



Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Terceira Secção)

11 de dezembro de 2019*

[Texto retificado por Despacho de 13 de fevereiro de 2020]

«Reenvio prejudicial — Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.º e 8.º — Diretiva 95/46/CE — Artigo 6.º, n.º 1, alínea c), e artigo 7.º, alínea f) — Legitimidade para o tratamento de dados pessoais — Legislação nacional que permite a videovigilância para garantir a segurança e proteção das pessoas, bens e valores e para a prossecução de interesses legítimos, sem o consentimento da pessoa em causa — Instalação de um sistema de videovigilância nas partes comuns de um edifício para habitação»

No processo C-708/18,

que tem por objeto um pedido de decisão prejudicial apresentado, nos termos do artigo 267.º TFUE, pelo Tribunalul București (Tribunal de Primeira Instância de Bucareste, Roménia), por Decisão de 2 de outubro de 2018, que deu entrada no Tribunal de Justiça em 6 de novembro de 2018, no processo

TK

contra

Asociația de Proprietari bloc M5A-ScaraA,

O TRIBUNAL DE JUSTIÇA (Terceira Secção),

composto por: A. Prechal (relatora), presidente de secção, L. S. Rossi, J. Malenovský, F. Biltgen e N. Wahl, juízes,

advogado-geral: G. Pitruzzella,

secretário: A. Calot Escobar,

vistos os autos,

vistas as observações apresentadas:

- em representação do Governo romeno, por C.-R. Canțăr, O.-C. Ichim e A. Wellman, na qualidade de agentes,
- em representação do Governo checo, por M. Smolek, J. Vlácil e O. Serdula, na qualidade de agentes,

* Língua do processo: romeno.

- em representação do Governo dinamarquês, por J. Nymann-Lindegren, M. Wolff e P. Z. L. Ngo, na qualidade de agentes,
- [Conforme retificado por Despacho de 13 de fevereiro de 2020] em representação da Irlanda, por M. Browne, G. Hodge e A. Joyce, na qualidade de agentes, assistidos por D. Fennelly, BL,
- em representação do Governo austríaco, inicialmente por G. Hesse e J. Schmolle e, em seguida por J. Schmoll, na qualidade de agentes,
- em representação do Governo português, por L. Inez Fernandes, P. Barros da Costa, L. Medeiros, I. Oliveira e M. Cancela Carvalho, na qualidade de agentes,
- em representação da Comissão Europeia, por H. Kranenborg, D. Nardi e L. Nicolae, na qualidade de agentes,

vista a decisão tomada, ouvido o advogado-geral, de julgar a causa sem apresentação de conclusões,
profere o presente

Acórdão

- 1 O pedido de decisão prejudicial tem por objeto a interpretação do artigo 6.º, n.º 1, alínea e), e do artigo 7.º, alínea f), da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO 1995, L 281, p. 31), bem como dos artigos 8.º e 52.º da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»).
- 2 Este pedido foi apresentado no âmbito de um litígio que opõe TK à AsociaȚia de Proprietari bloc M5A-Scara A (Associação dos condóminos do edifício M5A-Escada A, Roménia, a seguir designada «Associação dos Condóminos»), a respeito do pedido de TK para que esta associação desative o sistema de videovigilância deste edifício e retire as câmaras instaladas nas partes comuns do mesmo.

Quadro jurídico

Direito da União

- 3 A Diretiva 95/46 foi revogada e substituída, com efeitos a partir de 25 de maio de 2018, pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO 2016, L 119, p. 1). Todavia, tendo em conta a data dos factos em causa no processo principal, o litígio continua a ser regulado pelas disposições dessa diretiva.
- 4 A Diretiva 95/46, segundo o seu artigo 1.º, tinha por objetivo a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais, bem como a eliminação dos obstáculos à livre circulação desses dados.
- 5 O artigo 3.º dessa diretiva previa, no seu n.º 1:

«A presente diretiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados.»

