Coletânea da Jurisprudência

CONCLUSÕES DO ADVOGADO-GERAL
GIOVANNI PITRUZZELLA
apresentadas em 27 de abril de 2023 [1]

Processo C-340/21

VB
contra
Natsionalna agentsia za prihodite

[pedido de decisão prejudicial apresentado pelo Varhoven administrativen sad (Supremo Tribunal Administrativo, Bulgária)]

«Reenvio prejudicial — Proteção de dados pessoais — Regulamento (UE) 2016/679 — Responsabilidade do responsável pelo tratamento — Segurança do tratamento — Violação da segurança do tratamento de dados pessoais — Danos morais sofridos devido à inércia do responsável pelo tratamento — Ação de indemnização»

Pode a difusão ilícita, devida a um ataque pirata, de dados pessoais na posse de uma agência pública dar lugar a uma indemnização por danos morais a um titular dos dados pelo simples facto de este último recear uma eventual e futura utilização abusiva dos seus dados? Quais são os critérios de imputabilidade da responsabilidade ao responsável pelo tratamento? Como se reparte o ónus da prova no processo? Qual o âmbito da fiscalização do órgão jurisdicional?

I. Quadro jurídico

1. O artigo 4.º do Regulamento 2016/679 [2] (a seguir «regulamento»), sob a epígrafe «Definições», dispõe:

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

[…]

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

[…]»

[1] Língua original: italiano.

[2] 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).

2. O artigo 5.º, sob a epígrafe «Princípios relativos ao tratamento de dados pessoais», enuncia:

«1. Os dados pessoais são:

[…]

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").»

3. O artigo 24.º do mesmo regulamento, sob a epígrafe «Responsabilidade do responsável pelo tratamento», estabelece:

«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.»

4. O artigo 32.º, sob a epígrafe «Segurança do tratamento», prevê:

«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:

[…]

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.

[…]»

5. O artigo 82.º do mesmo regulamento, sob a epígrafe «Direito de indemnização e responsabilidade», dispõe:

«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.»

II. Matéria de facto, processo principal e questões prejudiciais

6. Em 15 de julho de 2019, os meios de comunicação social búlgaros noticiaram que se verificou um acesso não autorizado ao sistema de informação da Natsionalna agentsia za prihodite (Agência Nacional de Receitas Fiscais, a seguir «NAP» [3]) e que diversas informações fiscais e da segurança social de milhões de pessoas, tanto nacionais como estrangeiras, tinham sido publicadas na Internet.

7. Várias pessoas, entre as quais V.B., recorrente no processo principal, intentaram então uma ação judicial contra a NAP para obter uma indemnização por danos morais.

8. No processo em apreço, a recorrente no processo principal recorreu para o Administratibven sad Sofia-grad (Tribunal Administrativo de Sófia, Bulgária, a seguir «ASSG»), alegando que a NAP violou as normas nacionais, bem como a obrigação de tratamento dos dados pessoais, na qualidade de responsável pelo tratamento, para «garantir níveis de segurança adequados» através da adoção de medidas técnicas e organizativas apropriadas, em conformidade com os artigos 24.º e 32.º do Regulamento n.º 679/2016. Em seguida, a recorrente afirmou ter sofrido danos morais, sob a forma de preocupações e receios de uma futura utilização abusiva dos seus dados pessoais.

9. Em contrapartida, a parte recorrida sublinhou que não recebeu nenhum pedido da recorrente no processo principal com indicação dos dados pessoais que foram exatamente objeto de acesso. Além disso, indica que, depois de ter conhecimento da intrusão, convocou reuniões com peritos para proteger os direitos e os interesses dos cidadãos. Segundo a NAP, também não existe um nexo de causalidade entre o ataque informático e o dano alegadamente invocado, uma vez que a agência implementou todos os sistemas de gestão dos processos e da segurança das informações, em conformidade com as normas internacionais em vigor na matéria.

[3] A NAP é responsável pelo tratamento na aceção do artigo 4.º, ponto 7, do Regulamento. Nos termos do direito nacional, é um organismo administrativo dotado de uma competência específica, na dependência do Ministro das Finanças, e encarregado do apuramento, da salvaguarda e da cobrança das finanças, bem como do apuramento, da salvaguarda e da cobrança de créditos do Estado, públicos e privados determinados pela lei. No exercício dos poderes públicos de que está investida, trata dos dados pessoais.

10. O órgão jurisdicional de primeira instância, o ASSG, julgou a ação improcedente, considerando que a difusão dos dados não era imputável à Agência, que o ónus da prova da adequação das medidas adotadas cabia à recorrente e, por último, que não existia nenhum dano moral indemnizável.

11. A sentença de primeira instância foi posteriormente objeto de recurso perante o Varhoven administrativen sad (Supremo Tribunal Administrativo, Bulgária). Entre as observações formuladas, a recorrente no processo principal sublinhou que o órgão jurisdicional de primeira instância cometeu um erro na repartição do ónus da prova da não adoção das medidas de segurança. O dano moral também não deve ser objeto de prova a apresentar, uma vez que se trata de um dano efetivo e não meramente potencial.

12. A NAP, por seu turno, reiterou que tomou as medidas técnicas e organizativas necessárias na qualidade de responsável pelo tratamento e contestou a existência da prova de um dano moral efetivo. Com efeito, a ansiedade e os receios não são estados emocionais indemnizáveis.

13. O órgão jurisdicional de reenvio constatou que as ações intentadas pelas pessoas lesadas contra a NAP destinadas a obter a indemnização pelos danos morais tiveram resultados distintos.

14. Nestas condições, o órgão jurisdicional de reenvio suspendeu a instância e submeteu ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) Devem os artigos 24.º e 32.º do Regulamento (UE) 2016/679 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 Regulamento (UE) 2016/679, 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 Regulamento (UE) 2016/679?

3) Em caso de resposta negativa à primeira questão, deve o princípio da responsabilidade na aceção do artigo 5.º, n.º 2, e do artigo 24.º, em conjugação com o considerando 74 do Regulamento (UE) 2016/679, ser interpretado no sentido de que, num processo judicial nos termos do artigo 82.º, n.º 1, do Regulamento (UE) 2016/679, cabe ao responsável pelo tratamento provar que as medidas técnicas e organizativas tomadas são adequadas na aceção do artigo 32.º do Regulamento? 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 Regulamento (UE) 2016/679 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 Regulamento (UE) 2016/679, 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 Regulamento (UE) 2016/679, ser interpretado no sentido de que, num processo 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?»

