo de defender a segurança nacional. Uma vez que o requerente não demonstrara os danos efetivamente sofridos em resultado da recusa de entrada no espaço Schengen e dada que tinham sido adotadas medidas suficientes para o proteger de decisões arbitrárias, a ingerência no exercício do seu direito ao respeito pela vida privada tinha sido proporcional. Por conseguinte, a queixa do requerente ao abrigo do artigo 8.º foi declarada inadmissível.

O Sistema de Informação sobre Vistos

O Sistema de Informação sobre Vistos (VIS), também da responsabilidade da eu-LISA, foi desenvolvido com o objetivo de apoiar a implementação de uma política comum em matéria de vistos ao nível da UE.[279] O VIS permite aos Estados Schengen trocar dados sobre vistos através de um sistema que estabelece a ligação entre os consulados desses Estados em países não pertencentes à UE e pontos de passagem

278 TEDH, acórdão *Dalea c. França* (decisão sobre a admissibilidade) de 2 de fevereiro de 2010, petição n.º 964/07.

279 Conselho da União Europeia (2004), Decisão do Conselho de 8 de junho de 2004 que estabelece o Sistema de Informação sobre Vistos (VIS), JO 2004 L 213; Regulamento (CE) n.º 767/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, relativo ao Sistema de Informação sobre Vistos (VIS) e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração, JO 2008 L 218 (*Regulamento VIS*); Conselho da União Europeia (2008), Decisão 2008/633/JAI do Conselho, de 23 de junho de 2008, relativa ao acesso para consulta ao Sistema de Informação sobre Vistos (VIS) por parte das autoridades designadas dos Estados-Membros e por parte da Europol para efeitos de prevenção, deteção e investigação de infrações terroristas e outras infrações penais graves, JO 2008 L 218.

das fronteiras externas. O VIS trata dados relativos a pedidos de vistos de curta duração apresentados por pessoas que pretendem visitar ou que se encontram em trânsito pelo espaço Schengen. O VIS permite que as autoridades fronteiriças verifiquem, com o auxílio de dados biométricos, se a pessoa que apresenta o visto é ou não o seu legítimo titular e identifiquem pessoas sem documentos ou com documentos obtidos fraudulentamente.

Nos termos do Regulamento (CE) n.º 767/2008 do Parlamento Europeu e do Conselho relativo ao Sistema de Informação sobre Vistos (VIS) e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração (*Regulamento VIS*), apenas podem ser registados no VIS dados sobre o requerente, os seus vistos, fotografias, impressões digitais, ligações para pedidos anteriores e processos de pedidos de visto das pessoas que o acompanham.[280] O acesso ao VIS para introduzir, alterar ou apagar dados está reservado às autoridades responsáveis pela emissão de vistos dos Estados-Membros, enquanto o acesso para consulta dos dados é concedido às autoridades responsáveis pela emissão de vistos e às autoridades competentes para realizar controlos nos pontos de passagem das fronteiras externas e controlos em matéria de imigração e de asilo. Em certas condições, as autoridades policiais nacionais competentes e a Europol podem requerer o acesso a dados introduzidos no VIS para efeitos de prevenção, deteção e investigação de infrações terroristas e infrações penais.[281]

Eurodac

O nome do Eurodac tem origem na palavra «dactilograma», ou seja, impressão digital. Tratase de um sistema centralizado que contém os dados dactiloscópicos de nacionais de países terceiros que pedem asilo num dos Estados-Membros da UE.[282] O sistema está operacional desde janeiro de 2003 e visa ajudar a determinar que

280 Artigo 5.º do Regulamento (CE) n.º 767/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, relativo ao Sistema de Informação sobre Vistos (VIS) e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração (*Regulamento VIS*), JO 2008 L 218.

281 Conselho da União Europeia (2008), Decisão 2008/633/JAI do Conselho, de 23 de junho de 2008, relativa ao acesso para consulta ao Sistema de Informação sobre Vistos (VIS) por parte das autoridades designadas dos Estados-Membros e por parte da Europol para efeitos de prevenção, deteção e investigação de infrações terroristas e outras infrações penais graves, JO 2008 L 218.

282 Regulamento (CE) n.º 2725/2000 do Conselho, de 11 de dezembro de 2000, relativo à criação do sistema «Eurodac» de comparação de impressões digitais para efeitos da aplicação efetiva da Convenção de Dublim, JO 2000 L 316; Regulamento (CE) n.º 407/2002 do Conselho, de 28 de fevereiro de 2002, que fixa determinadas regras de execução do Regulamento CE) n.º 2725/2000 relativo à criação do sistema «Eurodac» de comparação de impressões digitais para efeitos da aplicação efetiva da Convenção de Dublim, JO 2002 L 62 (*Regulamento Eurodac*).

Estado-Membro deveria ser responsável pela análise de um determinado pedido de asilo ao abrigo do Regulamento (CE) n.º 343/2003 do Conselho que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de asilo apresentado num Estado-Membro por um nacional de um país terceiro (*Regulamento Dublim II*).[283] Os dados pessoais constantes do Eurodac só podem ser utilizados para efeitos de facilitar a aplicação do Regulamento Dublim II; qualquer outra utilização está sujeita a sanções.

O Eurodac consiste numa unidade central, gerida pela eu-LISA, para registar e comparar impressões digitais, e um sistema de transmissão eletrónica de dados entre os Estados-Membros e a base de dados central. Os Estados-Membros recolhem e transmitem as impressões digitais de todos os nacionais de países terceiros ou apátridas com, pelo menos, 14 anos que peçam asilo no seu território ou que sejam intercetadas por ocasião da passagem não autorizada da sua fronteira externa. Os Estados-Membros podem igualmente recolher e transmitir as impressões digitais de nacionais de países terceiros ou apátridas cuja permanência no seu território não esteja autorizada.

Os dados dactiloscópicos são registados na base de dados Eurodac sob forma pseudonimizada. Em caso de concordância, o pseudónimo, juntamente com o nome do primeiro Estado-Membro que transmitiu os dados dactiloscópicos, é divulgado ao segundo Estado-Membro. O segundo Estado-Membro contactará então o primeiro Estado-Membro porque, nos termos do Regulamento Dublim II, o primeiro Estado-Membro é responsável pelo tratamento do pedido de asilo.

Os dados pessoais registados no Eurodac que digam respeito a requerentes de asilo são conservados por um período de 10 anos a contar da data em que as impressões digitais foram recolhidas, salvo se a pessoa em causa adquirir a cidadania de um Estado-Membro da UE. Neste caso, os dados devem ser imediatamente apagados. Os dados relativos a nacionais de países estrangeiros que tenham sido intercetados por ocasião da passagem não autorizada da fronteira externa são conservados por um período de dois anos. Se a pessoa em causa obtiver uma autorização de residência, abandonar o território da UE ou adquirir a cidadania de um Estado-Membro, os dados devem ser imediatamente apagados.

283 Regulamento (CE) n.º 343/2003 do Conselho, de 18 de fevereiro de 2003, que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de asilo apresentado num Estado-Membro por um nacional de um país terceiro (*Regulamento Dublim II*), JO 2003 L 50.

Para além de todos os Estados-Membros da UE, a Islândia, a Noruega, o Listenstaine e a Suíça também utilizam o Eurodac com base em acordos internacionais.

Eurosur

O Sistema Europeu de Vigilância das Fronteiras (*Eurosur*)[284] pretende melhorar o controlo das fronteiras externas do espaço Schengen através da deteção, prevenção e combate à imigração ilegal e à criminalidade transfronteiriça. O Eurosur visa reforçar o intercâmbio de informações e a cooperação operacional entre os centros nacionais de coordenação e a Frontex, a agência da UE responsável pelo desenvolvimento e aplicação do novo modelo de gestão integrada das fronteiras.[285] Os seus objetivos gerais são os seguintes:

- reduzir o número de migrantes ilegais que entram na UE sem serem detetados;
- reduzir o número de mortes de migrantes ilegais, salvando mais vidas no mar;
- reforçar a segurança interna da UE no seu todo através da contribuição para a prevenção da criminalidade transfronteiriça.[286]

Entrou em funcionamento em 2 de dezembro de 2013 em todos os Estados-Membros com fronteiras externas e começará a ser implementado a partir de 1 de dezembro de 2014 nos restantes. O Regulamento será aplicável à vigilância das fronteiras externas terrestres e marítimas e das fronteiras aéreas dos Estados-Membros.

284 Regulamento (UE) n.º 1052/2013 do Parlamento Europeu e do Conselho, de 22 de outubro de 2013, que cria o Sistema Europeu de Vigilância das Fronteiras (Eurosur), JO 2013 L 295.

285 Regulamento (UE) n.º 1168/2011 do Parlamento Europeu e do Conselho, de 25 de outubro de 2011, que altera o Regulamento (CE) n.º 2007/2004 do Conselho que cria uma Agência Europeia de Gestão da Cooperação Operacional nas Fronteiras Externas dos Estados-Membros da União Europeia (*Regulamento Frontex*), JO 2011 L 394.

286 Ver também: Comissão Europeia (2008), Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões intitulada «Análise da criação de um Sistema Europeu de Vigilância das Fronteiras (Eurosur), COM(2008) 68 final, Bruxelas, 13 de fevereiro de 2008; Comissão Europeia (2011), Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (Eurosur) (Avaliação de impacto que acompanha a Proposta de Regulamento do Parlamento Europeu e do Conselho que cria o Sistema Europeu de Vigilância das Fronteiras [Eurosur]), Documento de trabalho dos serviços da Comissão, SEC(2011) 1536 final, Bruxelas, 12 de dezembro de 2011, p. 18.

Sistema de Informação Aduaneiro

Outro importante sistema de informação comum estabelecido ao nível da UE é o Sistema de Informação Aduaneiro (SIA).[287] Durante o processo de criação de um mercado interno, foram abolidos todos os controlos e formalidades em relação às mercadorias que entravam no território da UE, o que exacerbou o risco de fraude. Este risco foi contrabalançado pela intensificação da cooperação entre as administrações aduaneiras dos Estados-Membros. O SIA tem por objetivo auxiliar os Estados-Membros na prevenção, investigação e repressão de violações graves da legislação aduaneira e agrícola nacional e da UE.

As informações contidas no SIA abrangem dados pessoais relacionados com mercadorias, meios de transporte, empresas, pessoas e retenções, apreensões ou confiscos de mercadorias e de dinheiro líquido. Estas informações só podem ser utilizadas para efeitos de observação e informação, realização de controlos específicos ou de análise estratégia ou operacional relativamente a pessoas suspeitas de violarem disposições aduaneiras.