6 O capítulo II da referida diretiva incluía uma secção I, intitulada «Princípios relativos à qualidade dos dados», composta pelo artigo 6.º dessa mesma diretiva, que dispunha:

«1. Os Estados-Membros devem estabelecer que os dados pessoais serão:

- a) Objeto de um tratamento leal e lícito;
- b) Recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-Membros estabeleçam garantias adequadas;
- c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente;
- d) Exatos e, se necessário, atualizados; devem ser tomadas todas as medidas razoáveis para assegurar que os dados inexatos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente, sejam apagados ou retificados;
- e) 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. Os Estados-Membros estabelecerão garantias apropriadas para os dados pessoais conservados durante períodos mais longos do que o referido, para fins históricos, estatísticos ou científicos.

2. Incumbe ao responsável pelo tratamento assegurar a observância do disposto no n.º 1.»

7 Na secção II desse capítulo II, intitulada «Princípios relativos à legitimidade do tratamento de dados», o artigo 7.º da Diretiva 95/46 tinha a seguinte redação:

«Os Estados-Membros estabelecerão que o tratamento de dados pessoais só poderá ser efetuado se:

- a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento;
ou
- b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa;
ou
- c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito;
ou
- d) O tratamento for necessário para a proteção de interesses vitais da pessoa em causa;
ou
- e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

ou

- f) O tratamento 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 ao abrigo do n.º 1 do artigo 1.º»

Direito romeno

- 8 A Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Lei n.º 677/2001 sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados) (*Monitorul Oficial*, parte I, n.º 790, de 12 de dezembro de 2001), conforme alterada pela Lei n.º 102/2005 e pelo Decreto-Lei governamental de emergência n.º 36/2007, aplicável, *ratione temporis*, ao processo principal, foi adotada para a transposição da Diretiva 95/46 para o direito romeno.
- 9 O artigo 5.º dessa lei dispunha:
- «1. Qualquer tratamento de dados pessoais, exceto quando for referente a dados pertencentes às categorias mencionadas nos artigos 7.º, n.º 1, 8.º e 10.º, só pode ser efetuado se a pessoa em causa tiver dado expressa e inequivocamente o seu consentimento para esse tratamento.
2. O consentimento do titular dos dados não é exigido nos seguintes casos:
- a) quando o tratamento for necessário para a execução de um contrato ou em negociações pré-contratuais em que seja parte o titular dos dados ou para a adoção de medidas, a seu pedido, antes da celebração de um contrato ou durante as negociações pré-contratuais;
- b) quando o tratamento for necessário para a proteção da vida, da integridade física ou da saúde do titular dos dados ou de outra pessoa exposta a ameaça;
- c) quando o tratamento for necessário para o cumprimento de uma obrigação legal do responsável pelo tratamento;
- d) quando o tratamento for necessário para a execução de atribuições de interesse público ou destinadas ao exercício de prerrogativas de poder público de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;
- e) quando o tratamento for necessário para a realização de um interesse legítimo do responsável pelo tratamento ou do terceiro a quem os dados são comunicados, desde que esse interesse não afete os interesses ou os direitos e liberdades fundamentais do titular dos dados;
- f) quando o tratamento disser respeito a dados provenientes de documentos acessíveis ao público, nos termos da lei;
- g) quando o tratamento for efetuado exclusivamente para fins estatísticos, de investigação histórica ou científica, e os dados permanecerem anónimos durante todo o tratamento.
3. O disposto no n.º 2 não prejudica as disposições legais que regem a obrigação das autoridades públicas de respeitar e proteger a vida íntima, familiar e privada.»

- 10 A Decisão n.º 52/2012 da Autoritate Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Autoridade Nacional de Supervisão do Tratamento de Dados Pessoais, Roménia, a seguir «ANSPDCP»), relativa ao tratamento de dados pessoais obtidos por videovigilância, na versão aplicável ao processo principal, previa, no seu artigo 1.º:

«A recolha, gravação, armazenamento, utilização, transmissão, divulgação ou qualquer outra operação de tratamento de imagens por videovigilância, que permita, direta ou indiretamente, identificar pessoas singulares, constituem operações de tratamento de dados pessoais abrangidas pelo âmbito de aplicação da [Lei n.º 677/2001].»