III. Análise jurídica

A. Observações preliminares

15. O presente processo tem por objeto questões interessantes e, em parte, inéditas relativas à interpretação de várias disposições do regulamento [4].

16. As cinco questões prejudiciais andam à volta da mesma questão: as condições em que pode ser concedida uma indemnização por danos morais a uma pessoa cujos dados pessoais, na posse de uma agência pública, foram objeto de publicação na Internet na sequência de um ataque de *hackers*.

17. Por comodidade de exposição, proporei respostas sucintas separadas a todas as questões prejudiciais do despacho de reenvio, apesar de estar consciente de algumas sobreposições conceptuais, uma vez que as quatro primeiras questões se destinam a identificar os pressupostos da imputabilidade da violação das disposições do regulamento ao responsável pelo tratamento dos dados [5] e a quinta diz mais precisamente respeito ao conceito de dano moral para efeitos da indemnização [6].

18. Assinalo que estão atualmente pendentes no Tribunal de Justiça diversos processos relativos ao artigo 82.º do regulamento e que, num deles, já foram lidas as Conclusões do advogado-geral, que terei em conta no âmbito da presente análise [7].

[4] Artigo 5.º, n.º 2 (relativo ao princípio da responsabilidade de qualquer responsável pelo tratamento de dados pessoais), artigo 24.º (relativo às medidas que o responsável pelo tratamento é obrigado a aplicar para garantir que o seu tratamento está em conformidade com este regulamento), artigo 32.º (relativo a essa obrigação especificamente no que diz respeito à segurança do tratamento) e artigo 82.º, n.os 1 a 3 (relativo à indemnização dos danos resultantes da violação deste regulamento e à possibilidade de o responsável pelo tratamento tomar medidas para garantir o cumprimento deste regulamento), além dos considerandos 74, 85 e 146 que estão relacionados com os referidos artigos.

[5] a) a primeira pretende responder à questão de saber se da mera violação dos sistemas se pode deduzir a inadequação das medidas aplicadas; b) a segunda diz respeito ao alcance da fiscalização jurisdicional do caráter adequado das referidas medidas; c) a terceira refere-se ao ónus da prova da própria adequação e a algumas modalidades técnicas para a obtenção da prova; d) a quarta é relativa à importância do facto de o ataque ao sistema provir do exterior para feitos da isenção da responsabilidade.

[6] No que diz respeito às disposições do regulamento referidas, as três primeiras questões dizem respeito aos aspetos da responsabilidade do responsável pelo tratamento no que respeita à adequação das medidas a tomar (artigos 5.º, 24.º e 32.º), a quarta e a quinta, às condições de isenção da responsabilidade e ao conceito de dano moral indemnizável (artigo 82.º).

[7] V. Conclusões do advogado-geral M. Campos Sánchez-Bordona no processo Österreichische Post (Danos morais associados ao tratamento de dados pessoais) (C-300/21, EU:C:2022:756).

19. Antes de examinar as questões submetidas, considero oportuno formular algumas considerações preliminares sobre princípios e finalidades do regulamento, que serão úteis para a resolução de cada uma das questões prejudiciais.

20. O artigo 24.º do regulamento estabelece, em termos gerais, a obrigação, para o responsável pelo tratamento, de aplicar as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento de dados pessoais é realizado em conformidade com o próprio regulamento, enquanto o artigo 32.º estabelece mais especificamente a mesma obrigação no que diz respeito à segurança do tratamento. Os artigos 24.º e 32.º estabelecem de forma mais detalhada o previsto no artigo 5.º, n.º 2, que introduz, precisamente entre os «princípios relativos ao tratamento de dados pessoais», o «princípio da responsabilidade». Este princípio segue lógica e complementarmente o «princípio da integridade e confidencialidade» previsto no artigo 5.º, n.º 1, alínea f), e ambos devem ser lidos à luz da abordagem que assenta no risco em que se baseia o regulamento.

21. O princípio da responsabilidade é um dos pilares do regulamento e uma das suas inovações mais significativas. Atribui ao responsável pelo tratamento a responsabilidade de adotar medidas pró-ativas para garantir o cumprimento do regulamento e estar preparado para a comprovar [8].

22. Na doutrina, fala-se de uma verdadeira mudança cultural como efeito do «alcance global da obrigação de responsabilidade» [9]. Não é tanto o cumprimento formal da obrigação legal ou da medida pontual, mas a estratégia empresarial global adotada que isenta o responsável pelo tratamento da responsabilidade, enquanto *compliant* [em conformidade] da disciplina da proteção de dados.

23. As medidas técnicas e organizativas exigidas pelo princípio da responsabilidade devem ser «adequadas», tendo em conta os fatores especificados no artigo 24.º: a natureza, o âmbito de aplicação, o contexto e as finalidades do tratamento dos dados, bem como a probabilidade e a gravidade dos riscos para os direitos e liberdades das pessoas singulares.

24. Por conseguinte, o artigo 24.º impõe a adequação das medidas para poder comprovar que o tratamento é realizado em conformidade com os princípios e as disposições do regulamento.

25. O artigo 32.º, por seu turno, projeta o princípio da responsabilidade sobre as medidas concretas a tomar para assegurar «um nível de segurança adequado ao risco». Ao fazê-lo, acrescenta aos fatores já previstos a ter em conta na preparação das medidas técnicas e organizativas, as técnicas mais avançadas e os custos de aplicação.

26. O conceito de adequação exige que as soluções adotadas para assegurar os sistemas informáticos sejam aceitáveis, tanto em termos técnicos (pertinência das medidas) como qualitativos (eficácia da proteção). Para assegurar o respeito dos princípios da necessidade, da relevância e da proporcionalidade, os tratamentos devem ser, não só adequados, mas também

[8] C. Docksey, *Article 24. Responsibility of the controller*, *in* C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, p. 561. Os princípios e as obrigações decorrentes das regras sobre proteção de dados devem inspirar o tecido cultural das organizações, a todos os níveis, em vez de serem considerados como um conjunto de requisitos legais a impor pelo departamento jurídico.

