Coletânea da Jurisprudência

ACÓRDÃO DO TRIBUNAL DE JUSTIÇA (Terceira Secção)

14 de dezembro de 2023 *

«Reenvio prejudicial — Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais — Regulamento (UE) 2016/679 — Artigo 5.º — Princípios relativos a esse tratamento — Artigo 24.º — Responsabilidade do responsável pelo tratamento — Artigo 32.º — Medidas aplicadas para garantir a segurança do tratamento — Avaliação da adequação dessas medidas — Alcance da fiscalização jurisdicional — Administração da prova — Artigo 82.º — Direito de indemnização e responsabilidade — Eventual isenção de responsabilidade do responsável pelo tratamento em caso de violação cometida por terceiros — Pedido de indemnização por danos imateriais com base no receio de uma eventual utilização abusiva de dados pessoais»

No processo C-340/21,

que tem por objeto um pedido de decisão prejudicial apresentado, nos termos do artigo 267.º TFUE, pelo Varhoven administrativen sad (Supremo Tribunal Administrativo, Bulgária), por Decisão de 14 de maio de 2021, que deu entrada no Tribunal de Justiça em 2 de junho de 2021, no processo

VB

contra

Natsionalna agentsia za prihodite,

O TRIBUNAL DE JUSTIÇA (Terceira Secção),

composto por: K. Jürimäe, presidente de secção, N. Piçarra, M. Safjan, N. Jääskinen (relator) e M. Gavalec, juízes,

advogado-geral: G. Pitruzzella,

secretário: A. Calot Escobar,

vistos os autos,

vistas as observações apresentadas:

– em representação da Natsionalna agentsia za prihodite, por R. Spetsov,

* Língua do processo: búlgaro.

– em representação do Governo Búlgaro, por M. Georgieva e L. Zaharieva, na qualidade de agentes,

– em representação do Governo Checo, por O. Serdula, M. Smolek e J. Vláčil, na qualidade de agentes,

– em representação da Irlanda, por M. Browne, Chief State Solicitor, A. Joyce, J. Quaney e M. Tierney, na qualidade de agentes, assistidos por D. Fennelly, BL,

– em representação do Governo Italiano, por G. Palmieri, na qualidade de agente, assistida por E. De Bonis, avvocato dello Stato,

– em representação do Governo Português, por P. Barros da Costa, A. Pimenta, J. Ramos e C. Vieira Guerra, na qualidade de agentes,

– em representação da Comissão Europeia, por A. Bouchagiar, H. Kranenborg e N. Nikolova, na qualidade de agentes,

ouvidas as conclusões do advogado-geral na audiência de 27 de abril de 2023,

profere o presente

Acórdão

1 O pedido de decisão prejudicial tem por objeto a interpretação do artigo 5.º, n.º 2, dos artigos 24.º e 32.º, bem como do artigo 82.º, n.º 1 a 3, do 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO 2016, L 119, p. 1; a seguir «RGPD»).

2 Este pedido foi apresentado no âmbito de um litígio que opõe VB, uma pessoa singular, à Natsionalna agentsia za prihodite (Agência Nacional de Receitas Fiscais, Bulgária) (a seguir «NAP») a respeito da reparação dos danos imateriais que a referida pessoa afirma ter sofrido devido a um alegado incumprimento, por parte dessa autoridade pública, das suas obrigações legais enquanto responsável pelo tratamento de dados pessoais.

Quadro jurídico

3 Os considerandos 4, 10, 11, 74, 76, 83, 85 e 146 do RGPD têm a seguinte redação:

«(4) […] O presente regulamento respeita todos os direitos fundamentais e observa as liberdade[s] e os princípios reconhecidos na [Carta dos Direitos Fundamentais da União Europeia], consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, […] o direito à ação e a um tribunal imparcial […]

[…]

(10) A fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União [Europeia], o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros. É conveniente assegurar em toda a União a aplicação coerente e homogénea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais. […]

(11) A proteção eficaz dos dados pessoais na União exige o reforço e a especificação dos direitos dos titulares dos dados e as obrigações dos responsáveis pelo tratamento e pela definição do tratamento dos dados pessoais, […]

[…]

(74) Deverá ser consagrada a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas. Essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares.

[…]

(76) A probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento de dados. Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado.

[…]

(83) A fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a cifragem. Essas medidas deverão assegurar um nível de segurança adequado, nomeadamente a confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função dos riscos e da natureza dos dados pessoais a proteger. Ao avaliar os riscos para a segurança dos dados, deverão ser tidos em conta os riscos apresentados pelo tratamento dos dados pessoais, tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a danos físicos, materiais ou imateriais.

[…]

(85) Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais

protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares. Por conseguinte, logo que o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, deverá notificá-la à autoridade de controlo, sem demora injustificada […]

[…]

(146) O responsável pelo tratamento ou o subcontratante deverão reparar quaisquer danos de que alguém possa ser vítima em virtude de um tratamento que viole o presente regulamento […]. O responsável pelo tratamento ou o subcontratante pode ser exonerado da responsabilidade se provar que o facto que causou o dano não lhe é de modo algum imputável. O conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos do presente regulamento. Tal não prejudica os pedidos de indemnização por danos provocados pela violação de outras regras do direito da União ou dos Estados-Membros. Os tratamentos que violem o presente regulamento [a]brangem igualmente os que violem os atos delegados e de execução adotados nos termos do presente regulamento e o direito dos Estados-Membros que dê execução a regras do presente regulamento. Os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido. […]»

4 O artigo 4.º deste regulamento, sob a epígrafe «Definições», dispõe:

«Para efeitos do presente regulamento, entende-se por:

1) “Dados pessoais”, informação relativa a uma pessoa singular identificada ou identificável (“titular dos dados”); […]

2) “Tratamento”, uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados […]

[…]

7) “Responsável pelo tratamento”, a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; […]

[…]

10) “Terceiro”, a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais;

[…]

12) “Violação de dados pessoais”, uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;

[…]»

5 O artigo 5.º do referido regulamento, sob a epígrafe «Princípios relativos ao tratamento de dados pessoais», prevê:

«1. Os dados pessoais são:

a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados ("licitude, lealdade e transparência");

[…]

f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas ("integridade e confidencialidade");

2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo ("responsabilidade").»