- 11 O artigo 4.º dessa decisão dispunha:

«A videovigilância pode ser realizada principalmente para os seguintes fins:

- a) prevenção e combate à criminalidade;
- b) monitorização do tráfego rodoviário e das infrações ao direito estradal;
- c) segurança e proteção de pessoas, bens e valores, edifícios e instalações de utilidade pública e respetivos recintos;
- d) execução de medidas de interesse público ou exercício de prerrogativas de poder público;
- e) realização de interesses legítimos, desde que não sejam violados os direitos e liberdades fundamentais das pessoas em causa.»

- 12 Nos termos do artigo 5.º, n.ºs 1 a 3, da referida decisão:

«1. A videovigilância pode ser efetuada em locais e espaços abertos ou destinados ao público, incluindo vias públicas de acesso situadas no domínio público ou privado, nas condições previstas na lei.

2. As câmaras de videovigilância são instaladas de forma visível.

3. É proibida a utilização de câmaras de videovigilância dissimuladas, exceto nos casos previstos na lei.»

- 13 O artigo 6.º da mesma decisão estabelecia:

«O tratamento de dados pessoais através de sistemas de videovigilância é efetuado com o consentimento expreso e inequívoco da pessoa em causa ou nos casos previstos no artigo 5.º, n.º 2, da Lei n.º 677/2001 [...]»

Litígio no processo principal e questões prejudiciais

- 14 TK reside num apartamento, do qual é proprietário, localizado no edifício M5A. A associação dos condóminos desse edifício, a pedido de alguns condóminos, aprovou uma decisão na assembleia geral de 7 de abril de 2016 para a instalação de câmaras de videovigilância no edifício.

- 15 Em execução desta decisão, foram instaladas três câmaras de videovigilância nas partes comuns do edifício M5A. A primeira câmara foi direcionada para a fachada do edifício, enquanto a segunda e a terceira câmaras foram instaladas, respetivamente, no átrio do rés-do-chão e no elevador do edifício.

- 16 TK opôs-se à instalação deste sistema de videovigilância por constituir uma violação do direito à reserva da vida privada.
- 17 Tendo constatado que, apesar de todas as diligências que efetuou e do reconhecimento por escrito, por parte da associação dos condóminos do edifício, da ilegalidade do sistema de videovigilância instalado, esse sistema continuava a funcionar, TK intentou uma ação no órgão jurisdicional de reenvio para que a referida associação fosse condenada a retirar as três câmaras e a desativá-las definitivamente, sob pena de sanção pecuniária compulsória.
- 18 No referido órgão jurisdicional, TK alegou que o sistema de videovigilância em causa violava o direito primário e derivado da União, em especial o direito à reserva da vida privada, e o direito nacional relativo à reserva da vida privada. Alegou, por outro lado, que a associação dos condóminos do edifício tinha assumido a função de responsável pelo tratamento dos dados pessoais sem ter seguido o procedimento de registo previsto na lei para o efeito.
- 19 A associação dos condóminos do edifício informou que a decisão de instalar um sistema de videovigilância tinha sido tomada para controlar as movimentações no edifício da forma mais eficaz possível, devido ao facto de o elevador ter sido várias vezes vandalizado e vários apartamentos e partes comuns terem sido objeto de assaltos e furtos.
- 20 Esclareceu igualmente que as medidas que anteriormente tomou, nomeadamente a instalação de um sistema de entrada no edifício com intercomunicador e cartão magnético, não tinham impedido a prática repetida deste tipo de ilícitos.
- 21 Além disso, a associação dos condóminos do edifício enviou a TK a ata elaborada com a empresa que instalou as câmaras do sistema de videovigilância, indicando que, em 21 de outubro de 2016, o disco rígido do sistema tinha sido apagado e desligado, tendo sido posto fora de serviço e apagadas as imagens gravadas.
- 22 Enviou-lhe igualmente outra ata, datada de 18 de maio de 2017, da qual resulta que as três câmaras de videovigilância tinham sido desinstaladas. Esta ata precisava que a associação dos condóminos do edifício tinha, entretanto, concluído o procedimento que lhe permitia estar registada como responsável pelo tratamento de dados pessoais.
- 23 No entanto, TK assinalou ao órgão jurisdicional de reenvio que as três câmaras de videovigilância ainda se encontravam instaladas.
- 24 O órgão jurisdicional de reenvio salienta que o artigo 5.º da Lei n.º 677/2001 prevê, de um modo geral, que o tratamento de dados pessoais, como o registo de imagens através de um sistema de videovigilância, só pode ser efetuado se a pessoa em causa tiver dado o seu consentimento de modo expreso e inequívoco. No entanto, o n.º 2 do mesmo artigo prevê uma série de exceções a esta regra, entre as quais a de que o tratamento de dados pessoais seja necessário para proteger a vida, a integridade física ou a saúde do titular dos dados ou de outra pessoa exposta a ameaça. A Decisão n.º 52/2012 da ANSPDCP prevê uma exceção semelhante.
- 25 O órgão jurisdicional de reenvio refere em seguida, nomeadamente, o artigo 52.º, n.º 1, da Carta, que estabelece o princípio de que deve haver uma relação de proporcionalidade entre o objetivo prosseguido pela ingerência nos direitos e liberdades dos cidadãos e os meios utilizados.
- 26 Ora, segundo o referido órgão jurisdicional, o sistema de videovigilância em causa não parece ter sido utilizado de forma ou com uma finalidade que não correspondesse ao objetivo declarado pela associação dos condóminos do edifício, a saber, a proteção da vida, da integridade física e da saúde das pessoas em causa, ou seja, os condóminos do edifício em que o sistema foi instalado.