[9] E. Belisario, G. Riccio, G. Scorza, GDPR e *Normativa Privacy — Commentario*, Wolters Kluwer, 2022, p. 301.

satisfatórios em relação às finalidades que se pretendem prosseguir. Nesta lógica, o princípio da minimização, por força do qual todas as fases do tratamento de dados devem constantemente conduzir à redução ao mínimo dos riscos de segurança, desempenha um papel decisivo [10].

27. Todo o regulamento se caracteriza pela prevenção do risco e pela responsabilidade do responsável pelo tratamento e, por conseguinte, por uma abordagem teleológica que visa o melhor resultado possível em termos de eficácia, ou seja, bastante afastada das lógicas formalistas ligadas à simples obrigação de respeitar procedimentos específicos para se libertar da responsabilidade [11].

28. O artigo 24.º não contém uma enumeração exaustiva de medidas «adequadas»: deve proceder-se a uma avaliação caso a caso. Isso está em conformidade com a filosofia do regulamento, que revela que é preferível que os procedimentos a adotar sejam escolhidos com base numa avaliação atenta da situação específica, para poderem ser o mais eficazes possível [12].

B. Primeira questão prejudicial

29. Com a sua primeira questão, o órgão jurisdicional de reenvio pergunta, em substância, se os artigos 24.º e 32.º do regulamento devem ser interpretados no sentido de que a verificação de uma «violação de dados pessoais», conforme definida no artigo 4.º, ponto 12, basta, por si só, para concluir que as medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento não são «adequadas» para assegurar a proteção dos dados.

30. Resulta da redação dos artigos 24.º e 32.º do regulamento que o responsável pelo tratamento, quando escolhe as medidas técnicas e organizativas que está obrigado a aplicar para assegurar a conformidade com o próprio regulamento, deve ter em conta uma série de fatores de avaliação enumerados nesses artigos e acima recordados.

31. O responsável pelo tratamento dispõe de uma certa margem de manobra no que diz respeito à determinação das medidas mais adequadas à luz da sua situação específica, mas essa escolha está sujeita a uma eventual fiscalização jurisdicional da conformidade das medidas aplicadas com todas as obrigações e objetivos do próprio regulamento.

32. Em particular, no que respeita às medidas de segurança, o artigo 32.º, n.º 1, impõe ao responsável pelo tratamento que tenha em conta as «técnicas mais avançadas». Isso implica uma limitação do nível tecnológico das medidas a aplicar ao que é razoavelmente possível no momento em que as medidas são tomadas: a suscetibilidade da medida para prevenir o risco deve, por

[10] E. Belisario, G. Riccio, G. Scorza, GDPR *cit.*, p. 380.

[11] É por isso que, como veremos, a resposta à primeira e quarta questões prejudiciais não podem deixar de ser negativas. Não se pode deduzir qualquer automatismo das disposições do regulamento: nem o simples facto de ter havido uma divulgação dos dados pessoais é suficiente para considerar que as medidas técnicas e organizativas tomadas não são adequadas, nem a circunstância de a própria divulgação ter ocorrido pela intervenção de pessoas alheias à organização do responsável pelo tratamento e fora da sua esfera de controlo são suficientes para o isentar de responsabilidade.

[12] L. Bolognini, E. Pelino, *Codice della disciplina privacy*, Giuffrè, 2019, p. 201. O legislador europeu supera, por conseguinte, a conceção da segurança do tratamento baseada na existência de medidas de segurança predeterminadas e adota uma metodologia específica das normas internacionais sobre sistemas de informação baseada no risco: essa [metodologia] prevê a identificação de medidas de mitigação dos riscos que prescindem das listas de verificação pré-configuradas e são de aplicação geral. Por conseguinte, deve recorrer-se a orientações e normas internacionais. O resultado dessa avaliação dos riscos torna-se, portanto, vinculativo quando a organização aplica as decisões para mitigar os riscos identificados, tornando-se ela própria *accountable* [responsável].

conseguinte, ser proporcional às soluções oferecidas pelo progresso da ciência, da técnica, da tecnologia e da investigação atuais, tendo igualmente em conta, como se verá, os custos de aplicação.

33. As medidas podem ser «adequadas» num determinado momento e, apesar disso, ser contornadas por cibercriminosos que utilizam ferramentas muito sofisticadas suscetíveis de violar também medidas de segurança conformes com as técnicas mais avançadas.

34. Por outro lado, parece ilógico considerar que a intenção do legislador da União era impor ao responsável pelo tratamento a obrigação de prevenir qualquer violação de dados pessoais, independentemente da diligência na preparação das medidas de segurança [13].

35. Como já foi referido, o regulamento inscreve-se numa ótica alheia a automatismos, exigindo uma elevada responsabilidade do responsável pelo tratamento, que não pode, todavia, levar à impossibilidade de este último comprovar que cumpriu corretamente as obrigações que lhe incumbem.

36. Além disso, o artigo 32.º, n.º 1, prevê que se tenha em conta, como referido, os «custos de aplicação» das medidas técnicas e organizativas em causa. Daqui resulta que a avaliação da adequação dessas medidas deve assentar numa ponderação entre os interesses do titular dos dados, que geralmente tendem a um nível de proteção mais elevado, e os interesses económicos e a capacidade tecnológica do responsável pelo tratamento, que tendem por vezes a um nível de proteção inferior. Esta ponderação deve respeitar os requisitos do princípio geral da proporcionalidade.

37. A isto deve acrescentar-se, numa ótica de interpretação sistemática, que o legislador prevê a possibilidade de ocorrerem violações dos sistemas; o artigo 32.º, n.º 1, alínea c), inclui entre as medidas sugeridas a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico. A previsão dessa capacidade entre as medidas de segurança que asseguram um nível de segurança adequado ao risco dessa capacidade seria inútil se se considerasse que a simples violação dos sistemas constitui, por si só, a prova da inadequação das próprias medidas.

C. Segunda questão prejudicial

38. Com a sua segunda questão, o órgão jurisdicional de reenvio pergunta, em substância, qual deve ser o objeto e o alcance da fiscalização jurisdicional ao examinar se as medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento são adequadas na aceção do artigo 32.º do regulamento.

39. Dado o caráter variável das situações que podem ocorrer na prática, o regulamento, como referido, não estabelece disposições vinculativas para a determinação das medidas técnicas e organizativas que o responsável pelo tratamento deve tomar para cumprir os requisitos do próprio regulamento. Por conseguinte, a adequação das medidas tomadas deve ser avaliada *in concreto*, verificando se as medidas específicas são suscetíveis de prevenir razoavelmente o risco e de minimizar os efeitos negativos da violação.