6 Nos termos do artigo 24.º do mesmo regulamento, sob a epígrafe «Responsabilidade do responsável pelo tratamento»:

«1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

2. Caso sejam proporcionadas em relação às atividades de tratamento, as medidas a que se refere o n.º 1 incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento.

3. O cumprimento de códigos de conduta aprovados conforme referido no artigo 40.º ou de procedimentos de certificação aprovados conforme referido no artigo 42.º pode ser utilizada como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento.»

7 O artigo 32.º do RGPD, sob a epígrafe «Segurança do tratamento», dispõe:

«1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

a) A pseudonimização e a cifragem dos dados pessoais;

b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;

c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;

d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

2. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

3. O cumprimento de um código de conduta aprovado conforme referido no artigo 40.º ou de um procedimento de certificação aprovado conforme referido no artigo 42.º pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas no n.º 1 do presente artigo.

[…]»

8 O artigo 79.º deste regulamento, sob a epígrafe «Direito à ação judicial contra um responsável pelo tratamento ou um subcontratante», enuncia, no seu n.º 1:

«Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, nomeadamente o direito de apresentar reclamação a uma autoridade de controlo, nos termos do artigo 77.º, todos os titulares de dados têm direito à ação judicial se considerarem ter havido violação dos direitos que lhes assistem nos termos do presente regulamento, na sequência do tratamento dos seus dados pessoais efetuado em violação do referido regulamento.»

9 O artigo 82.º do referido regulamento, sob a epígrafe «Direito de indemnização e responsabilidade», prevê, nos seus n.ºs 1 a 3:

«1. Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos.

2. Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento. […]

3. O responsável pelo tratamento ou o subcontratante fica isento de responsabilidade nos termos do n.º 2, se provar que não é de modo algum responsável pelo evento que deu origem aos danos.»

Litígio no processo principal e questões prejudiciais

10 A NAP é uma autoridade na dependência do ministro das Finanças búlgaro. No âmbito das suas funções, que consistem, nomeadamente, no apuramento, na proteção e na recuperação de créditos públicos, é responsável pelo tratamento de dados pessoais, na aceção do artigo 4.º, ponto 7, do RGPD.

11 Em 15 de julho de 2019, os meios de comunicação social tornaram público que tinha havido um acesso não autorizado ao sistema informático da NAP e que, na sequência desse ataque informático, tinham sido publicados na Internet dados pessoais contidos no referido sistema.

12 Mais de seis milhões de pessoas singulares, de nacionalidade búlgara ou estrangeira, foram afetadas por estes acontecimentos. Algumas centenas de entre elas, entre as quais a recorrente no processo principal, intentaram ações de indemnização por danos imateriais contra a NAP, causados pela divulgação dos seus dados pessoais.

13 Foi neste contexto que a recorrente no processo principal intentou uma ação contra a NAP no Administrativen sad Sofia-grad (Tribunal Administrativo de Sófia, Bulgária) para pagamento de danos no montante de 1 000 levs (BGN) (aproximadamente 510 euros) a título de indemnização, com fundamento no artigo 82.º do RGPD e nas disposições do direito búlgaro. Em apoio deste pedido, alegou ter sofrido danos imateriais resultantes de uma violação de dados pessoais, na aceção do artigo 4.º, ponto 12, do RGPD, mais especificamente uma violação da segurança causada por um incumprimento pela NAP das obrigações que lhe incumbem, nomeadamente por força do artigo 5.º, n.º 1, alínea f), e dos artigos 24.º e 32.º deste regulamento. Os seus danos imateriais consistem no receio de que os seus dados pessoais que foram publicados sem o seu consentimento sejam objeto de utilização abusiva no futuro ou que ela própria sofra chantagem, uma agressão ou mesmo um rapto.

14 Em sua defesa, a NAP alegou, antes de mais, que a recorrente no processo principal não lhe tinha pedido informações sobre os dados precisos que foram divulgados. Em seguida, a NAP apresentou documentos destinados a provar que tinha tomado todas as medidas necessárias, a montante, para prevenir a violação dos dados pessoais contidos no seu sistema informático, bem como, a jusante, para limitar os efeitos dessa violação e para tranquilizar os cidadãos. Além disso, segundo a NAP, não existia um nexo de causalidade entre os danos imateriais alegados e a referida violação. Por último, alegou que, tendo ela própria sofrido um ataque mal-intencionado por parte de pessoas que não eram seus trabalhadores, não podia ser responsabilizada pelas consequências danosas dessa violação.

15 Por Decisão de 27 de novembro de 2020, o Administrativen sad Sofia-grad (Tribunal Administrativo de Sófia) julgou improcedente a ação da recorrente no processo principal. Esse órgão jurisdicional considerou, por um lado, que o acesso não autorizado à base de dados da NAP resultava de pirataria informática cometida por terceiros e, por outro, que a recorrente nos autos principais não havia comprovado uma falha da NAP quanto à adoção de medidas de segurança. Além disso, considerou que esta recorrente não tinha sofrido danos imateriais que conferissem direito a uma indemnização.

16 A recorrente no processo principal interpôs recurso da referida decisão para o Varhoven administrativen sad (Supremo Tribunal Administrativo, Bulgária), que é o órgão jurisdicional de reenvio no presente processo. Em apoio do seu recurso, a recorrente sustenta que o tribunal de primeira instância cometeu um erro de direito na repartição do ónus da prova relativo às medidas de segurança tomadas pela NAP e que esta última não demonstrou a inexistência de falha sua a este respeito. A recorrente no processo principal alega ainda que o receio de possíveis utilizações abusivas dos seus dados pessoais no futuro constitui um dano imaterial real e não hipotético. Em sua defesa, a NAP contesta cada um destes argumentos.

17 O órgão jurisdicional de reenvio considera, antes de mais, a possibilidade de que o facto de ter ocorrido uma violação de dados pessoais pode, por si só, levar à conclusão que as medidas aplicadas pelo responsável pelo tratamento desses dados não eram «adequadas», na aceção dos artigos 24.º e 32.º do RGPD.