27 Nestas circunstâncias, o Tribunalul București (Tribunal de Primeira Instância de Bucareste, Roménia) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

- «1) Devem os artigos 8.º e 52.º da [Carta] e o artigo 7.º, alínea f), da [Diretiva 95/46] ser interpretados no sentido de que se opõem a uma disposição nacional como a que está em causa no processo principal, concretamente, o artigo 5.º, n.º 2, da [Lei n.º 677/2001] e o artigo 6.º da [Decisão n.º 52/2012 da ANSPDCP], que prevê a possibilidade de utilização de videovigilância para garantir a segurança e a proteção das pessoas, bens e valores e para a prossecução de interesses legítimos, sem o consentimento da pessoa em causa?
- 2) Devem os artigos 8.º e 52.º da [Carta] ser interpretados no sentido de que a limitação dos direitos e das liberdades através da videovigilância respeita o princípio da proporcionalidade, preenche o requisito da necessidade e corresponde a finalidades de interesse geral ou à exigência de proteger os direitos e as liberdades de terceiros, quando o operador possa adotar outras medidas para a proteção do interesse legítimo em questão?
- 3) Deve o artigo 7.º, alínea f), da [Diretiva 95/46] ser interpretado no sentido de que o “interesse legítimo” do responsável pelo tratamento deve ser comprovado, existente e efetivo no momento do tratamento?
- 4) Deve o artigo 6.º, n.º 1, alínea e), da [Diretiva 95/46] ser interpretado no sentido de que um tratamento (a videovigilância) é excessivo ou inadequado quando o operador pode adotar outra medida para a proteção do interesse legítimo em questão?»