O acesso ao SIA é concedido às autoridades aduaneiras, fiscais, agrícolas, policiais e de saúde pública nacionais, bem como à Europol e à Eurojust.

O tratamento de dados pessoais tem de cumprir as regras específicas estabelecidas pelo Regulamento n.º 515/97 e pela Decisão SIA,[288] bem como as disposições da Diretiva de Proteção de Dados, do Regulamento Proteção de Dados (Instituições da UE), da Convenção 108 e da Recomendação sobre a atividade policial. A Autoridade de Controlo Comum (ACC) do SIA supervisiona a aplicação da Decisão SAI, enquanto a AEPD é responsável pela supervisão da observância do Regulamento n.º 45/2001 e convoca, pelo menos uma vez por ano, uma reunião com todas as autoridades nacionais de proteção de dados, competentes pelas questões de supervisão do sistema aduaneiro.

287 Conselho da União Europeia (1995), Ato do Conselho, de 26 de julho de 1995, que institui a Convenção sobre a utilização da informática no domínio aduaneiro, JO 1995 C 316, com a redação que lhe foi dada pela Decisão 2009/917/JAI do Conselho, de 30 de novembro de 2009, relativa à utilização da informática no domínio aduaneiro, JO 2009 L 323 (*Decisão SIA*). Regulamento (CE) n.º 515/97 do Conselho, de 13 de março de 1997, relativo à assistência mútua entre as autoridades administrativas dos Estados-membros e à colaboração entre estas e a Comissão, tendo em vista assegurar a correta aplicação das regulamentações aduaneira e agrícola.

288 *Ibid*.

8

Outra legislação europeia específica sobre proteção de dados

UE	Questões abrangidas	CdE
Diretiva de Proteção de Dados Diretiva Privacidade Eletrónica	**Comunicações eletrónicas**	Convenção 108 Recomendação sobre os serviços de telecomunicações
Diretiva de Proteção de Dados, artigo 8.º, n.º 2, al. b)	**Relações de emprego**	Convenção 108 Recomendação sobre o emprego
		TEDH, acórdão *Copland c. Reino Unido* de 3 de abril de 2007, petição n.º 62617/00
Diretiva de Proteção de Dados, artigo 8.º, n.º 3	**Dados médicos**	Convenção 108 Recomendação sobre os dados médicos
		TEDH, acórdão *Z. c. Finlândia* de 25 de fevereiro de 1997, petição n.º 22009/93
Diretiva Ensaios Clínicos	**Ensaios clínicos**	
Diretiva de Proteção de Dados, artigo 6.º, n.º 1, al. b) e artigo 13.º, n.º 2	**Estatísticas**	Convenção 108 Recomendação sobre os dados estatísticos
Regulamento (CE) n.º 223/2009 relativo às Estatísticas Europeias TJUE, acórdão de 16 de dezembro de 2008 no processo C-524/06, *Huber/Alemanha*	**Estatísticas oficiais**	Convenção 108 Recomendação sobre os dados estatísticos

UE	Questões abrangidas	CdE
Diretiva 2004/39/CE relativa aos mercados de instrumentos financeiros Regulamento (UE) n.º 648/2012 relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações Regulamento (CE) n.º 1060/2009 relativo às agências de notação de risco Diretiva 2007/64/CE relativa aos serviços de pagamento no mercado interno	Dados financeiros	Convenção 108 Recomendação 90(19) sobre dados pessoais utilizados para fins de pagamento e outras operações conexas TEDH, acórdão *Michaud c. França* de 6 de dezembro de 2012, petição n.º 12323/11

Em vários casos, foram adotados instrumentos jurídicos especiais ao nível europeu, que aplicam, em maior detalhe, as regras gerais da Convenção 108 ou da Diretiva de Proteção de Dados a situações concretas.

8.1. Comunicações eletrónicas

Pontos-chave

- A Recomendação do CdE, de 1995 contém regras específicas sobre a proteção de dados na área das telecomunicações, em especial no âmbito dos serviços telefónicos.
- O tratamento de dados pessoais no contexto da prestação de serviços de comunicações ao nível da UE é regulado pela Diretiva Privacidade Eletrónica.
- A confidencialidade das comunicações eletrónicas abrange não apenas o teor da comunicação como também dados de tráfego, tais como informações sobre quem comunicou com quem, quando e por quanto tempo, e dados de localização, tais como o local de onde os dados foram comunicados.

As redes de comunicações comportam um risco acrescido de ingerência injustificada na esfera pessoal dos utilizadores, dado que oferecem possibilidades técnicas adicionais de escuta e vigilância das comunicações que têm lugar nessas redes. Consequentemente, foi considerado necessário adotar uma regulamentação especial em matéria de proteção de dados para responder aos riscos específicos suportados pelos utilizadores dos serviços de comunicação.

Em 1995, o CdE adotou uma Recomendação relativa à proteção de dados no domínio das telecomunicações, em especial dos serviços telefónicos.[289] Segundo esta recomendação, a recolha e o tratamento de dados pessoais no contexto das telecomunicações devem ter unicamente como finalidades: ligação de um utilizador à rede, disponibilização do serviço de telecomunicações em causa, faturação, verificação, garantia do melhor funcionamento técnico possível e desenvolvimento da rede e do serviço.

Foi também dada especial atenção à utilização das redes de comunicações para enviar mensagens de marketing direto. Em regra, não é permitido enviar mensagens de marketing direto a qualquer assinante que tenha expressamente manifestado a sua vontade de não receber mensagens publicitárias. Os sistemas de chamada automatizados que transmitem mensagens publicitárias prégravadas só podem ser utilizados se o assinante tiver dado o seu consentimento expresso. O direito nacional estabelecerá regras detalhadas neste domínio.

No que respeita ao **quadro jurídico da UE,** após uma primeira tentativa em 1997, a Diretiva relativa à privacidade e às comunicações eletrónicas (*Diretiva Privacidade Eletrónica*) foi adotada em 2002 e alterada em 2009, com o objetivo de complementar e adaptar as disposições da Diretiva de Proteção de Dados ao setor das telecomunicações**.**[290] A Diretiva Privacidade Eletrónica é exclusivamente aplicável aos serviços de comunicações em redes eletrónicas públicas.

A Diretiva Privacidade Eletrónica distingue três grandes categorias de dados gerados durante uma comunicação:

- os dados que constituem o teor das mensagens enviadas durante a comunicação; estes dados são estritamente confidenciais;

289 CdE, Comité de Ministros (1995), *Recommendation Rec(95)4 to member states on the protection of personal data in the area of telecommunication services, with particular reference to telephone services* (Recomendação Rec(95)4 aos Estados membros sobre a proteção de dados pessoais no domínio das telecomunicações, em especial dos serviços telefónicos), de 7 de fevereiro de 1995.

290 Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (*Diretiva relativa à privacidade e às comunicações eletrónicas)*, JO 2002 L 201, com a redação que lhe foi dada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor, JO 2009 L 337.

- os dados necessários para estabelecer e manter a comunicação, os chamados dados de tráfego, tais como informações sobre os parceiros, a hora e a duração da comunicação;

- dentro dos dados de tráfego, existem dados especificamente relacionados com a localização do dispositivo de comunicação, os chamados dados de localização; estes dados são simultaneamente dados sobre a localização *dos utilizadores* dos dispositivos de comunicação e particularmente relevantes em relação aos utilizadores de dispositivos de comunicação móvel.

Os dados de tráfego só podem ser utilizados pelo prestador de serviços para efeitos de faturação e se forem necessários, em termos técnicos, para prestar o serviço. Porém, com o consentimento da pessoa em causa, estes dados podem ser divulgados a outros responsáveis pelo tratamento que ofereçam serviços de valor acrescentado, tais como o fornecimento de informações sobre a estação de metro ou a farmácia mais próxima em relação à localização do utilizador ou a previsão meteorológica para este local.

Outro acesso a dados sobre comunicações em redes eletrónicas, tal como o acesso para fins de investigação de crimes, deve, segundo o artigo 15.º da Diretiva Privacidade Eletrónica, cumprir o requisito da ingerência justificada no exercício do direito à proteção de dados, conforme estabelecido no artigo 8.º, n.º 2, da CEDH e confirmado pela Carta nos seus artigos 8.º e 52.º.

Em 2009, foram introduzidas as seguintes alterações à Diretiva Privacidade Eletrónica:[291]

- As restrições ao envio de mensagens de correio eletrónico para fins de marketing direto foram alargadas aos serviços SMS, MMS e a outros tipos de aplicações similares; o envio de mensagens de correio eletrónico para fins de marketing é proibido, a menos que tenha sido obtido o consentimento prévio. Sem tal consentimento, este tipo de mensagem só pode ser enviado a antigos clientes que tenham fornecido o seu endereço de correio eletrónico e não se opuserem.

291 Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor, JO 2009 L 337.

- Foi imposta sobre os Estados-Membros a obrigação de estabelecerem vias de recurso judicial em caso de violação da proibição de envio de comunicações não solicitadas.[292]

- A instalação de testemunhos de conexão (*cookies*), um software que monitoriza e regista as ações dos utilizadores dos computadores, deixa de ser permitida sem o consentimento destes. O direito nacional deve regular mais detalhadamente o modo de manifestação e obtenção do consentimento, a fim de oferecer um nível suficiente de proteção.[293]

Sempre que ocorra uma violação de dados pessoais em virtude de acesso não autorizado, perda ou destruição de dados, a autoridade de controlo competente deve ser imediatamente informada. Os assinantes devem ser informados da possibilidade de sofreram danos devido a uma violação de dados pessoais.[294]

A Diretiva Conservação de Dados[295] (invalidada em 8 de abril de 2014) obrigava os prestadores de serviços de comunicações a manter os dados de tráfego disponíveis, especificamente para fins de combate aos crimes graves, durante um período não inferior a seis meses e não superior a dois anos, independentemente destes dados serem ou não ainda necessários para efeitos de faturação ou para prestar tecnicamente o serviço.

Os Estados-Membros da UE designarão autoridades públicas independentes, que são responsáveis pelo controlo da segurança dos dados conservados.

---

292 Ver a Diretiva alterada, artigo 13.º.

293 Ver *Ibid.*, artigo 5.º; ver também Grupo de Trabalho do artigo 29.º (2012*), Parecer 4/2012 sobre a isenção de consentimento para a utilização de testemunhos de conexão*, WP 194, Bruxelas, 7 de junho de 2012.