[13] O conceito de adequação mostra inequivocamente a intenção de não considerar pertinentes todas as medidas técnicas e organizativas abstratamente possíveis. Neste sentido, M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, *in* V. Cuffaro, R. D'Orazio, V. Ricciuto, *I dati personali nel diritto europeo*, Giappichelli, 2019, p. 1059.

40. Embora seja verdade que a escolha e a aplicação dessas medidas faz parte da avaliação subjetiva do responsável pelo tratamento, uma vez que as medidas mencionadas no regulamento são apenas exemplos, a fiscalização do órgão jurisdicional não se pode limitar ao controlo da observância pelo responsável pelo tratamento das obrigações que resultam dos artigos 24.º e 32.º, ou seja, se este previu (formalmente) determinadas medidas técnicas e organizativas. O órgão jurisdicional deve proceder a uma análise concreta do conteúdo dessas medidas, do modo como foram aplicadas e dos seus efeitos práticos, com base nos elementos de prova de que dispõe e nas circunstâncias do caso concreto. Como observou, com justeza, o Governo português, «o modo como [o responsável] cumpriu as suas obrigações parece indissociável do mérito das medidas tomadas, no sentido de demonstrar que, atendendo ao tratamento de dados em concreto (à sua natureza, âmbito, contexto e finalidade), à tecnologia mais avançada disponível e aos seus custos, bem como aos riscos para os direitos e liberdades dos cidadãos, o responsável pelo tratamento adotou todas as medidas necessárias e apropriadas para garantir um nível de segurança adequado ao risco subjacente» [14].

41. A fiscalização jurisdicional deverá, portanto, ter em conta todos os fatores constantes dos artigos 24.º e 32.º que, como referido, enumeram uma série de critérios para avaliar a adequação e fornecem exemplos de medidas que podem ser consideradas adequadas. Além disso, como sublinharam a Comissão e todos os Estados-Membros que apresentaram observações sobre a segunda questão, o artigo 32.º, n.os 1 a 3, sublinha a necessidade de «assegurar um nível de segurança adequado ao risco», indicando outros fatores pertinentes para esse efeito, como a eventual adoção pelo responsável pelo tratamento de um código de conduta aprovado ou de um procedimento de certificação aprovado, como preveem, respetivamente, os artigos 40.º e 42.º do regulamento.

42. A adoção de códigos de conduta ou de procedimentos de certificação pode constituir um elemento útil de avaliação para efeitos da observância do ónus da prova e da respetiva fiscalização jurisdicional. Todavia, precisa-se que não basta que o responsável pelo tratamento cumpra um código de conduta, pois este tem o ónus de provar que adotou concretamente as medidas que o referido código prevê, em conformidade com o princípio da responsabilidade. Em contrapartida, a certificação constitui «em si mesma uma prova da conformidade dos tratamentos efetuados com o regulamento mesmo que possa ser desmentida no plano prático» [15].

43. Por último observa-se que essas medidas devem ser revistas e atualizadas se necessário, por força do artigo 24.º, n.º 1. Isto também será objeto de avaliação pelo órgão jurisdicional nacional. Com efeito, o artigo 32.º, n.º 1, do regulamento [16] impõe ao responsável pelo tratamento um dever de controlo e de vigilância constante, prévia e subsequentemente às atividades de tratamento, mas também de manutenção e eventual atualização das medidas tomadas, com o objetivo tanto de evitar violações como, eventualmente, de limitar os seus efeitos.

[14] Observações escritas, n.º 31.

[15] M. Gambini, *Responsabilità*, *cit.*, p. 1067. A titularidade de uma certificação traduz-se, portanto, numa inversão do ónus da prova para o responsável, cuja prova de que atuou respeitando as obrigações previstas pelo regulamento fica facilitada.

[16] Ao prever expressamente, na alínea d), que o juízo de adequação se estende à eficácia das medidas tomadas, que deve ser regularmente testada, apreciada e avaliada, quer na fase inicial, quer periodicamente, para garantir a segurança efetiva de todos os tipos de tratamento, independentemente do seu nível de risco, e, ainda, ao prever expressamente, na alínea c), que as medidas técnicas e organizativas aplicadas devem apresentar a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico. V. M. Gambini, Responsabilità *cit.*, pp. 1064-1065.

44. Tendo, no entanto, a considerar que não é oportuno que o próximo acórdão inclua uma enumeração de elementos substanciais, como a sugerida pelo Governo português [17]. Isso poderia dar lugar a interpretações contraditórias, dado que, como é evidente, a lista não pode nunca ser exaustiva.

D. Terceira questão prejudicial

45. Com a primeira parte da sua terceira questão, o órgão jurisdicional de reenvio pede, em substância, ao Tribunal de Justiça que determine se, tendo em conta o princípio da responsabilidade na aceção do artigo 5.º, n.º 2, e do artigo 24.º, em conjugação com o considerando 74 [18] do regulamento, no âmbito de uma ação de indemnização ao abrigo do artigo 82.º, o ónus da prova da adequação das medidas técnicas e organizativas nos termos do artigo 32.º cabe ao responsável pelo tratamento de dados pessoais.

46. As considerações precedentes permitem-me responder sucintamente a esta questão em sentido afirmativo.

47. Com efeito, a letra da lei, o contexto e as finalidades do regulamento apontam de forma unívoca no sentido de que o ónus da prova cabe ao responsável pelo tratamento.

48. Resulta da redação de várias disposições do regulamento que o responsável pelo tratamento deve «poder» ou ser «capaz» de «comprovar» o cumprimento das obrigações previstas pelo regulamento e, particularmente, que aplicou medidas adequadas para o efeito, como indicado no considerando 74, no artigo 5.º, n.º 2, e no artigo 24.º, n.º 1. Como sublinha o Governo português, o referido considerando 74 especifica que o ónus da prova que cabe assim ao responsável pelo tratamento deve incluir a prova da «eficácia das medidas» em causa.