18 No entanto, na hipótese de essa constatação ser insuficiente para chegar a essa conclusão, o órgão jurisdicional de reenvio interroga-se, por um lado, sobre o alcance da fiscalização que os juízes nacionais devem efetuar para avaliar a adequação das medidas em causa e, por outro, sobre as regras relativas à administração da prova que devem ser aplicadas nesse âmbito, tanto quanto ao ónus da prova como quanto aos meios de prova, nomeadamente quando esses juízes são chamados a conhecer de uma ação de indemnização baseada no artigo 82.º do referido regulamento.

19 Em seguida, esse órgão jurisdicional pretende saber se, à luz do artigo 82.º, n.º 3, do referido regulamento, o facto de a violação de dados pessoais resultar de um ato praticado por terceiros, neste caso, de um ataque informático, constitui um fator que isenta sistematicamente o responsável pelo tratamento desses dados da sua responsabilidade pelos danos causados à pessoa em causa.

20 Por último, o referido órgão jurisdicional interroga-se sobre se o receio sentido por uma pessoa de que os seus dados pessoais possam ser objeto de utilização abusiva no futuro, no caso em apreço na sequência de um acesso não autorizado a esses dados e da sua divulgação por cibercriminosos, é suscetível, por si só, de constituir «danos […] imateriais», na aceção do artigo 82.º, n.º 1, do RGPD. Em caso afirmativo, essa pessoa estaria dispensada de demonstrar que terceiros fizeram, antes do seu pedido de indemnização, uma utilização ilícita desses dados, tal como uma usurpação da sua identidade.

21 Nestas condições, o Varhoven administrativen sad (Supremo Tribunal Administrativo) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) Devem os artigos 24.º e 32.º do [RGPD] ser interpretados no sentido de que basta que se tenha verificado a divulgação ou o acesso não autorizados a dados pessoais, na aceção do artigo 4.º, ponto 12, do [RGPD], por pessoas que não são funcionários da administração do responsável pelo tratamento e não estão sujeitas ao seu controlo para se considerar que as medidas técnicas e organizativas tomadas não são adequadas?

2) Em caso de resposta negativa à primeira questão, qual deve ser o objeto e o alcance da fiscalização jurisdicional da legalidade ao examinar se as medidas técnicas e organizativas tomadas pelo responsável pelo tratamento são adequadas na aceção do artigo 32.º do [RGPD]?

3) Em caso de resposta negativa à primeira questão, deve o princípio da responsabilidade na aceção do artigo 5.º, n.º 2, [do RGPD,] e do artigo 24.º [deste regulamento], em conjugação com o considerando 74 [deste], ser interpretado no sentido de que, num processo judicial nos termos do artigo 82.º, n.º 1, do [referido regulamento], cabe ao responsável pelo tratamento provar que as medidas técnicas e organizativas tomadas são adequadas na aceção do artigo 32.º do [mesmo]?

Pode um parecer pericial ser considerado um meio de prova necessário e suficiente para comprovar que as medidas técnicas e organizativas tomadas pelo responsável pelo tratamento foram adequadas num [processo] como o presente, em que o acesso não autorizado e a divulgação de dados pessoais são o resultado de um "ataque de *hacker*"?

4) Deve o artigo 82.º, n.º 3, do [RGPD] ser interpretado no sentido de que a divulgação ou o acesso não autorizados a dados pessoais na aceção do artigo 4.º, ponto 12, do [RGPD], como no presente [processo], através de um "ataque de *hacker*" por pessoas que não são funcionários da administração do responsável pelo tratamento e não estão sujeitas ao seu controlo, constitui uma circunstância pela qual o responsável pelo tratamento não é de modo nenhum responsável e que lhe dá o direito de ser isentado de responsabilidade?

5) Deve o artigo 82.º, n.ºs 1 e 2, em conjugação com os considerandos 85 e 146 do [RGPD], ser interpretado no sentido de que, num caso como o presente, em que [se] verificou uma violação da proteção de dados pessoais, sob a forma de acesso não autorizado e de divulgação de dados pessoais através de um «ataque de *hacker*», as preocupações, os receios e as ansiedades do titular dos dados quanto a uma eventual futura utilização abusiva dos dados pessoais, por si só, enquadram se no conceito de dano imaterial, que deve ser interpretado em sentido amplo, e conferem lhe o direito a uma indemnização quando essa utilização abusiva não tenha sido comprovada e/ou quando o titular dos dados não tenha sofrido outros danos?»

Quanto às questões prejudiciais

Quanto à primeira questão

22 Com a sua primeira questão, o órgão jurisdicional de reenvio interroga-se, em substância, sobre a questão de saber se os artigos 24.º e 32.º do RGPD devem ser interpretados no sentido de que uma divulgação ou um acesso não autorizados a dados pessoais por «terceiro[s]», na aceção do artigo 4.º, ponto 10, deste regulamento, são suficientes, por si só, para se considerar que as medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento em causa não eram «adequadas», na aceção dos artigos 24.º e 32.º

23 A título preliminar, há que recordar que, segundo jurisprudência constante, os termos de uma disposição do direito da União que, como os artigos 24.º e 32.º do RGPD, não comportam uma remissão expressa para o direito dos Estados-Membros para determinar o seu sentido e o seu alcance devem normalmente ser objeto, em toda a União, de interpretação autónoma e uniforme, a qual deve, nomeadamente, ser procurada tendo em conta a redação da disposição em causa e o contexto em que se insere [v., neste sentido, Acórdãos de 18 de janeiro de 1984, Ekro, 327/82, EU:C:1984:11, n.º 11; de 1 de outubro de 2019, Planet49, C-673/17, EU:C:2019:801, n.ºs 47 e 48, e de 4 de maio de 2023, Österreichische Post (Dano imaterial relacionado com o tratamento de dados pessoais), C-300/21, EU:C:2023:370, n.º 29].

24 Em primeiro lugar, no que diz respeito à redação das disposições relevantes, há que salientar que o artigo 24.º do RGPD prevê a obrigação geral de o responsável pelo tratamento de dados pessoais aplicar as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que esse tratamento é realizado em conformidade com este regulamento.