294 Ver também Grupo de Trabalho do artigo 29.º (2011), *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments* (Documento de Trabalho 01/2011 sobre o atual quadro jurídico da UE em matéria de violação de dados pessoais e recomendações sobre as políticas a adotar no futuro), WP 184, Bruxelas, 5 de abril de 2011.

295 Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE, JO 2006 L 105.

A conservação dos dados de telecomunicações é, sem dúvida, uma ingerência no exercício do direito à proteção de dados.[296] A justificabilidade desta ingerência tem sido contestada em vários processos judiciais nos Estados-Membros da UE[297].

Exemplo: No processo *Digital Rights Ireland e Seitlinger e Outros*[298], o TJUE declarou inválida a Diretiva Conservação de Dados. De acordo com o Tribunal, «esta diretiva comporta uma ingerência nestes direitos fundamentais de grande amplitude e particular gravidade na ordem jurídica da União, sem que essa ingerência seja enquadrada com precisão por disposições que permitam garantir que a mesma se limita efetivamente ao estritamente necessário».

Uma questão crucial no contexto das comunicações eletrónicas é a ingerência das autoridades públicas. Só é permitida a utilização de meios de vigilância ou interceção das comunicações, tais como dispositivos de escuta, se tal estiver previsto na lei e se constituir uma medida necessária numa sociedade democrática para salvaguardar a segurança do Estado, a segurança pública e os interesses monetários do Estado, reprimir infrações penais ou proteger a pessoa em causa ou os direitos e liberdades de terceiros.

Exemplo: No processo que deu origem ao acórdão *Malone c. Reino Unido*[299], o requerente tinha sido acusado de recetação. Durante o julgamento, foi revelado que uma conversa telefónica do requerente tinha sido intercetada com base num mandado emitido pelo ministro da Administração Interna. Embora a forma como a comunicação do requerente tinha sido intercetada fosse lícita nos termos do direito nacional, o TEDH entendeu que não estavam previstas regras jurídicas sobre o âmbito e o modo de exercício do poder discricionário atribuído às autoridades públicas neste domínio e que, consequentemente, a ingerência resultante da existência da prática em causa não estava «de acordo com a lei». O TEDH concluiu que tinha havido uma violação do artigo 8.º da CEDH.

296 AEPD (2011), *Parecer de 31 de maio de 2011 sobre o Relatório de avaliação da Comissão ao Conselho e ao Parlamento Europeu sobre a Diretiva relativa à conservação de dados (Diretiva 2006/24/CE)*, 31 de maio de 2011.

297 Alemanha, Tribunal Constitucional Federal (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 de março de 2010; Roménia, Tribunal Constitucional da Roménia (*Curtea Constituțională a României*), n.º 1258, 8 de outubro de 2009; Tribunal Constitucional da República Checa (*Ústavní soud České republiky*), 94/2011 Coll., 22 de março de 2011.

298 TJUE, acórdão de 8 de abril de 2014, processos apensos C-293/12 e C-594/12, *Digital Rights Ireland e Seitling e Outros*, ponto 65.

299 TEDH, acórdão *Malone c. Reino Unido* de 2 de agosto de 1984, petição n.º 8691/79.

8.2. Dados sobre o emprego

Pontos-chave

- A Recomendação do CdE relativa aos dados sobre emprego contém regras específicas aplicáveis à proteção de dados no contexto das relações de emprego.
- Na Diretiva de Proteção de Dados, as relações de emprego só são expressamente mencionadas no contexto do tratamento de dados sensíveis.
- A validade do consentimento, que tem de ser prestado livremente, como base legal do tratamento de dados sobre os funcionários poderá ser questionável, tendo em conta o desequilíbrio económico existente entre o empregador e os funcionários. As circunstâncias em que o consentimento é prestado devem ser cuidadosamente examinadas.

Não existe um quadro jurídico específico na UE aplicável ao tratamento de dados no contexto do emprego. Na Diretiva de Proteção de Dados, as relações de emprego só são expressamente mencionadas no artigo 8.º, n.º 2, que diz respeito ao tratamento de dados sensíveis. Relativamente ao CdE, a Recomendação relativa aos dados sobre emprego foi adotada em 1989 e está em fase de atualização.[300]

Um documento de trabalho do Grupo de Trabalho do artigo 29.º contém um estudo dos problemas de proteção de dados mais comuns no âmbito do emprego.[301] O grupo de trabalho analisou a relevância do consentimento enquanto base legal do tratamento de dados sobre o emprego,[302] tendo concluído que o desequilíbrio económico entre o empregador que pede o consentimento e o funcionário que dá esse consentimento suscitará frequentemente dúvidas sobre se o consentimento foi ou não prestado livremente. Por conseguinte, na apreciação da validade do consentimento no âmbito do emprego, importa analisar cuidadosamente as circunstâncias em que o consentimento é solicitado.

300 Conselho da Europa, Comité de Ministros (1989), *Recommendation Rec(89)2 to member states on the protection of personal data used for employment purposes* (Recomendação Rec(89)2 aos Estados membros sobre a proteção dos dados pessoais utilizados para fins de emprego), 18 de janeiro de 1989. Ver ainda Comité Consultivo da Convenção 108, *Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation* (Estudo sobre a Recomendação n.º R (89) 2 sobre a proteção dos dados pessoais utilizados para fins de emprego e que apresenta propostas para a revisão desta Recomendação), 9 de setembro de 2011.

301 Grupo de Trabalho do artigo 29.º (2001), *Parecer 8/2001 sobre o tratamento de dados pessoais no âmbito do emprego*, WP 48, Bruxelas, 13 de Setembro de 2001.

302 Grupo de Trabalho do artigo 29.º (2005), *Documento de trabalho sobre uma interpretação comum do artigo 26.º, n.º 1, da Diretiva 95/46/CE de 24 de outubro de 1995*, WP 114, Bruxelas, 25 de novembro de 2005.

Um problema de proteção de dados comum no típico ambiente de trabalho dos dias de hoje é a extensão legítima do controlo das comunicações eletrónicas dos funcionários no local de trabalho. É frequente afirmarse que este problema poderia ser facilmente resolvido com a proibição do uso de equipamento de comunicação para fins pessoais no local de trabalho. Porém, esta proibição geral poderia ser desproporcionada e pouco realista. O acórdão do TEDH que se segue revestese de especial interesse neste contexto:

> Exemplo: No processo que deu origem ao acórdão *Copland c. Reino Unido*,[303] a utilização do telefone, do correio eletrónico e da Internet pela funcionária de uma faculdade tinha sido monitorizada sem o seu conhecimento para determinar se ela estava a utilizar excessivamente o equipamento da faculdade para fins pessoais. O TEDH considerou que as chamadas telefónicas efetuadas a partir de estabelecimentos comerciais estavam abrangidas pelos conceitos de vida privada e correspondência. Por conseguinte, as chamadas telefónicas e as mensagens de correio eletrónico enviadas do local de trabalho, bem como as informações obtidas através da monitorização da utilização da Internet para fins pessoais estavam protegidas pelo artigo 8.º da CEDH. No caso da requerente, as circunstâncias em que os empregadores podiam monitorizar a utilização do telefone, correio eletrónico e Internet pelos funcionários não estavam reguladas. Consequentemente, a ingerência não estava de acordo com a lei. O TEDH concluiu que tinha havido uma violação do artigo 8.º da CEDH.

De acordo com a Recomendação do CdE sobre o emprego, os dados pessoais recolhidos para fins de emprego deveriam ser obtidos diretamente junto do funcionário em causa.

Os dados pessoais recolhidos para fins de recrutamento devem limitarse às informações necessárias para avaliar a aptidão dos candidatos e o seu potencial profissional.

A recomendação também menciona expressamente dados subjetivos relativos ao desempenho ou ao potencial de funcionários específicos. Os dados subjetivos devem basearse em avaliações justas e honestas e não devem ser formulados em termos vexatórios. Tratase de exigências ditadas pelos princípios do tratamento leal dos dados e da exatidão dos dados.

303 TEDH, acórdão *Copland c. Reino Unido* de 3 de abril de 2007, petição n.º 62617/00.

Um aspeto específico da legislação sobre proteção de dados no contexto da relação empregador/funcionário é o papel desempenhado pelos representantes dos funcionários. Estes representantes só poderão receber os dados pessoais dos funcionários na medida necessária para representar os seus interesses.

Os dados pessoais sensíveis recolhidos para fins de emprego só poderão ser objeto de tratamento em casos específicos e de acordo com as garantias estabelecidas no direito interno. Os empregadores só poderão fazer perguntas aos funcionários ou aos candidatos a emprego sobre o seu estado de saúde ou submetêlos a exames médicos se tal for necessário para determinar a sua aptidão para o desempenho das funções, cumprir os requisitos da medicina preventiva ou possibilitar a atribuição de prestações sociais. Os dados sobre a saúde não podem ser obtidos de fontes diferentes do funcionário em causa, salvo quando tenha sido obtido o seu consentimento expresso e informado ou quando o direito nacional o preveja.

Nos termos da Recomendação sobre o emprego, os funcionários deveriam ser informados sobre a finalidade do tratamento dos seus dados pessoais, o tipo de dados pessoais armazenados, as entidades a quem os dados são regularmente comunicados e a base legal dessa comunicação. Os empregadores deveriam ainda informar antecipadamente os funcionários sobre a introdução ou adaptação de sistemas automatizados de tratamento dos seus dados pessoais ou de monitorização dos seus movimentos ou da sua produtividade.

Os funcionários devem ter o direito de acesso aos seus dados de emprego, bem como o direito de retificação ou apagamento dos mesmos. Em caso de tratamento de dados subjetivos, os funcionários devem ter ainda o direito de contestar a avaliação. No entanto, estes direitos poderão ser temporariamente limitados para fins de investigação interna. O direito nacional deve estabelecer procedimentos adequados a que o funcionário possa recorrer em caso de recusa de acesso, retificação ou apagamento dos seus dados de emprego pessoais.

8.3. Dados médicos

Ponto-chave

- Os dados médicos são dados sensíveis e, como tal, gozam de proteção específica.

Os dados pessoais sobre o estado de saúde da pessoa em causa são qualificados como dados sensíveis pelo artigo 8.º, n.º 1, da Diretiva de Proteção de Dados e pelo artigo 6.º da Convenção 108. Por conseguinte, os dados médicos estão sujeitos a um regime de tratamento de dados mais rigoroso do que os dados não sensíveis.