49. Esta interpretação literal parece-me apoiada pelas seguintes considerações práticas e teleológicas.

50. No que respeita à repartição do ónus da prova, no âmbito de uma ação de indemnização por danos baseada no artigo 82.º, o titular dos dados que intentou a ação contra o responsável pelo tratamento deve provar, em primeiro lugar, que houve uma violação do regulamento, em segundo lugar, que sofreu um dano e, em terceiro lugar, que existe um nexo de causalidade entre os dois elementos anteriores, como foi salientado em todas as observações escritas sobre a quinta questão

[17] N.º 30 das observações escritas: «será o responsável pelo tratamento a ter de comprovar de que modo avaliou todos os fatores e circunstâncias relacionados com o tratamento em causa, designadamente, o resultado da análise de riscos realizada, os riscos identificados, as medidas concretas que encontrou para mitigar esses riscos, a justificação das opções tomadas, atendendo às soluções tecnológicas existentes no mercado, a eficácia das medidas, a correlação entre as medidas técnicas e as medidas organizativas, a formação do pessoal que trata dados, se houve recurso a subcontratação para operações de tratamento de dados, incluindo em desenvolvimento e manutenção IT, e se houve controlo do responsável e foram dadas instruções precisas aos subcontratantes, nos termos do artigo 28.º RGPD, sobre o tratamento de dados realizado por estes, como foram avaliadas as infraestruturas de comunicação e de suporte ao sistema de informação e como foi classificado o nível de risco para os direitos e liberdades dos titulares».

[18] De acordo com o considerando 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.»

prejudicial. Trata-se de três requisitos cumulativos, como resulta também de jurisprudência consolidada do Tribunal de Justiça e do Tribunal Geral, no contexto da responsabilidade extracontratual da União [19].

51. Todavia, considero que a obrigação do recorrente de demonstrar a existência de uma violação do regulamento não pode ir ao ponto de exigir que demonstre em que medida as medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento não são adequadas, na aceção dos artigos 24.º e 32.º

52. Como sublinha a Comissão, frequentemente a apresentação dessas provas é quase impossível na prática, uma vez que os titulares dos dados, geralmente, não têm conhecimento suficiente para poderem analisar essas medidas, nem acesso a todas as informações na posse do responsável pelo tratamento contestado, particularmente no que respeita aos métodos aplicados para garantir a segurança desse tratamento. Além disso, o responsável pelo tratamento pode por vezes alegar que a sua recusa em revelar estes factos aos titulares dos dados se baseia no fundamento legítimo de não tornar públicos os seus assuntos internos, ou mesmo elementos abrangidos pelo segredo profissional, designadamente por razões de segurança.

53. Assim, se se considerar que o ónus da prova cabe ao titular dos dados, o resultado prático traduz-se no facto de o direito de ação previsto no artigo 82.º, n.º 1, perder grande parte do seu alcance. Na minha opinião, isto não está em conformidade com as intenções do legislador da UE que, ao adotar este regulamento, procurou reforçar os direitos dos titulares dos dados e as obrigações dos responsáveis pelo tratamento, em relação à Diretiva 95/46 que a substituiu. Por conseguinte, é mais lógico, e juridicamente defensável, que o responsável pelo tratamento seja obrigado a demonstrar, na sua defesa numa ação de indemnização, que respeitou as obrigações resultantes dos artigos 24.º e 32.º deste regulamento tomando medidas efetivamente adequadas.

54. Com a segunda parte da sua terceira questão, o órgão jurisdicional de reenvio pergunta ao Tribunal de Justiça, em substância, se uma perícia judicial pode ser considerada uma prova necessária e suficiente para avaliar a adequação das medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento dos dados pessoais numa situação em que o acesso não autorizado e a divulgação de dados pessoais são o resultado de uma atividade de *hacking*.

55. Considero, como sublinharam (em substância) igualmente os Governos búlgaro e italiano, a Irlanda e a Comissão, que a resposta a estas questões se deve basear na nossa jurisprudência consolidada segundo a qual, por força do princípio da autonomia processual, na falta de normas da União na matéria, cabe ao ordenamento jurídico interno de cada Estado-Membro regular as modalidades processuais dos processos judiciais destinados a proteger os direitos das pessoas, desde que essas regras, nas situações reguladas pelo direito da União, não sejam menos favoráveis do que as que regulam situações semelhantes sujeitas 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).

[19] V., nomeadamente, Acórdãos do Tribunal de Justiça de 5 de setembro de 2019, União Europeia/Guardian Europe e Guardian Europe/União Europeia (C-447/17 P e C-479/17 P, EU:C:2019:672, n.º 147), e de 28 de outubro de 2021, Vialto Consulting/Comissão (C-650/19 P, EU:C:2021:879, n.º 138), bem como Acórdãos do Tribunal Geral de 13 de janeiro de 2021, Helbert/EUIPO (T-548/18, EU:T:2021:4, n.º 116), e de 29 de setembro de 2021, Kočner/Europol (T-528/20, não publicado, EU:T:2021:631, n.º 61), nos quais se recorda que devem estar preenchidos três requisitos, a saber, «ilegalidade do comportamento de que vem acusada a instituição da União, a realidade do dano e a existência de um nexo de causalidade entre o comportamento dessa instituição e o dano invocado».

56. No processo em apreço, observo que o regulamento não contém nenhuma disposição destinada a determinar os meios de prova admissíveis e a sua força probatória, nomeadamente no que respeita às medidas de instrução (como uma perícia judicial) que os órgãos jurisdicionais nacionais podem ou devem ordenar para avaliar se um responsável pelo tratamento de dados pessoais tomou as medidas adequadas nos termos deste regulamento. Considero, portanto, que, na falta de normas harmonizadas na matéria, cabe ao ordenamento jurídico interno de cada Estado-Membro determinar essas modalidades processuais, sem prejuízo do respeito pelos princípios da equivalência e da efetividade.

57. O referido «princípio da efetividade», que implica que um órgão jurisdicional independente deve efetuar uma avaliação imparcial, pode ficar comprometido se o adjetivo «suficiente» for entendido no sentido que o órgão jurisdicional de reenvio parece atribuir-lhe, ou seja, de que se pode deduzir automaticamente de um parecer pericial que as medidas tomadas pelo responsável pelo tratamento são adequadas [20].

E. Quarta questão prejudicial

58. Com a quarta questão, o órgão jurisdicional de reenvio pergunta, em substância, se o artigo 82.º, n.º 3, do regulamento deve ser interpretado no sentido de que, aquando da violação do regulamento (que consiste, como neste processo, na «divulgação não autorizada» ou no «acesso não autorizado» a dados pessoais na aceção do artigo 4.º, ponto 12), por pessoas que não são funcionários do responsável pelo tratamento desses dados e que não estão sujeitas ao controlo deste último, tal constitui uma circunstância pela qual o responsável pelo tratamento não é de modo algum responsável e, portanto, um motivo de isenção da sua responsabilidade, na aceção do artigo 82.º, n.º 3.