25 Para o efeito, este artigo 24.º enumera, no seu n.º 1, alguns critérios a ter em conta para avaliar a adequação dessas medidas, a saber, a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, cuja probabilidade e gravidade varia, para os direitos e liberdades das pessoas singulares. Esta disposição acrescenta que as referidas medidas são revistas e atualizadas consoante as necessidades.

26 Nesta perspetiva, o artigo 32.º do RGPD especifica as obrigações do responsável pelo tratamento e de um eventual subcontratante quanto à segurança desse tratamento. Assim, o n.º 1 deste artigo dispõe que estes últimos devem aplicar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado aos riscos mencionados no número anterior do presente acórdão, tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento em causa.

27 Do mesmo modo, o n.º 2 do referido artigo enuncia que, ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas e à divulgação ou ao acesso não autorizados de dados pessoais.

28 Além disso, tanto o artigo 24.º, n.º 3, como o artigo 32.º, n.º 3, deste regulamento indicam que o responsável pelo tratamento ou o subcontratante pode demonstrar que cumpriu os requisitos dos respetivos n.ºs 1 desses artigos com base no facto de aplicar um código de conduta aprovado ou um procedimento de certificação aprovado, conforme previsto nos artigos 40.º e 42.º do referido regulamento.

29 A referência, que consta no artigo 32.º, n.ºs 1 e 2, do RGPD, a «um nível de segurança adequado ao risco» e a um «nível de segurança adequado» demonstra que este regulamento instaura um regime de gestão dos riscos e que não pretende de modo algum eliminar os riscos de violações de dados pessoais.

30 Assim, resulta da redação dos artigos 24.º e 32.º do RGPD que estas disposições se limitam a impor ao responsável pelo tratamento que adote medidas técnicas e organizativas destinadas a evitar, na medida do possível, qualquer violação dos dados pessoais. A adequação de tais medidas deve ser apreciada de forma concreta, examinando se essas medidas foram aplicadas pelo responsável pelo tratamento tendo em conta os diferentes critérios mencionados nos referidos artigos e as necessidades de proteção de dados especificamente inerentes ao tratamento em causa, bem como os riscos induzidos por este último.

31 Por conseguinte, os artigos 24.º e 32.º do RGPD não podem ser entendidos no sentido de que uma divulgação ou um acesso não autorizados a dados pessoais por um terceiro bastam para concluir que as medidas adotadas pelo responsável pelo tratamento em causa não eram adequadas, na aceção dessas disposições, sem sequer permitir que este último faça prova em contrário.

32 Tal interpretação impõe-se tanto mais quanto o artigo 24.º do RGPD prevê expressamente que o responsável pelo tratamento deve poder demonstrar a conformidade das medidas que aplicou com este regulamento, possibilidade de que ficaria privado se fosse admitida uma presunção inilidível.

33 Em segundo lugar, elementos de ordem contextual e teleológica corroboram esta interpretação dos artigos 24.º e 32.º do RGPD.

34 Por um lado, no que respeita ao contexto em que se inscrevem estes dois artigos, refira-se que resulta do artigo 5.º, n.º 2, do RGPD que o responsável pelo tratamento tem de poder comprovar que respeitou os princípios relativos ao tratamento de dados pessoais enunciados no n.º 1 do referido artigo. Esta obrigação é reproduzida e especificada no artigo 24.º, n.ºs 1 e 3, bem como no artigo 32.º, n.º 3, desse regulamento, quanto à obrigação de aplicação de medidas técnicas e

organizativas para proteger esses dados no tratamento efetuado por esse responsável. Ora, essa obrigação de demonstrar a adequação dessas medidas não teria sentido se o responsável pelo tratamento fosse obrigado a impedir qualquer violação dos referidos dados.

35 Além disso, o considerando 74 do RGPD salienta que é importante que o responsável pelo tratamento deve ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas, que deverão ter em conta os critérios, associados às características do tratamento em causa e ao risco por ele apresentado, que estão igualmente enunciados nos seus artigos 24.º e 32.º

36 Do mesmo modo, segundo o considerando 76 deste regulamento, a probabilidade e a gravidade dos riscos dependem das especificidades do tratamento em causa, devendo esses riscos ser aferidos com base numa avaliação objetiva.

37 Por outro lado, decorre do artigo 82.º, n.ºs 2 e 3, do RGPD que, embora um responsável pelo tratamento seja responsável pelos danos causados por um tratamento que viole o presente regulamento, fica, no entanto, isento de responsabilidade se provar que não é de modo algum responsável pelo evento que deu origem aos danos.

38 Por outro lado, a interpretação desenvolvida no n.º 31 do presente acórdão é também corroborada no considerando 83 do RGPD, que enuncia, no seu primeiro parágrafo, que, «[a] fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem». Ao fazê-lo, o legislador da União manifestou a sua intenção de «atenu[ar]» os riscos de violação dos dados pessoais, sem alegar que seria possível eliminá-los.

39 Tendo em conta os fundamentos que precedem, há que responder à primeira questão que os artigos 24.º e 32.º do RGPD devem ser interpretados no sentido de que uma divulgação ou um acesso não autorizados a dados pessoais por «terceiro[s]», na aceção do artigo 4.º, ponto 10, deste regulamento, não são suficientes, por si só, para se considerar que as medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento em causa não eram «adequadas», na aceção dos artigos 24.º e 32.º

Quanto à segunda questão

40 Com a sua segunda questão, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 32.º do RGPD deve ser interpretado no sentido de que a adequação das medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento, nos termos desse artigo, deve ser avaliada pelos órgãos jurisdicionais nacionais de forma concreta, tendo nomeadamente em conta os riscos associados ao tratamento em causa.

41 A este respeito, há que recordar que, como foi sublinhado no âmbito da resposta à primeira questão, o artigo 32.º do RGPD exige que o responsável pelo tratamento e o subcontratante, consoante os casos, apliquem as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, tendo em conta os critérios de apreciação enunciados no seu n.º 1. Além disso, o n.º 2 deste artigo enumera, de forma não taxativa, alguns fatores relevantes para avaliar o nível de segurança adequado à luz dos riscos que o tratamento em causa representa.