Exemplo: No processo que deu origem ao acórdão *Z. c. Finlândia*,[304] o ex-marido da requerente, que era seropositivo, tinha cometido uma série de crimes sexuais, tendo vindo a ser condenado pelo crime de homicídio não premeditado por ter exposto deliberadamente as suas vítimas ao risco de infeção pelo VIH. O tribunal nacional decidiu que a versão integral do acórdão e os autos deveriam ser mantidos confidenciais durante 10 anos, não obstante a requerente ter pedido a fixação de um período de confidencialidade mais longo. O tribunal de recurso negou provimento a estes pedidos e o seu acórdão continha os nomes completos da requerente e do seu ex-marido. O TEDH entendeu que esta ingerência não era considerada necessária numa sociedade democrática porque a proteção dos dados médicos revestiase de importância fundamental para o gozo do direito ao respeito pela vida privada e pela vida familiar, especialmente quando estivessem em causa informações sobre infeções pelo VIH, dado o estigma associado a esta doença em muitas sociedades. Consequentemente, o TEDH concluiu que a concessão de acesso à identidade e ao estado de saúde da requerente, conforme descritos no acórdão do tribunal de recurso, decorridos apenas 10 anos desde a data do acórdão violaria o artigo 8.º da CEDH.

O artigo 8.º, n.º 3, da Diretiva de Proteção de Dados permite o tratamento de dados médicos quando tal for necessário para efeitos de medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamentos médicos ou gestão de serviços de saúde. Porém, o tratamento só é admissível se for realizado por um profissional de saúde sujeito a uma obrigação de segredo profissional ou por outra pessoa sujeita a uma obrigação equivalente.[305]

304 TEDH, acórdão *Z. c. Finlândia* de 25 de fevereiro de 1997, petição n.º 22009/93, n.ºs 94 e 112; ver também TEDH, acórdão *M.S. c. Suécia* de 27 de agosto de 1997, petição n.º 20837/92; TEDH, acórdão *L.L. c. França* de 10 de outubro de 2006, petição n.º 7508/02; TEDH, acórdão *I. c. Finlândia* de 17 de julho de 2008, petição n.º 20511/03; TEDH, acórdão *K.H. e outros c. Eslováquia* de 28 de abril de 2009, petição n.º 32881/04; TEDH, acórdão *Szuluk c. Reino Unido* de 2 de junho de 2009, petição n.º 36936/05.

305 Ver também TEDH, acórdão *Biriuk c. Lituânia* de 25 de novembro de 2008, petição n.º 23373/03.

A Recomendação do CdE sobre dados médicos, de 1997 aplica os princípios da Convenção 108 ao tratamento de dados no domínio médico em maior detalhe.[306] As regras propostas estão em conformidade com as disposições da Diretiva de Proteção de Dados em matéria de legitimidade das finalidades do tratamento de dados médicos, das necessárias obrigações de segredo profissional das pessoas que utilizam dados sobre a saúde, e dos direitos das pessoas em causa à transparência e ao acesso, retificação e apagamento. Além disso, os dados médicos licitamente tratados por profissionais da saúde não podem ser transferidos para as autoridades policiais, a menos que estejam previstas garantias suficientes para prevenir a divulgação dos dados em violação do direito ao respeito pela vida privada garantido pelo artigo 8.º da CEDH.[307]

Por seu lado, a Recomendação sobre dados médicos contém disposições especiais sobre os dados médicos dos nascituros e dos incapazes e sobre o tratamento de dados genéticos. A investigação científica é expressamente identificada como um motivo legítimo de conservação dos dados por um período mais longo do que aquele durante o qual são necessários, embora, neste caso, seja normalmente exigida a sua anonimização. O artigo 12.º da Recomendação sobre dados médicos propõe regras detalhadas para as situações em que os investigadores necessitam de dados pessoais e os dados anonimizados não são suficientes.

A pseudonimização poderá ser um meio adequado de satisfazer as necessidades científicas e proteger simultaneamente os interesses dos doentes em causa. O conceito de pseudonimização no contexto da proteção de dados é explicado de forma mais detalhada na secção 2.1.3.

Está em curso um debate intensivo ao nível nacional e da UE sobre iniciativas relativas ao armazenamento de dados sobre o tratamento médico de um doente num ficheiro eletrónico de saúde.[308] Um aspeto especial da existência de sistemas nacionais de ficheiros eletrónicos de saúde é a sua disponibilidade transfronteiriça: um tópico de particular interesse na UE no contexto dos cuidados de saúde transfronteiriços.[309]

306 CdE, Comité de Ministros (1997), *Recommendation Rec(97)5 to member states on the protection of medical data* (Recomendação Rec(97)5 aos Estados membros sobre a proteção dos dados médicos), 13 de fevereiro de 1997.

307 TEDH, acórdão *Avilkina e outros c. Rússia* de 6 de junho de 2013, petição n.º 1585/09, n.º 53 (não definitivo).

308 Grupo de Trabalho do artigo 29.º (2007), *Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde eletrónicos (RSE)*, WP 131, Bruxelas, 15 de fevereiro de 2007.

309 Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços, JO 2011 L 88.

Outra área em debate em relação a novas disposições são os ensaios clínicos, ou seja, testar novos medicamentos em doentes num ambiente de investigação documentado; este tópico também tem implicações consideráveis em matéria de proteção de dados. Os ensaios clínicos de medicamentos para uso humano são regulados pela Diretiva 2001/20/CE do Parlamento Europeu e do Conselho, de 4 de abril d 2001, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros respeitantes à aplicação de boas práticas clínicas na condução dos ensaios clínicos de medicamentos para uso humano (*Diretiva Ensaios Clínicos*).[310] Em dezembro de 2012, a Comissão Europeia propôs um regulamento para substituir a Diretiva Ensaios Clínico, com o objetivo de tornar mais uniformes e eficientes os procedimentos dos ensaios.[311]

Existem muitas outras iniciativas, nomeadamente iniciativas legislativas, pendentes na UE respeitantes aos dados pessoais no setor da saúde.[312]

8.4. Tratamento de dados para fins estatísticos

Pontos-chave

- Os dados recolhidos para fins estatísticos não podem ser utilizados para qualquer outro fim.
- Os dados legitimamente recolhidos para qualquer fim podem ser também utilizados para fins estatísticos, desde que o direito nacional estabeleça garantias adequadas que sejam respeitadas pelos utilizadores. Para este efeito, deve ser prevista, em especial, a anonimização ou pseudonimização dos dados antes da transmissão para terceiros.

Na Diretiva de Proteção de Dados, o tratamento de dados para fins estatísticos é mencionado no contexto de possíveis derrogações aos princípios da proteção de

310 Diretiva 2001/20/CE do Parlamento Europeu e do Conselho, de 4 de abril de 2001, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros respeitantes à aplicação de boas práticas clínicas na condução dos ensaios clínicos de medicamentos para uso humano, JO 2001 L 121.

311 Comissão Europeia (2012), *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo aos ensaios clínicos de medicamentos para uso humano e que revoga a Diretiva 2001/20/CE*, COM(2012) 369 final, Bruxelas, 17 de julho de 2012.

312 AEPD (2013) *Parecer da Autoridade Europeia para a Proteção de Dados sobre a Comunicação da Comissão intitulada «Plano de ação para a saúde em linha 20122020 - Cuidados de saúde inovadores para o século XXI»*, Bruxelas, 27 de março de 2013.

dados. O artigo 6.º, n.º 1, alínea b), da Diretiva permite que o legislador nacional preveja uma derrogação ao princípio da limitação da finalidade a favor do tratamento ulterior de dados para fins estatísticos, desde que estabeleça também todas as garantias necessárias. O artigo 13.º, n.º 2, da Diretiva permite que o legislador nacional estabeleça restrições aos direitos de acesso se os dados forem tratados exclusivamente para fins estatísticos; mais uma vez, o direito nacional deve prever garantias adequadas. Neste contexto, a Diretiva de Proteção de Dados estabelece a exigência de que nenhum dos dados adquiridos ou criados durante a investigação estatística seja utilizado para tomar decisões concretas sobre as pessoas em causa.

Embora os dados licitamente recolhidos por um responsável pelo tratamento para qualquer finalidade possam ser reutilizados por este responsável pelo tratamento para os seus próprios fins estatísticos – as chamadas estatísticas secundárias – esses dados teriam de ser anonimizados ou pseudonimizados, dependendo do contexto, antes da sua transmissão para terceiros para fins estatísticos, salvo se a pessoa em causa tivesse dado o seu consentimento ou se essa transmissão estivesse expressamente prevista na legislação nacional. É o que resulta da exigência de adoção de garantias adequadas prevista no artigo 6.º, n.º 1, alínea b), da Diretiva de Proteção de Dados.

Os casos mais importantes de utilização de dados para fins estatísticas são as estatísticas oficiais, produzidas pelos serviços de estatística nacionais e da UE com base em leis nacionais e da UE sobre estatísticas oficiais. De acordo com estas leis, os cidadãos e as empresas são geralmente obrigados a divulgar dados às autoridades estatísticas. Os funcionários dos serviços de estatística estão sujeitos a obrigações especiais de segredo profissional que são rigorosamente respeitadas, na medida em que são essenciais para o elevado nível de confiança que é necessário para que os cidadãos disponibilizem os dados às autoridades estatísticas.

O Regulamento (CE) n.º 223/2009 relativo às Estatísticas Europeias (*Regulamento Estatísticas Europeias*) contém regras essenciais para a proteção de dados no contexto das estatísticas oficiais e, como tal, também pode ser considerado relevante para as disposições sobre estatísticas oficiais ao nível nacional.[313] O Regulamento

313 Regulamento (CE) n.º 223/2009 do Parlamento Europeu e do Conselho, de 11 de março de 2009, relativo às Estatísticas Europeias e que revoga o Regulamento (CE, Euratom) n.º 1101/2008 relativo à transmissão de informações abrangidas pelo segredo estatístico ao Serviço de Estatística das Comunidades Europeias, o Regulamento (CE) n.º 322/97 relativo às estatísticas comunitárias e a Decisão 89/382/CEE, Euratom do Conselho que cria o Comité do Programa Estatístico das Comunidades Europeias, JO 2009 L 87.

estabelece o princípio de que as operações estatísticas oficiais exigem uma base legal suficientemente específica.[314]

> Exemplo: No acórdão *Huber/Alemanha*,[315] o TJUE considerou que a recolha e o armazenamento de dados pessoais por uma autoridade para fins estatísticos não era, por si só, motivo suficiente para que o tratamento fosse lícito. A lei que previa o tratamento de dados pessoais também teria de cumprir o requisito da necessidade, o que não acontecia naquele caso.