Quanto às questões prejudiciais

- 28 A título preliminar, importa declarar, em primeiro lugar, que, embora o órgão jurisdicional de reenvio se refira, na sua quarta questão, ao artigo 6.º, n.º 1, alínea e), da Diretiva 95/46, não fornece nenhuma explicação sobre a relevância dessa disposição para a decisão da causa principal.
- 29 Com efeito, essa disposição diz apenas respeito aos requisitos que a conservação de dados pessoais deve observar. No entanto, nada no processo à disposição do Tribunal de Justiça permite considerar que o litígio no processo principal diga respeito a este aspeto.
- 30 Em contrapartida, na medida em que, através dessa questão, o órgão jurisdicional de reenvio pergunta, em substância, se a instalação de um sistema de videovigilância, como o que está em causa, é proporcional aos fins prosseguidos, importa salientar que a questão de saber se os dados pessoais recolhidos por esse sistema cumprem o requisito da proporcionalidade diz respeito à interpretação do artigo 6.º, n.º 1, alínea c), da Diretiva 95/46.
- 31 Ora, esta última disposição deve ser tida em conta aquando da verificação do segundo requisito de aplicação previsto no artigo 7.º, alínea f), da Diretiva 95/46, segundo o qual o tratamento de dados pessoais deve ser «necessário» à realização do interesse legítimo prosseguido.
- 32 Em segundo lugar, com a sua primeira e segunda questões, o órgão jurisdicional de reenvio refere-se aos artigos 8.º e 52.º da Carta, isoladamente considerados ou conjugados com o artigo 7.º, alínea f), da Diretiva 95/46. Ora, o Tribunal de Justiça já esclareceu que a apreciação do requisito previsto nessa disposição, relativo à existência de direitos e liberdades fundamentais da pessoa em causa para a proteção de dados que prevaleceriam sobre o interesse legítimo prosseguido pelo responsável pelo tratamento dos dados ou pelo terceiro ou terceiros a quem os dados são comunicados, necessita que se proceda a uma ponderação dos direitos e interesses opostos em causa em função das circunstâncias concretas do caso em apreço, no âmbito da qual deve ser tida em conta a importância dos direitos da

pessoa em causa resultantes dos artigos 7.º e 8.º da Carta (Acórdão de 24 de novembro de 2011, Asociación Nacional de Establecimientos Financieros de Crédito, C-468/10 e C-469/10, EU:C:2011:777, n.º 40). Daqui resulta que os artigos 8.º e 52.º não devem, no caso vertente, ser aplicados isoladamente.

- 33 Em face do exposto, há que considerar que, com as suas questões, que importa analisar em conjunto, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 6.º, n.º 1, alínea c), e o artigo 7.º, alínea f), da Diretiva 95/46, lidos à luz dos artigos 7.º e 8.º da Carta, devem ser interpretados no sentido de que se opõem a disposições nacionais que autorizam a instalação de um sistema de videovigilância, como o sistema em causa no processo principal, instalado nas partes comuns de um imóvel para habitação, para prosseguir interesses legítimos de garantia da segurança e da proteção das pessoas e dos bens, sem o consentimento das pessoas em causa.
- 34 Importa recordar que uma vigilância efetuada por meio de uma gravação vídeo de pessoas, guardada num dispositivo de gravação em circuito contínuo, a saber, o disco rígido, constitui, nos termos do artigo 3.º, n.º 1, da Diretiva 95/46, um tratamento de dados pessoais automatizado (Acórdão de 11 de dezembro de 2014, Ryněš, C-212/13, EU:C:2014:2428, n.º 25).
- 35 Por conseguinte, um sistema de videovigilância através de uma câmara deve ser qualificado de tratamento de dados pessoais automatizado, na aceção dessa disposição, quando o dispositivo instalado permita gravar e armazenar dados pessoais, tais como imagens que permitam identificar pessoas singulares. Incumbe ao órgão jurisdicional de reenvio verificar se o sistema em causa no processo principal apresenta essas características.
- 36 Além disso, qualquer tratamento de dados pessoais deve, por um lado, ser conforme com os princípios relativos à qualidade dos dados, enunciados no artigo 6.º da Diretiva 95/46, e, por outro, cumprir um dos princípios relativos à legitimidade do tratamento de dados, enumerados no artigo 7.º dessa diretiva (Acórdão de 13 de maio de 2014, Google Spain e Google, C-131/12, EU:C:2014:317, n.º 71 e jurisprudência aí referida).
- 37 O artigo 7.º da Diretiva 95/46 estabelece uma lista exaustiva e taxativa dos casos em que o tratamento de dados pessoais pode ser considerado lícito. Os Estados-Membros não podem acrescentar novos princípios relativos à legitimidade do tratamento de dados pessoais ao referido artigo nem prever exigências suplementares que venham alterar o alcance de um dos seis princípios previstos nesse artigo (Acórdão de 19 de outubro de 2016, Breyer, C-582/14, EU:C:2016:779, n.º 57).
- 38 Daqui decorre que, para ser considerado legítimo, o tratamento de dados pessoais deve integrar-se num dos seis casos previstos no artigo 7.º da Diretiva 95/46.
- 39 As questões submetidas pelo órgão jurisdicional de reenvio dizem respeito, em especial, ao princípio da legitimidade do tratamento de dados previsto no artigo 7.º, alínea f), da Diretiva 95/46, disposição que foi transposta para o ordenamento jurídico romeno pelo artigo 5.º, n.º 2, alínea e), da Lei n.º 677/2001, para o qual remete também o artigo 6.º da Decisão n.º 52/2012 da ANSPDCP no que diz especificamente respeito ao tratamento de dados pessoais através de videovigilância.
- 40 A este propósito, o artigo 7.º, alínea f), da Diretiva 95/46 prevê três requisitos cumulativos para que o tratamento de dados pessoais seja lícito, a saber, em primeiro lugar, a prossecução de interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, em segundo lugar, a necessidade do tratamento dos dados pessoais para a realização do interesse legítimo e, em terceiro lugar, o requisito de os direitos e as liberdades fundamentais da pessoa a que a proteção de dados diz respeito não prevalecerem sobre o interesse legítimo prosseguido (Acórdão de 4 de maio de 2017, Rigas satiksme, C-13/16, EU:C:2017:336, n.º 28).