42 Resulta do referido artigo 32.º, n.ºs 1 e 2, que a adequação de tais medidas técnicas e organizativas deve ser apreciada em duas fases. Por um lado, há que identificar os riscos de violação dos dados pessoais causados pelo tratamento em causa e as suas eventuais consequências para os direitos e liberdades das pessoas singulares. Esta avaliação deve ser conduzida de forma concreta, tomando em consideração a probabilidade dos riscos identificados e a sua gravidade. Por outro lado, há que verificar se as medidas aplicadas pelo responsável pelo tratamento são adequadas a esses riscos, tendo em conta as técnicas mais avançadas, os custos de aplicação, bem como a natureza, o âmbito, o contexto e as finalidades desse tratamento.

43 É certo que o responsável pelo tratamento dispõe de uma certa margem de apreciação para determinar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, como exige o artigo 32.º, n.º 1, do RGPD. Não deixa de ser verdade que um tribunal nacional deve poder avaliar a apreciação complexa feita pelo responsável pelo tratamento e, ao fazê-lo, garantir que as medidas adotadas por este último são adequadas para assegurar esse nível de segurança.

44 Tal interpretação é, aliás, suscetível de garantir, por um lado, a efetividade da proteção dos dados pessoais que os considerandos 11 e 74 deste regulamento evidenciam e, por outro, o direito a uma ação judicial efetiva contra um responsável pelo tratamento, conforme protegido pelo artigo 79.º, n.º 1, do referido regulamento, lido em conjugação com o considerando 4 do mesmo.

45 Por conseguinte, para fiscalizar a adequação de medidas técnicas e organizativas aplicadas ao abrigo do artigo 32.º do RGPD, um tribunal nacional não se deve limitar a verificar de que modo o responsável pelo tratamento em causa pretendeu cumprir as obrigações que lhe incumbem por força deste artigo, mas sim proceder a um exame de mérito dessas medidas, à luz de todos os critérios mencionados no referido artigo, bem como das circunstâncias próprias do caso concreto e dos elementos de prova de que esse tribunal dispõe a esse respeito.

46 Esse exame exige que se proceda a uma análise concreta simultaneamente da natureza e do teor das medidas implementadas pelo responsável pelo tratamento, da forma como essas medidas foram aplicadas e dos seus efeitos práticos no nível de segurança que este era obrigado a assegurar, tendo em conta os riscos inerentes a esse tratamento.

47 Por conseguinte, há que responder à segunda questão que o artigo 32.º do RGPD deve ser interpretado no sentido de que a adequação das medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento nos termos deste artigo deve ser apreciada pelos órgãos jurisdicionais nacionais de forma concreta, tendo em conta os riscos associados ao tratamento em causa e apreciando se a natureza, o teor e a aplicação dessas medidas são adequados a esses riscos.

Quanto à terceira questão

Quanto à primeira parte da terceira questão

48 Com a primeira parte da sua terceira questão, o órgão jurisdicional de reenvio pergunta, em substância, se o princípio da responsabilidade do responsável pelo tratamento, enunciado no artigo 5.º, n.º 2, do RGPD e concretizado no artigo 24.º deste, deve ser interpretado no sentido de

que, no âmbito de uma ação de indemnização ao abrigo do artigo 82.º deste regulamento, o responsável pelo tratamento em causa suporta o ónus de provar a adequação das medidas de segurança que aplicou ao abrigo do artigo 32.º do referido regulamento.

49 A este respeito, importa, em primeiro lugar, recordar que o artigo 5.º, n.º 2, do RGPD estabelece um princípio de responsabilidade, por força do qual o responsável pelo tratamento é responsável pelo cumprimento dos princípios relativos ao tratamento de dados pessoais estabelecidos no n.º 1 deste artigo, e prevê que o referido responsável deve poder comprovar que esses princípios são respeitados.

50 Em especial, o responsável pelo tratamento deve, em conformidade com o princípio da integridade e da confidencialidade dos dados pessoais enunciado no artigo 5.º, n.º 1, alínea f), deste regulamento, assegurar que esses dados sejam tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas, e deve poder comprovar que esse princípio é respeitado.

51 Refira-se ainda que tanto o artigo 24.º, n.º 1, do RGPD, à luz do seu considerando 74, como o artigo 32.º, n.º 1, deste regulamento impõem ao responsável pelo tratamento, relativamente a qualquer tratamento de dados pessoais efetuado por ele próprio ou por sua conta, que aplique as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o referido regulamento.

52 Resulta inequivocamente da redação do artigo 5.º, n.º 2, do artigo 24.º, n.º 1, e do artigo 32.º, n.º 1, do RGPD que o ónus de provar que os dados pessoais são tratados de uma forma que garanta a sua segurança, na aceção do artigo 5.º, n.º 1, alínea f), e do artigo 32.º deste regulamento, incumbe ao responsável pelo tratamento em causa [v., por analogia, Acórdãos de 4 de maio de 2023, Bundesrepublik Deutschland (Caixa de correio eletrónico dos tribunais), C-60/22, EU:C:2023:373, n.ºs 52 e 53, e de 4 de julho de 2023, Meta Platforms e o. (Condições gerais de utilização de uma rede social), C-252/21, EU:C:2023:537, n.º 95].

53 Estes três artigos enunciam assim uma regra, de aplicação geral, que, na falta de indicação em contrário no RGPD, há que aplicar igualmente no âmbito de uma ação de indemnização com base no artigo 82.º deste regulamento.

54 Em segundo lugar, há que verificar que esta interpretação literal é corroborada pela consideração dos objetivos prosseguidos pelo RGPD.

55 Por um lado, uma vez que o nível de proteção visado pelo RGPD depende das medidas de segurança adotadas pelos responsáveis pelo tratamento de dados pessoais, estes devem ser incentivados a fazer tudo o que estiver ao seu alcance para evitar a ocorrência de operações de tratamento não conformes com o presente regulamento, cabendo-lhes o ónus de demonstrar a adequação dessas medidas.