No contexto do CdE, a Recomendação sobre dados estatísticos, de 1997 abrange a produção de estatísticas nos setores público e privado.[316] Esta recomendação subscreve princípios que coincidem com as principais regras da Diretiva de Proteção de Dados acima descritas. São enunciadas regras mais detalhadas em relação às seguintes questões.

Enquanto os dados recolhidos pelo responsável pelo tratamento para fins estatísticos não podem ser utilizados para qualquer outro fim, os dados recolhidos para fins não estatísticos podem ser posteriormente objeto de utilização estatística. A Recomendação sobre dados estatísticos permite inclusivamente a comunicação de dados a terceiros se for exclusivamente para fins estatísticos. Nestes casos, as partes devem chegar a acordo sobre o âmbito da utilização posterior legítima para fins estatísticos e reduzir esse acordo a escrito. Uma vez que este acordo não pode substituir o consentimento da pessoa em causa, presumese que existirão garantias adequadas adicionais previstas no direito nacional para minimizar o risco de utilização abusiva dos dados pessoais, tais como a obrigação de anonimizar ou pseudonimizar os dados antes da transmissão.

As pessoas profissionalmente envolvidas na investigação científica deveriam estar sujeitas a obrigações especiais de segredo profissional – como acontece habitualmente no caso das estatísticas oficiais – nos termos do direito nacional. Os

314 Este princípio será desenvolvido no Código de Prática do Eurostat, que deverá, nos termos do artigo 11.º do Regulamento Estatísticas Europeias, fornecer orientações étnicas sobre a produção de estatísticas oficiais, incluindo a utilização ponderada de dados pessoais, disponível em: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 TJUE, acórdão de 16 de dezembro de 2008 no processo C-524/06, *Huber/Alemanha;* ver, em especial, n.º 68.

316 Conselho da Europa, Comité de Ministros (1997), *Recommendation Rec(97)18 to member states on the protection of personal data collected and processed for statistical purposes* (Recomendação Rec(97)10 aos Estados membros sobre a proteção dos dados pessoais recolhidos e tratados para fins estatísticos), 30 de Setembro de 1997.

entrevistadores que recolham dados junto das pessoas em causa ou de outras pessoas também devem estar sujeitos a esta obrigação.

Se um inquérito estatístico que utilize dados pessoais não estiver previsto na lei, as pessoas em causa terão de dar o seu consentimento para a utilização dos seus dados a fim de a legitimar ou, pelo menos, deveriam ter a oportunidade de se opor a essa utilização. Se forem recolhidos dados pessoais para fins estatísticos mediante a realização de entrevistas, os entrevistados devem ser claramente informados se a divulgação dos dados é ou não obrigatória nos termos do direito nacional. Os dados sensíveis devem ser recolhidos de modo a impedir a identificação da pessoa, salvo se tal for expressamente permitido pelo direito nacional.

Se não for possível realizar um inquérito estatístico sem dados anonimizados e forem efetivamente necessários dados pessoais, os dados recolhidos para este fim deverão ser anonimizados logo que possível. Os resultados do inquérito estatístico não poderão, pelo menos, permitir a identificação das pessoas em causa, salvo se tal não apresentar manifestamente qualquer risco.

Uma vez concluída a análise estatística, os dados pessoais utilizados deverão ser eliminados ou anonimizados. Neste caso, a Recomendação sobre dados estatísticos propõe que os dados de identificação sejam conservados separadamente dos outros dados pessoais. Isto significa, por exemplo, que os dados deverão ser pseudonimizados e a chave de encriptação ou a lista com os sinónimos identificadores deve ser conservada separadamente dos dados pseudonimizados.

8.5. Dados financeiros

Pontos-chave

- Embora os dados financeiros não sejam dados sensíveis na aceção da Convenção 108 ou da Diretiva de Proteção de Dados, o seu tratamento exige garantias especiais para assegurar a exatidão e a segurança dos dados.
- É necessário incorporar mecanismos de proteção de dados nos sistemas de pagamento eletrónicos (a chamada «privacidade desde a conceção»).
- A exigência de mecanismos de autenticação adequados coloca problemas específicos em matéria de proteção de dados nesta área.

Exemplo: No processo que deu origem ao acórdão *Michaud c. França*,[317] o requerente, um advogado francês, contestou a obrigação que lhe era imposta pelo direito francês de comunicar suspeitas sobre possíveis atividades de branqueamento de capitais dos seus clientes. Segundo o TEDH, exigir que os advogados comunicassem às autoridades administrativas informações relativas a outra pessoa que tivessem chegado ao seu conhecimento através de conversas com essa pessoa constituía uma ingerência no direito dos advogados ao respeito pela correspondência e vida privada nos termos do artigo 8.º da CEDH, uma vez que este conceito abrangia atividades de natureza profissional e comercial. Contudo, essa ingerência estava de acordo com a lei e prosseguia um objetivo legítimo, ou seja, a prevenção de distúrbios e da criminalidade. Uma vez que os advogados só estavam obrigados a comunicar suspeitas em casos muito específicos, o TEDH considerou que esta obrigação era proporcional e concluiu que não tinha havido uma violação do artigo 8.º.

O CdE adaptou o quadro jurídico geral da proteção de dados, conforme estabelecido na Convenção 108, ao contexto dos pagamentos na Recomendação Rec(90)19 de 1990.[318] Esta recomendação clarifica o âmbito da recolha e utilização lícitas de dados no contexto dos pagamentos, especialmente através de cartões de pagamento. Além disso, propõe aos legisladores nacionais regras detalhadas sobre os limites da comunicação de dados de pagamento a terceiros, limites temporais da conservação dos dados, transparência, segurança dos dados e fluxos transfronteiriços de dados e, por último, supervisão e vias de recurso. As soluções propostas correspondem às disposições do quadro jurídico geral da UE em matéria de proteção de dados aprovado posteriormente sob a forma da Diretiva de Proteção de Dados.

Estão a ser criados vários instrumentos jurídicos para regular os mercados de instrumentos financeiros e as atividades das instituições de crédito e das sociedades de

317 TEDH, acórdão *Michaud c. França* de 6 de dezembro de 2012, petição n.º 12323/11; ver também TEDH, acórdão *Niemietz c. Alemanha* de 16 de dezembro de 1992, petição n.º 13710/88, n.º 29, e TEDH, acórdão *Halford c. Reino Unido* de 25 de junho de 1997, petição n.º 20605/92, n.º 42.

318 CdE, Comité de Ministros (1990), *Recommendation No. R(90)19 on the protection of personal data used for payment and other related operations*, 13 de setembro de 1990.

investimento.[319] Outros instrumentos jurídicos apoiam o combate ao abuso de informação privilegiada e à manipulação de mercado.[320] As questões mais importantes nestas áreas com relevância para a proteção de dados são:

- a conservação de registos sobre transações financeiras;
- a transferência de dados pessoais para países terceiros;
- a gravação de conversas telefónicas ou comunicações eletrónicas, incluindo o dever de fornecer às autoridades competentes registos telefónicos e do tráfego de dados;
- a divulgação de informações pessoais, incluindo a publicação de sanções;
- os poderes de controlo e inquérito das autoridades competentes, incluindo a realização de inspeções *in loco* e o acesso a instalações privadas para apreender documentos;
- os mecanismos de comunicação de violações, ou seja, os sistemas de denúncia; e
- a cooperação entre as autoridades competentes dos Estados-Membros e a Autoridade Europeia dos Valores Mobiliários e dos Mercados (ESMA).

---

319 Comissão Europeia (2011), *Proposta de Diretiva do Parlamento Europeu e do Conselho relativa aos mercados de instrumentos financeiros, que revoga a Diretiva 2004/39/CE do Parlamento Europeu e do Conselho*, COM(2011) 656 final, Bruxelas, 20 de outubro de 2011; Comissão Europeia (2011), *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo aos mercados de instrumentos financeiros, que altera o Regulamento [EMIR] relativo aos derivados OTC, às contrapartes centrais e aos repositórios de transações*, COM(2011) 652 final, Bruxelas, 20 de outubro de 2011; Comissão Europeia (2011), *Proposta de Diretiva do Parlamento Europeu e do Conselho relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento e que altera a Diretiva 2002/87/CE do Parlamento Europeu e do Conselho relativa à supervisão complementar de instituições de crédito, empresas de seguros e empresas de investimento de um conglomerado financeiro*, COM(2011) 453 final, Bruxelas, 20 de julho de 2011.

320 Comissão Europeia (2011), *Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao abuso de informação privilegiada e à manipulação de mercado (abuso de mercado)*, COM(2011) 651 final, Bruxelas, 20 de outubro de 2011; Comissão Europeia (2011), *Proposta de Diretiva do Parlamento Europeu e do Conselho relativa às sanções penais aplicáveis ao abuso de informação privilegiada e à manipulação de mercado (abuso de mercado)*, COM(2011) 654 final, Bruxelas, 20 de outubro de 2011.

Há outras questões nestas áreas que também são expressamente abordadas, tais como a recolha de dados sobre a situação financeira das pessoas em causa[321] ou o pagamento transfronteiriço através de transferência bancária, que implica necessariamente fluxos de dados pessoais.[322]

321 Regulamento (CE) n.º 1060/2009 do Parlamento Europeu e do Conselho, de 16 de Setembro de 2009, relativo às agências de notação de risco, JO 2009 L 302; Comissão Europeia, *Proposta de Regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (CE) n.º 1060/2009 relativo às agências de notação de risco*, COM(2010) 289 final, Bruxelas, 2 de junho de 2010.

322 Diretiva 2007/64/CE do Parlamento Europeu e do Conselho, de 13 de novembro de 2007, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE e revoga a Diretiva 97/5/CE, JO 2007 L 319.

Leitura complementar

Capítulo

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbau, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Viena, Manzsche Verlags- und Universitätsbuchhandlung.

EDRi, *An introduction to data protection*, Bruxelas, disponível em: www.edri.org/files/paper06_datap.pdf.

Frowein, J. E Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlim, N. P. Engel Verlag.

Grabenwarter, C. e Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Munique, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. e Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Munique, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. e Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antuérpia, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. e Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Bruxelas, Emile Bruylant.

Simitis, S. (1997), «Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?», *Neue Juristische Wochenschrift*, n.º 5, p. 281–288.

Warren, S. e Brandeis, L. (1890), «The right to privacy», *Harvard Law Review,* vol. 4, n.º 5, p. 193–220, disponível em: www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. e Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Capítulo 2

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Gabinete do Comissário para a Informação do Reino Unido (2012), *Anonymisation: managing data protection risk. Code of practice*, disponível em: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

Morgan, R. e Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, Londres, Sweet & Maxwell.