- 41 Há que sublinhar que o artigo 7.º, alínea f), da Diretiva 95/46 não exige o consentimento da pessoa em causa. No entanto, esse consentimento, enquanto requisito para o tratamento dos dados pessoais, figura apenas na alínea a) do artigo 7.º dessa diretiva.
- 42 No caso em apreço, o objetivo que, em substância, é visado pelo responsável pelo tratamento dos dados quando instala um sistema de videovigilância como o que está em causa no processo principal, a saber, a proteção dos bens, da saúde e da vida dos condóminos de um imóvel, é suscetível de ser qualificado de «interesse legítimo», na aceção do artigo 7.º, alínea f), da Diretiva 95/46. Em princípio, afigura-se que o primeiro requisito previsto nesta disposição está preenchido (v., por analogia, Acórdão de 11 de dezembro de 2014, Ryneš, C-212/13, EU:C:2014:2428, n.º 34).
- 43 Todavia, o órgão jurisdicional de reenvio interroga-se sobre se o primeiro dos requisitos previstos neste artigo 7.º, alínea f), deve ser entendido no sentido de que o interesse prosseguido pelo responsável em causa deve, por um lado, ser «comprovado» e, por outro, ser «existente e efetivo no momento do tratamento».
- 44 A este respeito, deve salientar-se que, à semelhança do que alegaram os Governos romeno e checo, a Irlanda, o Governo austríaco, o Governo português e a Comissão, uma vez que, em conformidade com o artigo 7.º, alínea f), da Diretiva 95/46, o responsável pelo tratamento dos dados pessoais ou o terceiro a quem os dados são comunicados deve prosseguir um interesse legítimo que justifique esse tratamento, esse interesse deve ser existente e efetivo no momento do tratamento, e não de natureza hipotética. No entanto, não é necessariamente de exigir, na avaliação de todas as circunstâncias do presente caso, que tenha havido um prejuízo concreto anterior para a segurança dos bens e das pessoas.
- 45 No caso em apreço, numa situação como a que está em causa no processo principal, o requisito da verificação de um interesse existente e efetivo parece, em todo o caso, estar preenchido, uma vez que o órgão jurisdicional de reenvio declara que os furtos, os assaltos e os atos de vandalismo ocorreram antes da instalação do sistema de videovigilância e apesar da instalação, na entrada do edifício, de um sistema de segurança constituído por um intercomunicador e um cartão magnético.
- 46 No que respeita ao segundo requisito previsto no artigo 7.º, alínea f), da Diretiva 95/46, relativo à necessidade do tratamento dos dados pessoais para a prossecução do interesse legítimo, o Tribunal de Justiça recordou que as derrogações e as restrições ao princípio da proteção dos dados pessoais devem ocorrer na estrita medida do necessário (Acórdão de 4 de maio de 2017, Rīgas satiksme, C-13/16, EU:C:2017:336, n.º 30 e jurisprudência aí referida).
- 47 Este requisito impõe ao órgão jurisdicional de reenvio que verifique se o interesse legítimo do tratamento dos dados prosseguido pela videovigilância em causa no processo principal, que consiste, em substância, em garantir a segurança dos bens e das pessoas e prevenir a ocorrência de infrações, não pode razoavelmente ser alcançado de modo igualmente eficaz através de outros meios menos atentatórios dos direitos e liberdades fundamentais das pessoas em causa, em especial dos direitos à reserva da vida privada e à proteção dos dados pessoais garantidos pelos artigos 7.º e 8.º da Carta.
- 48 Além disso, como defendeu a Comissão, o requisito da necessidade do tratamento deve ser analisado juntamente com o chamado princípio da «minimização dos dados», consagrado no artigo 6.º, n.º 1, alínea c), da Diretiva 95/46, segundo o qual os dados pessoais devem ser «adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente».
- 49 Resulta do processo no Tribunal de Justiça que os requisitos relativos à proporcionalidade do tratamento dos dados em causa no processo principal parecem ter sido tomados em consideração. Com efeito, está assente que foram inicialmente postas em prática medidas alternativas constituídas