56 Por outro lado, se viesse a considerar-se que o ónus da prova relativo à adequação das referidas medidas recai sobre os titulares dos dados, conforme definidos no artigo 4.º, ponto 1, do RGPD, daí resultaria que o direito a indemnização previsto no seu artigo 82.º, n.º 1, ficaria privado de uma parte importante do seu efeito útil, apesar de o legislador da União ter pretendido reforçar simultaneamente os direitos desses titulares e as obrigações dos responsáveis pelo tratamento, em relação às disposições anteriores a este regulamento, como indica o seu considerando 11.

57 Por conseguinte, há que responder à primeira parte da terceira questão que o princípio da responsabilidade do responsável pelo tratamento, enunciado no artigo 5.º, n.º 2, do RGPD e concretizado no artigo 24.º deste, deve ser interpretado no sentido de que, no âmbito de uma ação de indemnização intentada ao abrigo do artigo 82.º deste regulamento, o responsável pelo tratamento em causa suporta o ónus de provar a adequação das medidas de segurança que aplicou ao abrigo do artigo 32.º do referido regulamento.

Quanto à segunda parte da terceira questão

58 Com a segunda parte da sua terceira questão, o órgão jurisdicional de reenvio pretende saber, em substância, se o artigo 32.º do RGPD e o princípio da efetividade do direito da União devem ser interpretados no sentido de que, para apreciar a adequação das medidas de segurança que o responsável pelo tratamento aplicou nos termos deste artigo, uma peritagem judicial constitui um meio de prova necessário e suficiente.

59 A este respeito, importa recordar que, em conformidade com jurisprudência constante, na falta de regras da União na matéria, cabe ao ordenamento jurídico interno de cada Estado-Membro instituir as normas processuais das ações judiciais destinadas a garantir a salvaguarda dos direitos dos particulares, ao abrigo do princípio da autonomia processual, desde que, no entanto, essas regras não sejam, nas situações abrangidas pelo direito da União, menos favoráveis do que as que regulam situações semelhantes submetidas ao direito interno (princípio da equivalência) e não tornem impossível, na prática, ou excessivamente difícil o exercício dos direitos conferidos pelo direito da União (princípio da efetividade) [Acórdão de 4 de maio de 2023, Österreichische Post (Dano imaterial relacionado com o tratamento de dados pessoais), C-300/21, EU:C:2023:370, n.º 53 e jurisprudência referida].

60 No caso, refira-se que o RGPD não enuncia regras relativas à admissão e ao valor probatório de um meio de prova, como uma peritagem judicial, que devem ser aplicadas pelos juízes nacionais chamados a pronunciar-se sobre uma ação de indemnização baseada no artigo 82.º deste regulamento e encarregados de apreciar, à luz do seu artigo 32.º, a adequação das medidas de segurança que o responsável pelo tratamento em causa aplicou. Por conseguinte, em conformidade com o que foi recordado no número anterior do presente acórdão e na falta de regras do direito da União na matéria, cabe ao ordenamento jurídico interno de cada Estado-Membro fixar as modalidades das ações destinadas a garantir a salvaguarda dos direitos conferidos aos sujeitos de direito por esse artigo 82.º, em especial, os critérios relativos aos meios de prova que permitem avaliar a adequação dessas medidas neste contexto, sem prejuízo do respeito dos referidos princípios da equivalência e da efetividade [v., por analogia, Acórdão de 21 de junho de 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, n.º 297, e de 4 de maio de 2023, Österreichische Post (Dano imaterial relacionado com o tratamento de dados pessoais), C-300/21, EU:C:2023:370, n.º 54].

61 No presente processo, o Tribunal de Justiça não dispõe de nenhum elemento suscetível de suscitar dúvidas quanto ao respeito pelo princípio da equivalência. A situação é diferente no que respeita à conformidade com o princípio da efetividade, uma vez que a própria redação da segunda parte da terceira questão apresenta o recurso a uma peritagem judicial como um «meio de prova necessário e suficiente».

62 Em especial, uma regra processual nacional por força da qual fosse sistematicamente «necessário» que os órgãos jurisdicionais nacionais ordenassem uma perícia judicial seria suscetível de colidir com o princípio da efetividade. Com efeito, o recurso sistemático a essa peritagem pode

revelar-se supérfluo à luz das outras provas detidas pelo órgão jurisdicional chamado a decidir, nomeadamente, como indica o Governo Búlgaro nas suas observações escritas, atendendo aos resultados de uma fiscalização do respeito das medidas de proteção dos dados pessoais que foi efetuada por uma autoridade independente e estabelecida por lei, desde que essa fiscalização seja recente, uma vez que as referidas medidas devem, em conformidade com o artigo 24.º, n.º 1, do RGPD, ser revistas e atualizadas consoante as necessidades.

63 Além disso, como salientou a Comissão Europeia nas suas observações escritas, o princípio da efetividade poderia ser violado se o termo «suficiente» viesse a ser entendido no sentido de que um órgão jurisdicional nacional deve deduzir exclusiva ou automaticamente de um relatório de peritagem judicial que as medidas de segurança aplicadas pelo responsável pelo tratamento em causa são «adequadas», na aceção do artigo 32.º do RGPD. Ora, a salvaguarda dos direitos conferidos por este regulamento, pretendida pelo referido princípio da efetividade, e especialmente o direito à ação judicial contra um responsável pelo tratamento, que é garantido pelo artigo 79.º, n.º 1, deste regulamento, exigem que um tribunal imparcial proceda a uma apreciação objetiva da adequação das medidas em causa, em vez de se limitar a essa dedução (v., neste sentido, Acórdão de 12 de janeiro de 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, EU:C:2023:2, n.º 50).

64 Tendo em conta os fundamentos que precedem, há que responder à segunda parte da terceira questão que o artigo 32.º do RGPD e o princípio da efetividade do direito da União devem ser interpretados no sentido de que, para apreciar a adequação das medidas de segurança que o responsável pelo tratamento aplicou nos termos deste artigo, uma peritagem judicial não pode constituir um meio de prova sistematicamente necessário e suficiente.

Quanto à quarta questão

65 Com a sua quarta questão, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 82.º, n.º 3, do RGPD deve ser interpretado no sentido de que o responsável pelo tratamento fica isento da sua obrigação de reparar o dano sofrido por uma pessoa, nos termos do artigo 82.º, n.ºs 1 e 2, deste regulamento, pelo simples facto de esse dano resultar de uma divulgação ou acesso não autorizados a dados pessoais por «terceiro[s]», na aceção do artigo 4.º, ponto 10, do referido regulamento.