59. A resposta à questão decorre linearmente do anteriormente exposto sobre a filosofia geral do regulamento: não estão previstos automatismos e, portanto, o simples facto de a divulgação ou o acesso não autorizados a dados pessoais ter ocorrido devido a pessoas externas à esfera de controlo do responsável pelo tratamento não o isenta da sua responsabilidade.

60. Em primeiro lugar, em termos literais, note-se que nem o artigo 82.º, n.º 3, nem o considerando 146 estabelecem condições particulares que possam ser preenchidas para que o responsável pelo tratamento fique isento da responsabilidade, a menos que se prove que «não é de modo algum responsável pelo evento que deu origem aos danos». Resulta desta formulação, por um lado, que o responsável pelo tratamento só pode ser isento da sua responsabilidade se provar que não é responsável pelo evento que causou o dano em questão e, por outro, que o nível de prova exigido por esta disposição é elevado, devido à utilização do termo «de modo algum», como sublinhou a Comissão [21].

61. O regime de responsabilidade previsto no artigo 82.º e, mais genericamente, em todo o regulamento, foi objeto de um amplo debate na doutrina dos diferentes Estados-Membros. Com efeito, contém elementos tradicionais próprios da responsabilidade extracontratual, mas também elementos que, na estrutura das disposições, o aproximam da responsabilidade contratual ou

[20] Observações escritas, n.º 39.

[21] Em conformidade com a jurisprudência constante do Tribunal de Justiça segundo a qual as exceções a uma regra geral devem ser interpretadas de forma estrita, a eventual isenção de responsabilidade prevista no artigo 82.º, n.º 3, deve ser interpretada de forma estrita. V., por analogia, Acórdãos de 15 de outubro de 2020, Association française des usagers de banques (C-778/18, EU:C:2020:831, n.º 53), e de 5 de abril de 2022, Commissioner of An Garda Síochána e o. (C-140/20, EU:C:2022:258, n.º 40).

mesmo de uma forma de responsabilidade objetiva, devido à perigosidade intrínseca da atividade de tratamento de dados. Não é este o local para dar conta do debate pormenorizado, mas, na minha opinião, o artigo 82.º não parece instituir um regime de responsabilidade objetiva [22].

62. Os danos causados pela violação de dados pessoais podem configurar-se como a consequência culposa da não adoção das medidas técnicas e organizativas razoáveis e, em qualquer caso, adequadas para o evitar, tendo em conta os riscos para os direitos e liberdades das pessoas associados à atividade de tratamento. Esses riscos tornam mais rigorosa a obrigação de prevenir e evitar o dano, ampliando o dever de diligência do autor do tratamento. Por conseguinte, é possível, da leitura coordenada dos deveres de conduta que cabem aos autores do tratamento e da disposição relativa à prova liberatória do autor do dano, extrair argumentos a favor do reconhecimento da natureza de responsabilidade agravada por culpa presumida em caso de responsabilidade por tratamento ilícito de dados pessoais, prevista pelo artigo 82.º do regulamento [23].

63. Daqui resulta a possibilidade de o responsável pelo tratamento produzir uma prova liberatória (não autorizada na responsabilidade objetiva). No que respeita à articulação do ónus da prova, o artigo 82.º, n.º 3, do regulamento prevê um regime favorável ao lesado [24], ao estabelecer uma forma de inversão do ónus da prova da culpa do infrator, em total simetria com a referida inversão do ónus da prova no que respeita à adequação das medidas tomadas. O legislador mostra assim que está consciente dos perigos inerentes à aceitação de uma repartição diferente do ónus da prova; que, se imputasse à pessoa singular lesada a obrigação de provar a culpa do infrator, acabaria por agravar excessivamente a posição desta e, portanto, por comprometer, de facto, a operacionalidade da proteção indemnizatória, no âmbito de normas ligadas à utilização das novas tecnologias. Pode, de facto, tornar-se particularmente oneroso para o titular dos dados reconstruir e ter acesso às modalidades de produção do dano e, em consequência, provar a culpa do responsável. Pelo contrário, o responsável pelo tratamento está na melhor posição para oferecer a prova liberatória destinada a demonstrar que não é de modo algum responsável pelo evento que deu origem aos danos [25].

64. O responsável pelo tratamento terá igualmente de provar, em conformidade com o princípio da responsabilidade anteriormente descrito, que fez tudo quanto era possível para restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada.

65. Voltando à questão do órgão jurisdicional de reenvio, com base no que acaba de ser exposto quanto à natureza da responsabilidade do responsável pelo tratamento, se, como referido, o responsável pelo tratamento pode ser isento de responsabilidade provando que a violação se deveu a uma causa pela qual não é de modo algum responsável, o simples facto de o evento ter sido causado por uma pessoa fora da sua esfera de controlo não pode ser considerado como tal.

[22] A responsabilidade civil tende a ser qualificada de objetiva sempre que o agente é obrigado a tomar todas as medidas abstratamente possíveis para evitar o dano, independentemente do conhecimento efetivo que delas tenha tido ou da sua sustentabilidade económica. Em contrapartida, quando é imposta ao agente a adoção de medidas que devem ser normalmente observadas por um operador do setor económico de referência para manter a segurança e prevenir os prejuízos que podem resultar da atividade exercida, a imputação desse dano tende a aproximar-se de um regime de responsabilidade por culpa específica. Gambini, M., *Responsabilità*, já referido, p. 1055.

[23] M. Gambini, Responsabilità *cit.* p. 1059. No mesmo sentido, para a tese segundo a qual a prova de que tomou as medidas adequadas não consiste numa simples alegação da maior diligência exigível, mas na demonstração de um facto externo gerador do dano, com características de imprevisibilidade e de inevitabilidade próprias do caso fortuito e da força maior, S. Sica, Sub art. 82, *in* R. D'Orazio, G. Finocchia, O. Pollicino, G. Resta, *Codice della privacy* e *data protection*, Giuffrè, 2021.

[24] «[S]*e provar* que não é de modo algum responsável pelo evento que deu origem aos danos.»

[25] M. Gambini, Responsabilità *cit.*, p. 1060.