Ohm, P. (2010), «Broken promises of privacy: Responding to the surprising failure of anonymization», *UCLA Law Review*, vol. 57, n.º 6, p. 1701–1777.

Tinnefeld, M., Buchner, B. e Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Munique, Oldenbourg Wissenschaftsverlag.

Capítulos 3 a 5

Autoridade de Proteção de Dados do Reino Unido, *Privacy Impact Assessment*, disponível em: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

Brühann, U. (2012), «Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr» *in*: Grabitz, E., Hilf, M. e Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Munique, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cádis, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrücken, Éditions universitaires européennes.

Dammann, U. e Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (Agência dos Direitos Fundamentais da União Europeia) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxemburgo, Serviço de Publicações da União Europeia (Serviço de Publicações).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (edição para a Conferência), Viena, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxemburgo, Serviço de Publicações.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

Capítulo 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. e Nouwt, S. (2009), *Reinventing data protection?*, Berlim, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Capítulo 7

Europol (2012), *Data Protection at Europol*, Luxemburgo, Serviço de Publicações, disponível em: www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, a Haia, Eurojust.

Drewer, D., Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime,* ERA Forum, vol. 13, n.º 3, p. 381–395.

Gutwirth, S., Poullet, Y. e De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. e Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, *European Law Review*, vol. 36, n.º 5, p. 722–776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers 2013/2, disponível em: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Capítulo 8

Büllesbach, A., Gijrath, S., Poullet, Y. e Hacon, R. (2010), *Concise European IT law*, Amesterdão, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. e Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. e De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. e Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem, *European Law Review*, vol. 36, n.º 5, p. 722–776.

Rosemary, J. e Hamilton, A. (2012), *Data protection law and practice*, Londres, Sweet & Maxwell.

Jurisprudência

Jurisprudência selecionada do Tribunal Europeu dos Direitos do Homem

Acesso a dados pessoais

Acórdão *Gaskin c. Reino Unido* de 7 de junho de 1989, petição n.º 10454/83
Acórdão *Godelli c. Itália* de 25 de setembro de 2012, petição n.º 33783/09
Acórdão *K.H. e outros c. Eslováquia* de 28 de abril de 2009, petição n.º 32881/04
Acórdão *Leander c. Suécia* de 26 de março de 1987, petição n.º 9248/81
Acórdão *Odièvre c. França* [GS] de 13 de fevereiro de 2003, petição n.º 42326/98

Conciliação da proteção de dados com a liberdade de expressão

Acórdão *Axel Springer AG c. Alemanha* [GS] de 7 de fevereiro de 2012, petição n.º 39954/08
Acórdão *Von Hannover c. Alemanha* de 24 de junho de 2004, petição n.º59320/00
Acórdão *Von Hannover c. Alemanha (n.º 2)* [GS] de 7 de fevereiro de 2012, petições n.ºs 40660/08 e 60641/08

Desafios na proteção de dados na Internet

Acórdão *K.U. c. Finlândia* de 2 de dezembro de 2008, petição n.º 2872/02

Correspondência

Acórdão *Amann c. Suíça* [GS] de 16 de fevereiro de 2000, petição n.º 27798/95

Acórdão *Bernh Larsen Holding AS e outros c. Noruega* de 14 de março de 2013, petição n.º 24117/08
Acórdão *Cemalettin Canli c. Turquia* de 18 de novembro de 2008, petição n.º 22427/04
Acórdão *Dalea c. França* de 2 de fevereiro de 2010, petição n.º 964/07
Acórdão *Gaskin c. Reino Unido* de 7 de junho de 1989, petição n.º 10454/83
Acórdão *Haralambie c. Roménia* de 27 de outubro de 2009, petição n.º 21737/03
Acórdão *Khelili c. Suíça* de 18 de outubro de 2011, petição n.º 16188/07
Acórdão *Leander c. Suécia* de 26 de março de 1987, petição n.º 9248/81
Acórdão *Malone c. Reino Unido* de 2 de agosto de 1984, petição n.º 8691/79
Acórdão *McMichael c. Reino Unido* de 24 de fevereiro de 1995, petição n.º 16424/90
Acórdão *M. G. c. Reino Unido* de 24 de setembro de 2002, petição n.º 39393/98
Acórdão *Rotaru c. Roménia* [GS] de 4 de maio de 2000, petição n.º 28341/95
Acórdão *S. e Marper c. Reino Unido* de 4 de dezembro de 2008, petições n.ºs 30562/04 e 30566/04
Acórdão *Shimovolos c. Rússia* de 21 de junho de 2011, petição n.º 30194/09
Acórdão *Turek c. Eslováquia* de 14 de fevereiro de 2006, petição n.º 57986/00

Bases de dados de registos criminais

Acórdão *B.B. c. França* de 17 de dezembro de 2009, petição n.º 5335/06
Acórdão *M.M. c. Reino Unido* de 13 de novembro de 2012, petição n.º 24029/07

Bases de dados de ADN

Acórdão *S. e Marper c. Reino Unido* de 4 de dezembro de 2008, petições n.ºs 30562/04 e 30566/04

Dados GPS

Acórdão *Uzun c. Alemanha* de 2 de setembro de 2010, petição n.º 35623/05

Dados sobre a saúde

Acórdão *Biriuk c. Lituânia* de 25 de novembro de 2008, petição n.º 23373/03
Acórdão *I. c. Finlândia* de 17 de julho de 2008, petição n.º 20511/03
Acórdão *L.L. c. França* de 10 de outubro de 2006, petição n.º 7508/02
Acórdão *M.S. c. Suécia* de 2 de julho de 2002, petição n.º 34209/96
Acórdão *Szuluk c. Reino Unido* de 2 de junho de 2009, petição n.º 36936/05
Acórdão *Z. c. Finlândia* de 25 de fevereiro de 1997, petição n.º 22009/93

Identidade

Acórdão *Ciubotaru c. Moldávia* de 27 de abril de 2010, petição n.º 27138/04
Acórdão *Godelli c. Itália* de 25 de setembro de 2012, petição n.º 33783/09
Acórdão *Odièvre c. França* [GS] de 13 de fevereiro de 2003, petição n.º 42326/98

Informações sobre atividades profissionais

Acórdão *Michaud c. França* de 6 de dezembro de 2012, petição n.º 12323/11
Acórdão *Niemietz c. Alemanha* de 16 de dezembro de 1992, petição n.º 13710/88

Interceção das comunicações

Acórdão *Amann c. Suíça* [GS] de 16 de fevereiro de 2000, petição n.º 27798/95
Acórdão *Copland c. Reino Unido* de 3 de abril de 2007, petição n.º 62617/00
Acórdão *Cotlet c. Roménia* de 3 de junho de 2003, petição n.º 38565/97
Acórdão *Kruslin c. França* de 24 de abril de 1990, petição n.º 11801/85
Acórdão *Lambert c. França* de 24 de agosto de 1998, petição n.º 23618/94
Acórdão *Liberty e outros c. Reino Unido* de 1 de julho de 2008, petição n.º 58243/00
Acórdão *Malone c. Reino Unido* de 2 de agosto de 1984, petição n.º 8691/79
Acórdão *Halford c. Reino Unido* de 25 de junho de 1997, petição n.º 20605/92
Acórdão *Szuluk c. Reino Unido* de 2 de junho de 2009, petição n.º 36936/05

Obrigações dos responsáveis pela proteção dos direitos humanos

Acórdão *B.B. c. França* de 17 de dezembro de 2009, petição n.º 5335/06
Acórdão *I. c. Finlândia* de 17 de julho de 2008, petição n.º 20511/03
Acórdão *Mosley c. Reino Unido* de 10 de maio de 2011, petição n.º 48009/08

Fotografias

Acórdão *Sciacca c. Itália* de 11 de janeiro de 2005, petição n.º 50774/99
Acórdão *Von Hannover c. Alemanha* de 24 de junho de 2004, petição n.º59320/00

Direito a ser esquecido

Acórdão *Segerstedt-Wiberg e outros c. Suécia* de 6 de junho de 2006, petição n.º 62332/00

Direito de oposição

Acórdão *Leander c. Suécia* de 26 de março de 1987, petição n.º 9248/81

Acórdão *Mosley c. Reino Unido* de 10 de maio de 2011, petição n.º 48009/08
Acórdão *M.S. c. Suécia* de 2 de julho de 2002, petição n.º 34209/96
Acórdão *Rotaru c. Roménia* [GS] de 4 de maio de 2000, petição n.º 28341/95

Categorias sensíveis de dados

Acórdão *I. c. Finlândia* de 17 de julho de 2008, petição n.º 20511/03
Acórdão *Michaud c. França* de 6 de dezembro de 2012, petição n.º 12323/11
Acórdão *S. e Marper c. Reino Unido* de 4 de dezembro de 2008, petições n.ºs 30562/04 e 30566/04

Controlo e fiscalização do cumprimento (papel dos diferentes intervenientes, incluindo as autoridades de proteção de dados)

Acórdão *I. c. Finlândia* de 17 de julho de 2008, petição n.º 20511/03
Acórdão *K.U. c. Finlândia* de 2 de dezembro de 2008, petição n.º 2872/02
Acórdão *Von Hannover c. Alemanha* de 24 de junho de 2004, petição n.º59320/00
Acórdão *Von Hannover c. Alemanha (n.º 2)* [GS] de 7 de fevereiro de 2012, petições n.ºs 40660/08 e 60641/08

Métodos de vigilância

Acórdão *Allan c. Reino Unido* de 5 de novembro de 2002, petição n.º 48539/99
Acórdão *Association «21 Décembre 1989» e outros c. Roménia* de 24 de maio de 2011, petições n.ºs 33810/07 e 18817/08
Acórdão *Bykov c. Rússia* [GS] de 10 de março de 2009, petição n.º 4378/02
Acórdão *Kennedy c. Reino Unido* de 18 de maio de 2010, petição n.º 26839/05
Acórdão *Klass e outros c. Alemanha* de 6 de setembro de 1978, petição n.º 5029/71
Acórdão *Rotaru c. Roménia* [GS] de 4 de maio de 2000, petição n.º 28341/95
Acórdão *Taylor-Sabori c. Reino Unido* de 22 de outubro de 2002, petição n.º 47114/99
Acórdão *Uzun c. Alemanha* de 2 de setembro de 2010, petição n.º 35623/05
Acórdão *Vetter c. França* de 31 de maio de 2005, petição n.º 59842/00

Videovigilância

Acórdão *Köpke c. Alemanha* de 5 de outubro de 2010, petição n.º 420/07
Acórdão *Peck c. Reino Unido* de 28 de janeiro de 2003, petição n.º 44647/98