66 A título preliminar, importa especificar que decorre do artigo 4.º, ponto 10, do RGPD que têm a qualidade de «terceiro[s]», nomeadamente, as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais. Esta definição abrange pessoas que não são funcionários do responsável pelo tratamento e que não estão sob o controlo deste, como as referidas na questão submetida.

67 Em seguida, há que recordar, em primeiro lugar, que o artigo 82.º, n.º 2, do RGPD dispõe que «[q]ualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole [este] regulamento» e que o n.º 3 deste artigo prevê que o responsável pelo tratamento ou um subcontratante, consoante o caso, fica isento dessa responsabilidade «se provar que não é de modo algum responsável pelo evento que deu origem aos dano».

68 Além disso, o considerando 146 do RGPD, que se refere especificamente ao seu artigo 82.º, enuncia, na sua primeira e segunda frases, que «[o] responsável pelo tratamento ou o subcontratante deverão reparar quaisquer danos de que alguém possa ser vítima em virtude de um tratamento que viole o presente regulament[o]» e «pode ser exonerado da responsabilidade se provar que o facto que causou o dano não lhe é de modo algum imputável».

69 Resulta destas disposições, por um lado, que o responsável pelo tratamento em causa deve, em princípio, reparar um dano causado por uma violação deste regulamento relacionada com esse tratamento e, por outro, que só pode ficar isento da sua responsabilidade se provar que não é de modo algum responsável pelo evento que deu origem aos danos.

70 Assim, como revela o aditamento expresso do advérbio «não» durante o processo legislativo, as circunstâncias em que o responsável pelo tratamento pode invocar o direito a ficar isento da responsabilidade civil em que incorre nos termos do artigo 82.º do RGPD devem ser estritamente limitadas àquelas em que esse responsável pode comprovar a inexistência de imputabilidade do dano por sua própria iniciativa.

71 Quando, como no caso em apreço, uma violação de dados pessoais, na aceção do artigo 4.º, ponto 12, do RGPD, tiver sido cometida por cibercriminosos, e, portanto, por «terceiro[s]», na aceção do artigo 4.º, ponto 10, deste regulamento, essa violação não pode ser imputada ao responsável pelo tratamento, salvo se este tiver possibilitado a referida violação ao incumprir uma obrigação prevista no RGPD, nomeadamente a obrigação de proteção dos dados a que está obrigado por força do artigo 5.º, n.º 1, alínea f), e dos artigos 24.º e 32.º do mesmo regulamento.

72 Assim, no caso de uma violação de dados pessoais cometida por um terceiro, o responsável pelo tratamento pode ficar isento de responsabilidade, com base no artigo 82.º, n.º 3, do RGPD, provando que não existe um nexo de causalidade entre qualquer violação da sua obrigação de proteção de dados e o dano sofrido pelo indivíduo.

73 Em segundo lugar, a interpretação anterior deste artigo 82.º, n.º 3, é igualmente conforme com o objetivo do RGPD, que consiste em assegurar um elevado nível de proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais, enunciado nos considerandos 10 e 11 deste regulamento.

74 Tendo em conta todas estas considerações, há que responder à quarta questão que o artigo 82.º, n.º 3, do RGPD deve ser interpretado no sentido de que o responsável pelo tratamento não pode ficar isento da sua obrigação de reparar o dano sofrido por uma pessoa, nos termos do artigo 82.º, n.ºs 1 e 2, deste regulamento, pelo simples facto de esse dano resultar de uma divulgação ou acesso não autorizados a dados pessoais por «terceiro[s]», na aceção do artigo 4.º, ponto 10, do referido regulamento, devendo então o referido responsável provar que não é de modo nenhum responsável pelo evento que deu origem aos danos.

Quanto à quinta questão

75 Com a sua quinta questão, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 82.º, n.º 1, do RGPD deve ser interpretado no sentido de que o receio que um titular dos dados sinta de uma eventual utilização abusiva dos seus dados pessoais por terceiros, na sequência de uma violação deste regulamento é suscetível, por si só, de constituir «danos […] imateriais», na aceção dessa disposição.

76 No que respeita, em primeiro lugar, à redação do artigo 82.º, n.º 1, do RGPD, há que observar que este prevê que «[q]ualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos».

77 A este respeito, o Tribunal de Justiça salientou que resulta claramente da redação do artigo 82.º, n.º 1, do RGPD que a existência de um «dano» ou de um «[prejuízo]» que foi «sofrido» constitui um dos pressupostos do direito de indemnização previsto na referida disposição, tal como a existência de uma violação deste regulamento e de um nexo de causalidade entre esse dano e essa violação, sendo cumulativos esses três pressupostos [Acórdão de 4 de maio de 2023, Österreichische Post (Dano imaterial relacionado com o tratamento de dados pessoais), C-300/21, EU:C:2023:370, n.º 32].

78 Por outro lado, baseando-se em considerações de ordem simultaneamente literal, sistémica e teleológica, o Tribunal de Justiça interpretou o artigo 82.º, n.º 1, do RGPD no sentido de que se opõe a uma norma ou a uma prática nacional que subordina a indemnização de «danos […] imateriais», na aceção desta disposição, à condição de os danos sofridos pelo titular dos dados atingirem um certo grau de gravidade. [Acórdão de 4 de maio de 2023, Österreichische Post (Dano imaterial relacionado com o tratamento de dados pessoais), C-300/21, EU:C:2023:370, n.º 51].

79 Relembrada esta jurisprudência, importa sublinhar, no caso em apreço, que o artigo 82.º, n.º 1, do RGPD não distingue as situações em que, na sequência de uma violação comprovada de disposições deste regulamento, os «danos […] imateriais» alegados pelo titular dos dados, por um lado, estão ligados a uma utilização abusiva dos seus dados pessoais por terceiros que já se produziu, à data do seu pedido de indemnização, ou, por outro, está ligado ao medo sentido por essa pessoa de que essa utilização possa ocorrer no futuro.