66. Quando um responsável pelo tratamento é vítima de um ataque por cibercriminosos, o evento causador do dano pode ser considerado não imputável ao responsável pelo tratamento, mas não se exclui que a negligência do responsável pelo tratamento dos dados tenha estado na origem do ataque em causa, facilitando-o devido à falta ou inadequação das medidas de segurança dos dados pessoais que este último é obrigado a aplicar. Trata-se de apreciações factuais, específicas para cada caso, que são deixadas ao órgão jurisdicional nacional chamado a pronunciar-se, à luz das provas que lhe são apresentadas.

67. Além disso, resulta da experiência comum que os ataques externos aos sistemas de entidades públicas ou privadas responsáveis por uma grande quantidade de dados pessoais são bastante mais frequentes do que os ataques internos. O responsável pelo tratamento deve, portanto, preparar medidas adequadas para lidar, particularmente, com ataques externos.

68. Por último, de um ponto de vista teleológico, note-se que o regulamento prossegue o objetivo de um nível elevado de proteção. A este respeito, o Tribunal de Justiça já sublinhou que decorre do artigo 1.º, n.º 2, do regulamento, em conjugação com os considerandos 10, 11 e 13, que este regulamento impõe às instituições, aos órgãos, organismos e agências da União e às autoridades competentes dos Estados-Membros, a tarefa de assegurar um nível elevado de proteção dos direitos garantidos no artigo 16.º TFUE e no artigo 8.º da Carta [26].

69. Se o Tribunal de Justiça optar pela interpretação segundo a qual, quando a violação do regulamento é cometida por um terceiro, o responsável pelo tratamento deve ser automaticamente isento de responsabilidade nos termos do artigo 82.º, n.º 3, essa interpretação tem um efeito incompatível com o objetivo de proteção prosseguido por este instrumento, uma vez que fragilizaria os direitos dos titulares de dados, na medida em que limitaria essa responsabilidade aos casos em que a violação é devida a pessoas que se encontrem sob a autoridade e/ou o controlo do responsável pelo tratamento.

F. Quinta questão prejudicial

70. Com a quinta questão, o órgão jurisdicional nacional pede ao Tribunal de Justiça, em substância, que interprete o conceito de «danos morais» (na linguagem do regulamento «imateriais») na aceção do artigo 82.º do regulamento. Em particular, pergunta se o artigo 82.º, n.ºs 1 e 2, do regulamento, em conjugação com os seus considerandos 85 e 146 [27], devem ser interpretadas no sentido de que, numa situação em que a violação deste regulamento consiste num acesso não autorizado a dados pessoais e numa divulgação não autorizada desses dados por cibercriminosos, o facto de o titular dos dados recear uma eventual utilização abusiva dos seus dados pessoais no futuro pode constituir, por si só, um dano (moral) que confere direito a uma indemnização.

[26] V., neste sentido, Acórdão de 15 de junho de 2021, Facebook Ireland e o. (C-645/19, EU:C:2021:483, n.ºs 44 e 45).

[27] De acordo com o considerando 85: «Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares […]». Nos termos do considerando 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 titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido […]».

71. Nem o artigo 82.º nem os considerandos relativos à indemnização dos danos fornecem uma resposta clara à questão, mas deles podem extrair-se alguns elementos úteis para a análise: os danos imateriais (ou morais) podem ser objeto de indemnização a acrescer aos danos materiais (ou patrimoniais); a violação do regulamento não implica automaticamente os danos que «causou» ou, mais precisamente, a violação de dados pessoais «pode causar» danos físicos, materiais ou imateriais às pessoas singulares; 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 regulamento; os danos «sofridos» devem ser «integral e efetivamente» indemnizados.

72. O teor literal das disposições do regulamento já exclui qualquer eventual ideia de danos presumidos: o objetivo primário da responsabilidade civil prevista pelo regulamento consiste em que o titular dos dados seja «integral e efetivamente» indemnizado pelos danos que tenha sofrido e, portanto, em restabelecer o equilíbrio da situação jurídica alterada negativamente pela violação do direito [28].

73. Por outro lado, também de um ponto de vista sistemático, como no direito da concorrência, o regulamento prevê dois pilares de proteção: um de natureza pública, com a previsão de sanções em caso de violação das disposições do regulamento, outra de natureza privada, que prevê precisamente uma responsabilidade civil de natureza extracontratual, suscetível de ser qualificada como agravada por culpa presumida com as características acima referidas, incluindo no que respeita à prova liberatória [29].

74. Por conseguinte, uma interpretação ampla [30] do conceito de dano (moral) não pode levar a considerar que o legislador renunciou à necessidade de que se verifique um verdadeiro «dano».

75. O verdadeiro problema de fundo consiste em saber se, uma vez demonstrada a existência da violação e do nexo de causalidade, pode existir um direito a indemnização fundado em meras preocupações, receios e ansiedades do titular dos dados quanto a uma eventual futura utilização abusiva dos dados pessoais, quando essa utilização abusiva não tenha sido comprovada e/ou quando o titular dos dados não tenha sofrido outros danos.

76. Segundo jurisprudência constante do Tribunal de Justiça, aos conceitos de uma disposição do direito da União, que não remete expressamente para o direito dos Estados-Membros para determinar o seu sentido e o seu alcance deve, normalmente, ser dada uma interpretação autónoma e uniforme em toda a União, que tenha em conta não só os termos dessa disposição, mas também o contexto em que se insere, os objetivos que prossegue o ato de que faz parte e a génese da mesma [31].

[28] V. Conclusões do advogado-geral M. Campos Sánchez-Bordona, supramencionadas, n.º 29 e nota 11. Nessas conclusões, o advogado-geral conclui corretamente a sua análise sob os pontos de vista literal, histórico, contextual e teleológico, excluindo a natureza «punitiva» dos danos indemnizáveis aos titulares de dados nos termos do artigo 82.º (n.os 27 a 55), salientando, por um lado, que os Estados-Membros «não têm de escolher (e não podem, na realidade) entre os mecanismos do capítulo VIII para assegurar a proteção dos dados. Perante uma violação que não dê origem a um dano, é ainda oferecida ao titular dos dados (pelo menos) o direito de apresentar uma reclamação a uma autoridade de controlo» e, por outro, que «a perspetiva de obtenção de uma compensação sem a existência de qualquer dano incentivasse os litígios pela via civil, eventualmente com ações nem sempre justificadas, e, nessa medida, poderia desencorajar a atividade de tratamento de dados» (n.os 54 e 55).