por um sistema de segurança, instalado na entrada do edifício, composto por um intercomunicador e um cartão magnético, que se revelaram insuficientes. Além disso, o sistema de videovigilância em questão está limitado às partes comuns do condomínio e às suas vias de acesso.

- 50 Todavia, a proporcionalidade do tratamento dos dados através de um sistema de videovigilância deve ser apreciada tendo em conta o modo concreto de instalação e de funcionamento desse dispositivo, que devem limitar o seu impacto sobre os direitos e liberdades das pessoas em causa, garantindo simultaneamente a eficácia do sistema de videovigilância em questão.
- 51 Assim, tal como argumentou a Comissão, o requisito da necessidade do tratamento implica que o responsável pelo tratamento deva analisar, por exemplo, se é suficiente que a videovigilância funcione apenas durante a noite ou fora do horário normal de trabalho e que bloqueie ou desfoque as imagens captadas em áreas onde a vigilância não seja necessária.
- 52 Por último, quanto ao terceiro requisito previsto no artigo 7.º, alínea f), da Diretiva 95/46, relativo à existência de direitos e liberdades fundamentais da pessoa afetada pela proteção de dados que prevaleçam sobre o interesse legítimo prosseguido pelo responsável pelo tratamento dos dados ou pelo terceiro ou terceiros a quem os dados sejam comunicados, há que recordar, como já foi mencionado no n.º 32 do presente acórdão, que a apreciação deste requisito implica uma ponderação dos direitos e interesses opostos em causa em função das circunstâncias concretas do caso concreto, no âmbito da qual se deve ter em conta a importância dos direitos da pessoa em causa que resultam dos artigos 7.º e 8.º da Carta.
- 53 Neste contexto, o Tribunal de Justiça já considerou que o artigo 7.º, alínea f), da Diretiva 95/46 se opõe a que um Estado-Membro exclua de forma categórica e generalizada a possibilidade de tratamento de algumas categorias de dados pessoais, sem permitir uma ponderação dos direitos e interesses opostos em causa num caso específico. Um Estado-Membro não pode assim prescrever, para essas categorias, de forma definitiva, o resultado da ponderação dos direitos e dos interesses opostos sem permitir um resultado diferente devido a circunstâncias particulares de um caso concreto (Acórdão de 19 de outubro de 2016, Breyer, C-582/14, EU:C:2016:779, n.º 62).
- 54 Resulta igualmente da jurisprudência do Tribunal de Justiça que, para proceder a essa ponderação, é possível tomar em consideração o caráter variável, em função da possibilidade de aceder aos dados em causa através de fontes acessíveis ao público, da gravidade da violação dos direitos fundamentais da pessoa em causa pelo referido tratamento (v., neste sentido, Acórdão de 4 de maio de 2017, Rīgas satiksme, C-13/16, EU:C:2017:336, n.º 32).
- 55 Diversamente dos tratamentos de dados que emanam de fontes acessíveis ao público, os tratamentos de dados que decorrem de fontes não acessíveis ao público implicam que certas informações sobre a vida privada da pessoa em causa passem a ser conhecidas pelo responsável pelo tratamento e, eventualmente, pelo terceiro ou terceiros a quem os dados sejam comunicados. Esta violação mais grave dos direitos da pessoa em causa, consagrados nos artigos 7.º e 8.º da Carta, deve ser tida em conta e ponderada com o interesse legítimo prosseguido pelo responsável pelo tratamento ou pelo terceiro ou terceiros a quem os dados sejam comunicados (v., neste sentido, Acórdão de 24 de novembro de 2011, Asociación Nacional de Establecimientos Financieros de Crédito, C-468/10 e C-469/10, EU:C:2011:777, n.º 45).
- 56 O critério relativo à gravidade da violação dos direitos e liberdades da pessoa em causa é um elemento essencial do exercício de ponderação casuístico exigido pelo artigo 7.º, alínea f), da Diretiva 95/46.
- 57 A este respeito, deve nomeadamente ser tida em conta a natureza dos dados pessoais em questão, em especial a natureza potencialmente sensível desses dados, bem como a natureza e as modalidades concretas do tratamento dos dados em questão, sobretudo o número de pessoas que têm acesso a esses dados e as modalidades de acesso aos mesmos.