Amostras de voz

Acórdão *P.G. e J.H. c. Reino Unido* de 25 de setembro de 2001, petição n.º 44787/98
Acórdão *Wisse c. França* de 20 de dezembro de 2005, petição n.º 71611/01

Jurisprudência selecionada do Tribunal de Justiça da União Europeia

Jurisprudência relacionada com a Diretiva de Proteção de Dados

Acórdão de 16 de dezembro de 2008 no processo C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy e Satamedia Oy*
[Conceito de «atividades jornalísticas» na aceção do artigo 9.º da Diretiva de Proteção de Dados]

Acórdão de 9 de novembro de 2010 nos processos apensos C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen*
[Proporcionalidade da obrigação legal de publicar dados pessoais sobre os beneficiários de certos fundos agrícolas da UE]

Acórdão de 6 de novembro de 2003 no processo C-101/01, *Bodil Lindqvist*
[Legitimidade da publicação por particulares de dados sobre a vida privada de terceiros na Internet]

Acórdão de 13 de maio de 2014 no processo C-131/12, *Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González*, pedido de decisão prejudicial apresentado pela Audiencia Nacional (Espanha) em 9 de março de 2012, 25 de maio de 2012, pendente
[Obrigação das empresas que exploram os motores de pesquisa de se absterem de mostrar dados pessoais nos resultados da pesquisa, caso tal seja solicitado pelo titular dos dados]

Acórdão de 30 de maio de 2013 no processo C-270/11, *Comissão Europeia/Reino da Suécia*
[Multa pela não transposição de uma diretiva]

Acórdão de 29 de janeiro de 2008 no processo C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*
[Obrigação dos prestadores de serviços de acesso à Internet de divulgarem a identidade de utilizadores dos programas de partilha de ficheiros KaZaA à associação de proteção da propriedade intelectual]

Acórdão de 8 de abril de 2014 no processo C-288/12, *Comissão Europeia/Hungria*
[Legitimidade da exoneração da autoridade nacional de proteção de dados]

Conclusões do advogadogeral P. Mengozzi apresentadas em 13 de junho de 2013 no processo C-291/12, *Michael Schwarz/Stadt Bochum*
[Violação do direito primário da UE pelo Regulamento (CE) n.º 2252/2004 que estabelece que a imagem das impressões digitais tem de ser armazenada nos passaportes]

Acórdão de 8 de abril de 2014 nos processos apensos C-293/12 e C594/12, *Digital Rights Ireland e Seitling and Outros*
[Violação do direito primário da UE pela Diretiva Conservação de Dados]

Acórdão de 16 de fevereiro de 2012 no processo C-360/10, *SABAM/Netlog N.V.*
[Obrigação dos prestadores de serviços de redes sociais de impedirem a utilização ilícita de obras musicais e audiovisuais pelos utilizadores da rede]

Acórdão de 20 de maio de 2003 nos processos apensos C-465/00, C-138/01 e C-139/01, *Rechnungshof/Österreichischer Rundfunk e o., e Neukomm e Lauermann/Österreichischer Rundfunk*
[Proporcionalidade da obrigação legal de publicar dados pessoais sobre os salários de funcionários de certas instituições relacionadas com o setor público]

Acórdão de 24 de novembro de 2011 nos processos apensos C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*
[Correta transposição do artigo 7.º, alínea f), da Diretiva de Proteção de Dados – «interesses legítimos de terceiros» – para o direito nacional]

Acórdão de 9 de março de 2010 no processo C-518/07, *Comissão Europeia/República Federal da Alemanha*
[Independência de uma autoridade nacional de controlo]

Acórdão de 16 de dezembro de 2008 no processo C-524/06, *Huber/Alemanha*
[Legitimidade da conservação de dados sobre estrangeiros num registo estatístico]

Acórdão de 5 de maio de 2011 no processo C-543/09, *Deutsche Telekom AG/Bundesrepublik Deutschland*
[Necessidade de novo consentimento]

Acórdão de 7 de maio de 2009 no processo C-553/07, *College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer*
[Direito de acesso do titular dos dados]

Acórdão de 16 de outubro de 2012 no processo C-614/10, *Comissão Europeia/República da Áustria*
[Independência de uma autoridade nacional de controlo]

Jurisprudência relacionada com o Regulamento Proteção de Dados (Instituições da UE)

Acórdão de 29 de junho de 2010 no processo C28/08 P, *Comissão Europeia/The Bavarian Lager Co. Ltd*
[Acesso aos documentos]

Acórdão de 6 de março de 2003 no processo C-41/00 P, *Interporc Im- und Export GmbH/Comissão das Comunidades Europeias*
[Acesso aos documentos]

Acórdão do Tribunal da Função Pública de 15 de junho de 2010 no processo F-35/08, *Pachtitis/Comissão*
[Utilização de dados pessoais no contexto do emprego em instituições da UE]

Acórdão do Tribunal da Função Pública de 5 de julho de 2011 no processo F46/09, *V/Parlamento*
[Utilização de dados pessoais no contexto do emprego em instituições da UE]

Lista de processos

Jurisprudência do Tribunal de Justiça da União Europeia

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado, nos processos apensos C-468/10 e C-469/10, 24 de novembro de 2011 ..... 18, 23, 83, 86, 90, 91, 204

Bodil Lindqvist, P.º C-101/01, 6 de novembro de 2003 ..... 35, 36, 45, 48, 52, 100, 137, 138, 203

College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer, P.º C-553/07, 7 de maio de 2009 ..... 109, 115, 205

Comissão Europeia/Hungria, P.º C-288/12, 8 de abril de 2012 ..... 110, 126, 204

Comissão Europeia/Reino da Suécia, P.º C-270/11, 30 de maio de 2013 203

Comissão Europeia/República da Áustria, P.º C-614/10, 16 de outubro de 2012 ..... 110, 125, 205

Comissão Europeia/República Federal da Alemanha, P.º C-518/07, 9 de março de 2010 ..... 110, 124, 204

Comissão Europeia/The Bavarian Lager Co. Ltd, P.º C28/08 P, 29 de junho de 2010 ..... 13, 28, 30, 111, 134, 205

Deutsche Telekom AG/Bundesrepublik Deutschland, P.º C-543/09, 5 de maio de 2011 ..... 36, 63, 205

Digital Rights Ireland e Seitling and Outro, nos processos apensos C-293/12 e C594/12, 8 de abril de 2014 ..... 133, 180, 204

Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos, Mario Costeja González, processo C131/12, pedido de decisão prejudicial apresentado pela Audiencia Nacional (Espanha) em 9 de março de 2012, 25 de maio de 2012, pendente 203

Huber/Alemanha, P.º C-524/06, 16 de dezembro de 2008 ..... 65, 83, 86, 88, 175, 188, 205

Interporc Im- und Export GmbH/Comissão das Comunidades Europeias, P.º C-41/00 P, 6 de março de 2003 ..... 30, 205

M.H. Marshall Southampton and South-West Hampshire Area Health Authority, P.º C-152/84, 26 de fevereiro de 1986 111
Michael Schwarz/Stadt Bochum, P.º C-291/12, conclusões do advogadogeral P. Mengozzi apresentadas em 13 de junho de 2013 204

Pachtitis/Comissão, P.º F-35/08, acórdão do Tribunal da Função Pública de 15 de junho de 2010 205
Parlamento Europeu c.Conselho da União Europeia, nos processos apensos C-317/04 e C-318/04, acórdão de 30 de maio de 2006 149
Productores de Música de España (Promusicae)/Telefónica de España SAU, P.º C-275/06, 29 de janeiro de 2008 ..... 13, 23, 33, 35, 40, 204

Rechnungshof/Österreichischer Rundfunk e o., e Neukomm e Lauermann/Österreichischer Rundfunk, nos processos apensos C-465/00, C-138/01 e C-139/01, 20 de maio de 2003 ..... 86, 204

SABAM/Netlog N.V., P.º C-360/10, 16 de fevereiro de 2012 ..... 34, 204
Sabine von Colson e Elisabeth Kamann/Land Nordrhein-Westfalen, P.º C-14/83, 10 de abril de 1984 ..... 111, 136

Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy e Satamedia Oy, P.º C-73/07, 16 de dezembro de 2008 ..... 13, 24, 203

V/Parlamento, P.º F46/09, Acórdão do Tribunal da Função Pública de 5 de julho de 2011 205
Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen, nos processos apensos C-92/09 e C-93/09, 9 de novembro de 2010 ..... 13, 22, 31, 35, 39, 43, 65, 71, 203

Jurisprudência do Tribunal Europeu dos Direitos do Homem

Allan c. Reino Unido de 5 de novembro de 2002, petição n.º 48539/99 ..... 156, 202
Amann c. Suíça [GS] de 16 de fevereiro de 2000,
petição n.º 27798/95 ..... 38, 40, 43, 67, 68, 199, 201
Ashby Donald e outros c. França de 10 de janeiro de 2013,
petição n.º 36769/08 33
Association «21 Décembre 1989» e outros c. Roménia de
24 de maio de 2011, petições n.ºs 33810/07 e 18817/08 202
*Association for European Integration and Human Rights e Ekimdzhiev
c. Bulgária* de 28 de junho de 2007, petição n.º 62540/00 68
Avilkina e outros c. Rússia de 6 de junho de 2013, petição n.º 1585/09 185
Axel Springer AG c. Alemanha [GS] de 7 de fevereiro de 2012,
petição n.º 39954/08 ..... 13, 25, 199

B.B. c. França de 17 de dezembro de 2009,
petição n.º 5335/06 ..... 153, 155, 200, 201
Bernh Larsen Holding AS e outros c. Noruega
de 14 de março de 2013, petição n.º 24117/08 ..... 35, 38, 200
Biriuk c. Lituânia de 25 de novembro de 2008,
petição n.º 23373/03 ..... 27, 111, 184, 200
Bykov c. Rússia [GS] de 10 de março de 2009, petição n.º 4378/02 202

Cemalettin Canli c. Turquia de 18 de novembro de 2008,
petição n.º 22427/04 ..... 109, 116, 200
Ciubotaru c. Moldávia de 27 de abril de 2010,
petição n.º 27138/04 ..... 109, 118, 201
Copland c. Reino Unido de 3 de abril de 2007,
petição n.º 62617/00 ..... 15, 175, 182, 201
Cotlet c. Roménia de 3 de junho de 2003, petição n.º 38565/97 201

Dalea c. França de 2 de fevereiro de 2010,
petição n.º 964/07 ..... 116, 154, 170, 200