80 Por conseguinte, a redação do artigo 82.º, n.º 1, do RGPD não exclui que o conceito de «danos […] imateriais» que consta dessa disposição abranja uma situação, como a referida pelo órgão jurisdicional de reenvio, em que o titular dos dados invoca, com vista a obter uma indemnização com fundamento nesta disposição, o seu receio de que os seus dados pessoais sejam objeto de uma futura utilização abusiva por terceiros, em resultado de qualquer infração ao presente regulamento.

81 Esta interpretação literal é corroborada, em segundo lugar, pelo considerando 146 do RGPD, que tem especificamente por objeto o direito de indemnização previsto no seu artigo 82.º, n.º 1, e que menciona, no terceiro período, que «[o] conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos» deste regulamento. Ora, uma interpretação do conceito de «danos […] imateriais», na aceção deste artigo 82.º, n.º 1, que não inclua as situações em que a pessoa afetada por uma violação deste regulamento invoca o receio de que os seus próprios dados pessoais possam ser utilizados de forma abusiva no futuro não corresponderia a um entendimento amplo deste conceito, como pretendido pelo legislador da União [v., por analogia, Acórdão de 4 de maio de 2023, Österreichische Post (Dano imaterial relacionado com o tratamento de dados pessoais), C-300/21, EU:C:2023:370, n.ºs 37 e 46].

82 Por outro lado, o considerando 85, primeiro período, do RGPD refere que «[s]e não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados

pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeira, […] ou qualquer outra desvantagem económica ou social significativa». Resulta desta lista exemplificativa dos «danos» suscetíveis de ser sofridos pelas pessoas em causa que o legislador da União pretendeu incluir nestes conceitos, em especial, a simples «perda de controlo» sobre os seus próprios dados, na sequência de uma violação deste regulamento, ainda que não tenha havido uma utilização efetivamente abusiva dos dados em causa em detrimento das referidas pessoas.

83 Em terceiro e último lugar, a interpretação que figura no n.º 80 do presente acórdão é corroborada pelos objetivos do RGPD, que importa ter plenamente em conta para definir o conceito de «dano», como indica o considerando 146, terceiro período, deste regulamento. Ora, uma interpretação do artigo 82.º, n.º 1, do RGPD segundo a qual o conceito de «danos […] imateriais», na aceção desta disposição, não inclui as situações em que um titular dos dados invoca unicamente o seu receio de que os seus dados sejam objeto de uma utilização abusiva por terceiros, no futuro, não é conforme com a garantia de um elevado nível de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais na União, que é visada por esse instrumento.

84 No entanto, importa sublinhar que um titular dos dados, afetado negativamente pela violação do RGPD, tem de provar que essas consequências são constitutivas de danos imateriais, na aceção do artigo 82.º deste regulamento [v., neste sentido, Acórdão de 4 de maio de 2023, Österreichische Post (Dano imaterial relacionado com o tratamento de dados pessoais), C-300/21, EU:C:2023:370, n.º 50].

85 Em especial, quando uma pessoa que pede uma indemnização com esse fundamento invoca o receio de uma utilização abusiva dos seus dados pessoais no futuro devido à existência dessa violação, o tribunal nacional da causa deve verificar se esse receio pode ser considerado fundado, nas circunstâncias específicas em causa e em relação à pessoa em questão.

86 Tendo estas considerações em conta, há que responder à quinta questão que o artigo 82.º, n.º 1, do RGPD deve ser interpretado no sentido de que o receio que um titular dos dados sinta de uma eventual utilização abusiva dos seus dados pessoais por terceiros, na sequência de uma violação deste regulamento é suscetível, por si só, de constituir «danos […] imateriais», na aceção desta disposição.

Quanto às despesas

87 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:

1) Os artigos 24.º e 32.º, do 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados),

devem ser interpretados no sentido de que:

uma divulgação ou um acesso não autorizados a dados pessoais por «terceiro[s]», na aceção do artigo 4.º, ponto 10, deste regulamento, não são suficientes, por si só, para se considerar que as medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento em causa não eram «adequadas», na aceção dos artigos 24.º e 32.º

2) **O artigo 32.º do Regulamento 2016/679**

deve ser interpretado no sentido de que:

a adequação das medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento nos termos deste artigo deve ser apreciada pelos órgãos jurisdicionais nacionais de forma concreta, tendo em conta os riscos associados ao tratamento em causa e apreciando se a natureza, o teor e a aplicação dessas medidas são adequados a esses riscos.

3) **O princípio da responsabilidade do responsável pelo tratamento, enunciado no artigo 5.º, n.º 2, do Regulamento 2016/679 e concretizado no seu artigo 24.º,**

deve ser interpretado no sentido de que:

no âmbito de uma ação de indemnização intentada ao abrigo do artigo 82.º deste regulamento, o responsável pelo tratamento em causa suporta o ónus de provar a adequação das medidas de segurança que aplicou ao abrigo do artigo 32.º do referido regulamento.

4) **O artigo 32.º do Regulamento 2016/679 e o princípio da efetividade do direito da União**

devem ser interpretados no sentido de que:

para apreciar a adequação das medidas de segurança que o responsável pelo tratamento aplicou nos termos deste artigo, uma peritagem judicial não pode constituir um meio de prova sistematicamente necessário e suficiente.

5) **O artigo 82.º, n.º 3, do Regulamento 2016/679**

deve ser interpretado no sentido de que:

o responsável pelo tratamento não pode ficar isento da sua obrigação de reparar o dano sofrido por uma pessoa, nos termos do artigo 82.º, n.ºs 1 e 2, deste regulamento, pelo simples facto de esse dano resultar de uma divulgação ou acesso não autorizados a dados pessoais por «terceiro[s]», na aceção do artigo 4.º, ponto 10, do referido regulamento, devendo então o referido responsável provar que não é de modo nenhum responsável pelo evento que deu origem aos danos.

6) **O artigo 82.º, n.º 1, do Regulamento 2016/679**

deve ser interpretado no sentido de que:

o receio que um titular dos dados sinta de uma eventual utilização abusiva dos seus dados pessoais por terceiros, na sequência de uma violação deste regulamento é suscetível, por si só, de constituir «danos [...] imateriais», na aceção desta disposição.

Assinaturas