- 58 Para efeitos desta ponderação, são igualmente relevantes as expectativas razoáveis da pessoa em causa de que os seus dados pessoais não serão tratados se, nas circunstâncias do caso concreto, a mesma não puder razoavelmente esperar um tratamento posterior dos dados.
- 59 Por último, estes elementos devem ser ponderados com a importância, para todos os condóminos do edifício em causa, do interesse legítimo prosseguido no caso vertente pelo sistema de videovigilância em questão, na medida em que visa essencialmente garantir a proteção dos bens, da saúde e da vida dos referidos condóminos.
- 60 Em face do exposto, há que responder às questões submetidas que o artigo 6.º, n.º 1, alínea c), e o artigo 7.º, alínea f), da Diretiva 95/46, lidos à luz dos artigos 7.º e 8.º da Carta, devem ser interpretados no sentido de que não se opõem a disposições nacionais que autorizam a instalação de um sistema de videovigilância, como o sistema em causa no processo principal, instalado nas partes comuns de um imóvel para habitação, para prosseguir interesses legítimos de garantia da segurança e da proteção das pessoas e dos bens, sem o consentimento das pessoas em causa, se o tratamento dos dados pessoais recolhidos através desse sistema de videovigilância cumprir os requisitos previstos no mencionado artigo 7.º, alínea f), o que incumbe ao órgão jurisdicional de reenvio verificar.

Quanto às despesas

- 61 Revestindo o processo, quanto às partes na causa principal, a natureza de incidente suscitado perante o órgão jurisdicional de reenvio, compete a este decidir quanto às despesas. As despesas efetuadas pelas outras partes para a apresentação de observações ao Tribunal de Justiça não são reembolsáveis.

Pelos fundamentos expostos, o Tribunal de Justiça (Terceira Secção) declara:

O artigo 6.º, n.º 1, alínea c), e o artigo 7.º, alínea f), da 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, lidos à luz dos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, devem ser interpretados no sentido de que não se opõem a disposições nacionais que autorizam a instalação de um sistema de videovigilância, como o sistema em causa no processo principal, instalado nas partes comuns de um imóvel para habitação, para prosseguir interesses legítimos de garantia da segurança e da proteção das pessoas e dos bens, sem o consentimento das pessoas em causa, se o tratamento dos dados pessoais recolhidos através desse sistema de videovigilância cumprir os requisitos previstos no mencionado artigo 7.º, alínea f), o que incumbe ao órgão jurisdicional de reenvio verificar.

Assinaturas