Gaskin c. Reino Unido de 7 de julho de 1989,
petição n.º 10454/83 ..... 113, 199, 200
Godelli c. Itália de 25 de setembro de 2012,
petição n.º 33783/09 ..... 40, 113, 199, 201

Halford c. Reino Unido de 25 de junho de 1997, petição n.º 20605/92 ..... 190, 201
Haralambie c. Roménia de 27 de outubro de 2009,
petição n.º 21737/03 ..... 66, 79, 200

I. c. Finlândia de 17 de julho de 2008,
petição n.º 20511/03 ..... 15, 84, 98, 135, 184, 200, 201, 202
Iordachi e outros c. Moldávia de 10 de fevereiro de 2009, petição n.º 25198/02 67

K.H. e outros c. Eslováquia de 28 de abril de 2009,
petição n.º 32881/04 ..... 66, 80, 113, 184, 199
K.U. c. Finlândia de 2 de dezembro de 2008,
petição n.º 2872/02 ..... 15, 111, 131, 135, 199, 202
Kennedy c. Reino Unido de 18 de maio de 2010, petição n.º 26839/05 202
Khelili c. Suíça de 18 de outubro de 2011, petição n.º 16188/07 ..... 65, 69, 200
Klass e outros c. Alemanha de 6 de setembro de 1978,
petição n.º 5029/71 ..... 15, 156, 202
Köpke c. Alemanha de 5 de outubro de 2010, petição n.º 420/07 ..... 44, 131, 202
Kopp c. Suíça de 25 de março de 1998, petição n.º 23224/94 67
Kruslin c. França de 24 de abril de 1990, petição n.º 11801/85 201

L.L. c. França de 10 de outubro de 2006, petição n.º 7508/02 ..... 184, 200
Lambert c. França de 24 de agosto de 1998, petição n.º 23618/94 201
Leander c. Suécia de 26 de março de 1987,
petição n.º 9248/81 ..... 15, 65, 69, 70, 113, 121, 155, 199, 200, 201
Liberty e outros c. Reino Unido de 1 de julho de 2008,
petição n.º 58243/00 ..... 38, 201

M. G. c. Reino Unido de 24 de setembro de 2002, petição n.º 39393/98 200
M.K. c. França de 18 de abril de 2013, petição n.º 19522/09 ..... 117, 155
M.M. c. Reino Unido de 13 de novembro de 2012,
petição n.º 24029/07 ..... 78, 155, 200
M.S. c. Suécia de 27 de agosto de 1997 petição n.º 34209/96 ..... 121, 200, 202
Malone c. Reino Unido de 2 de agosto de 1984,
petição n.º 8691/79 ..... 15, 68, 180, 200, 201
McMichael c. Reino Unido de 24 de fevereiro de 1995, petição n.º 16424/90 200
Michaud c. França de 6 de dezembro de 2012,
petição n.º 12323/11 ..... 176, 190, 201, 202
Mosley c. Reino Unido de 10 de maio de 2011,
petição n.º 48009/08 ..... 13, 26, 121, 201, 202

Müller e outros c. Suíça de 24 de maio de 1988, petição n.º 10737/84 32

Niemietz c. Alemanha de 16 de dezembro de 1992,
petição n.º 13710/88 ..... 37, 190, 201

Odièvre c. França [GS] de 13 de fevereiro de 2003,
petição n.º 42326/98.....40, 113, 199, 201

P.G. e J.H. c. Reino Unido de 25 de setembro de 2001,
petição n.º 44787/98 ..... 44, 203
Peck c. Reino Unido de 28 de janeiro de 2003,
petição n.º 44647/98..... 44, 65, 69, 202

Rotaru c. Roménia [GS] de 4 de maio de 2000,
petição n.º 28341/95.....37, 65, 68, 118, 200, 202

S. e Marper c. Reino Unido de 4 de dezembro de 2008,
petições n.ºs 30562/04 e 30566/04..... 15, 78, 153, 155, 200, 202
Sciacca c. Itália de 11 de janeiro de 2005, petição n.º 50774/99..... 44, 201
Segerstedt-Wiberg e outros c. Suécia de 6 de junho de 2006,
petição n.º 62332/00..... 109, 117, 201
Shimovolos c. Rússia de 21 de junho de 2011, petição n.º 30194/09.....68, 200
Silver e outros c. Reino Unido de 25 de março de 1983,
petições n.ºs 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 68
Szuluk c. Reino Unido de 2 de junho de 2009,
petição n.º 36936/05..... 184, 200, 201

Társaság a Szabadságjogokért c. Hungria de 14 de abril de 2009 .....13, 30
Taylor-Sabori c. Reino Unido de 22 de outubro de 2002,
petição n.º 47114/99 ..... 65, 68, 202
The Sunday Times c. Reino Unido de 26 de abril de 1979, petição n.º 6538/74 68
Turek c. Eslováquia de 14 de fevereiro de 2006, petição n.º 57986/00..... 200

Uzun c. Alemanha de 2 de setembro de 2010,
petição n.º 35623/05.....15, 44, 200, 202

Vereinigung bildender Künstler c. Áustria, de 25 de janeiro de 2007,
petição n.º 68345/01.....13, 32

Vetter c. França de 31 de maio de 2005, petição n.º 59842/00 ..... 68, 153, 157, 202
Von Hannover c. Alemanha (n.º 2) [GS] de 7 de fevereiro de 2012, petições n.ºs 40660/08 e 60641/08 ..... 23, 25, 199, 202
Von Hannover c. Alemanha de 24 de junho de 2004, petição n.º59320/00 ..... 44, 199, 201, 202

Wisse c. França de 20 de dezembro de 2005, petição n.º 71611/01 ..... 44, 203

Z. c. Finlândia de 25 de fevereiro de 1997, petição n.º 22009/93 ..... 175, 184, 200

Jurisprudência dos tribunais nacionais

Alemanha, Tribunal Constitucional Federal (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 de março de 2010 180

Roménia, Tribunal Constitucional da Roménia (*Curtea Constituțională a României*), n.º 1258, 8 de outubro de 2009 180

Tribunal Constitucional da República Checa (*Ústavní soud České republiky*), 94/2011 Coll., 22 de março de 2011 180

Agência dos Direitos Fundamentais da União Europeia
Conselho da Europa – Tribunal Europeu dos Direitos do Homem

Manual da Legislação Europeia sobre Proteção de Dados

2014 — 212 páginas — 14,8 × 21 cm

ISBN 978-92-871-9939-3 (Conselho da Europa)
ISBN 978-92-9239-498-1 (FRA)
doi:10.2811/73790

Sobre a Agência dos Direitos Fundamentais da União Europeia, está disponível um vasto conjunto de informação, que pode ser consultado através do sítio da Internet da FRA em (fra.europa.eu).

Encontram-se disponíveis numerosas outras informações sobre o Conselho da Europa na rede Internet, via servidor hub.coe.int.

Sobre a jurisprudência do Tribunal Europeu dos Direitos do Homem, está disponível mais informação no sítio da Internet do Tribunal: echr.coe.int. O portal de pesquisa HUDOC dá acesso aos julgamentos e decisões em inglês e/ou francês, traduções para línguas adicionais, sumários legais, comunicados de imprensa e outra informação sobre os trabalhos do Tribunal.

COMO OBTER PUBLICAÇÕES DA UNIÃO EUROPEIA

Publicações gratuitas:
- um exemplar:
  via EU Bookshop (http://bookshop.europa.eu);
- mais do que um exemplar/cartazes/mapas:
  nas representações da União Europeia (http://ec.europa.eu/represent_pt.htm),
  nas delegações em países fora da UE (http://eeas.europa.eu/delegations/index_pt.htm),
  contactando a rede Europe Direct (http://europa.eu/europedirect/index_pt.htm)
  ou pelo telefone 00 800 6 7 8 9 10 11 (gratuito em toda a UE) (*).

Publicações pagas:
- via EU Bookshop (http://bookshop.europa.eu);

Assinaturas pagas:
- através de um dos agentes de vendas do Serviço das Publicações da União Europeia (http://publications.europa.eu/others/agents/index_pt.htm).

(*) As informações prestadas são gratuitas, tal como a maior parte das chamadas, embora alguns operadores, cabinas telefónicas ou hotéis as possam cobrar.

Como obter publicações do Conselho da Europa

O Serviço de Publicações do Conselho da Europa produz obras em todas as áreas de referência da organização, incluindo direitos do Homem, ciência jurídica, saúde, ética, assuntos sociais, ambiente, educação, cultura, desporto, juventude e património arquitetónico. Os livros e as publicações eletrónicas deste vasto catálogo podem ser encomendados em linha (http://book.coe.int/).

Uma sala de leitura virtual permite que os utilizadores consultem gratuitamente excertos das principais obras acabadas de publicar ou o texto completo de certos documentos oficiais.

Estão disponíveis informações sobre as convenções do Conselho da Europa, bem como os textos completos das mesmas, no sítio web do Gabinete do Tratado: http://conventions.coe.int/.

10.2811/73790
TK-01-13-772-PT-C

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

A rápida evolução das tecnologias da informação e da comunicação reforça a necessidade de assegurar uma proteção sólida dos dados pessoais – um direito garantido por instrumentos da União Europeia (UE) e do Conselho da Europa (CdE). Os avanços tecnológicos expandem as fronteiras, por exemplo, da vigilância, da interceção das comunicações e do armazenamento dos dados; todas estas atividades colocam desafios significativos ao direito à proteção de dados. O presente manual visa familiarizar os profissionais do Direito que não são especializados em proteção de dados com esta área do Direito. Apresenta uma visão geral dos quadros jurídicos da UE e do CdE aplicáveis. Explica a jurisprudência mais importante, resumindo as principais decisões do Tribunal Europeu dos Direitos do Homem (TEDH) e do Tribunal de Justiça da União Europeia (TJUE). Nos casos em que ainda não existe jurisprudência, apresenta exemplos práticos com cenários hipotéticos. Em resumo, o presente manual visa ajudar a garantir uma defesa vigorosa e determinada do direito à proteção de dados.

AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA
Schwarzenbergplatz 11 – 1040 Viena – Áustria
Tel. +43 (1) 580 30-60 – Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

CONSELHO DA EUROPA
TRIBUNAL EUROPEU DOS DIREITOS DO HOMEM
67075 Estrasburgo Cedex – França
Tel. +33 (0) 3 88 41 20 00 – Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Serviço das Publicações
ISBN 978-92-871-9939-3 (Conselho da Europa)
ISBN 978-92-9239-498-1 (FRA)