[29] Recusar o direito a indemnização pelos sentimentos ou emoções fracos e temporários relacionados com a violação de regras relativas ao tratamento não deixa o titular dos dados totalmente desamparado (neste sentido, v. Conclusões do advogado-geral M. Campos Sánchez-Bordona *cit*., n.º 115).

[30] Ou «em sentido lato» nos termos do considerando 146.

[31] V. Acórdãos de 15 de abril de 2021, The North of England P & I Association (C-786/19, EU:C:2021:276, n.º 48), e de 10 de junho de 2021, KRONE — Verlag (C-65/20, EU:C:2021:471, n.º 25).

77. Como recordou o advogado-geral M. Campos Sánchez-Bordona [32], o Tribunal de Justiça não elaborou uma definição geral de «danos» aplicável indistintamente em qualquer domínio [33]. No que respeita aos danos morais, pode deduzir-se da sua jurisprudência que: quando um dos objetivos da disposição interpretada consiste na proteção do indivíduo ou de uma determinada categoria de indivíduos [34], o conceito de danos deve ser amplo; em coerência com esse critério, a indemnização estende-se aos danos imateriais, mesmo que não sejam referidos na disposição interpretada [35].

78. Embora a jurisprudência do Tribunal de Justiça permita considerar que, nos termos expostos, existe no direito da União um princípio de indemnização dos danos imateriais, concordo com o advogado-geral M. Campos Sánchez-Bordona no sentido de que daí não se não possa inferir uma regra por força da qual *qualquer* dano imaterial seja indemnizável, independentemente da sua gravidade [36].

79. Neste contexto, é relevante a distinção, proposta ao Tribunal de Justiça, entre danos imateriais indemnizáveis e *outros inconvenientes resultantes do desrespeito da legalidade* que, dada a sua fraca importância, não dão necessariamente direito a indemnização [37].

80. O Tribunal de Justiça admite esta distinção quando faz referência aos transtornos e inconvenientes como categoria autónoma relativamente à dos danos, em domínios em que considera que devem ser indemnizados [38].

[32] V. Conclusões do advogado-geral M. Campos Sánchez-Bordona, supramencionadas, n.º 104.

[33] Também não indicou um método de interpretação — autónomo ou por remissão para as ordens jurídicas nacionais — preferencial: depende da matéria que é objeto da análise. Compare-se os Acórdãos de 10 de maio de 2001, Veedfald (C-203/99, EU:C:2001:258, n.º 27), em matéria de produtos defeituosos; de 6 de maio de 2010, Walz (C-63/09, EU:C:2010:251, n.º 21), sobre responsabilidade das transportadoras aéreas; ou de 10 de junho de 2021, Van Ameyde España (C-923/19, EU:C:2021:475, n.ºs 37 e segs.), relativo à responsabilidade civil aplicável aos acidentes resultantes da circulação de veículos automóveis.

[34] Por exemplo, os consumidores de produtos ou as vítimas de acidentes de viação.

[35] Em matéria de viagens organizadas, v. Acórdão de 12 de março de 2002, Leitner (C-168/00, EU:C:2002:163); no âmbito da responsabilidade civil resultante da circulação de veículos automóveis, Acórdãos de 24 de outubro de 2013, Haasová (C-22/12, EU:C:2013:692, n.ºs 47 a 50); de 24 de outubro de 2013, Drozdovs (C-277/12, EU:C:2013:685, n.º 40), e de 23 de janeiro de 2014, Petillo (C-371/12, EU:C:2014:26, n.º 35).

[36] V. Conclusões do advogado-geral M. Campos Sánchez-Bordona, supramencionadas, n.º 105. O Tribunal de Justiça, por exemplo, reconheceu a compatibilidade com as normas europeias de uma lei nacional que, para efeitos de cálculo da indemnização, distingue os danos imateriais relacionados com lesões corporais causadas por um acidente de acordo com a origem deste último; v. Acórdão de 23 de janeiro de 2014, Petillo (C-371/12, EU:C:2014:26), dispositivo: o direito da União não se opõe «a uma legislação nacional […] que prevê um regime especial de indemnização dos danos imateriais resultantes de lesões corporais pouco significativas causadas por acidentes de circulação rodoviária, que limita a indemnização desses danos relativamente ao que é admitido em matéria de reparação de danos idênticos resultantes de outras causas que não sejam esses acidentes».

[37] Esta distinção é compreendida nas ordens jurídicas nacionais como corolário inevitável da vida em sociedade. Recentemente, em matéria de proteção de dados, em Itália, Tribunale di Palermo (Tribunal de Primeira Instância de Palermo), Secção I Cível, Sentença n.º 5261, de 5 de outubro de 2017, e Acórdão do Supremo Tribunal de Cassação, n.º 17383/2020, Secção VI, Cível (comum). Na Alemanha, entre outras, AG Diez, de 7 de novembro de 2018 - 8 C 130/18; LG Karlsruhe, de 2 de agosto de 2019 — 8 O 26/19, e AG Frankfurt am Main, de 10 de julho de 2020 — 385 C 155/19 (70). Na Áustria, OGH 6 Ob 56/21k.

[38] V. Acórdão de 23 de outubro de 2012, Nelson e o. (C-581/10 e C-629/10, EU:C:2012:657, n.º 51), sobre a distinção entre «danos» na aceção artigo 19.º da Convenção para a unificação de certas regras relativas ao transporte aéreo internacional, celebrada em Montreal, em 28 de maio de 1999, e «inconvenientes» na aceção do Regulamento n.º 261/2004, que são indemnizáveis ao abrigo do artigo 7.º deste último, por força do Acórdão de 19 de novembro de 2009, Sturgeon e o. (C-402/07 e C-432/07, EU:C:2009:716). Neste setor, como no do transporte marítimo e por vias navegáveis interiores de passageiros a que se refere o Regulamento n.º 1177/2010, o legislador pôde reconhecer uma categoria abstrata graças à circunstância de o fator que dá origem ao transtorno e a sua essência serem idênticos para todos os afetados. Não penso que se possa inferir o mesmo em matéria de proteção de dados.

81. De forma empírica, pode observar-se que qualquer violação de uma norma relativa à proteção de dados pessoais dará origem a uma reação negativa do titular dos dados. Uma indemnização decorrente do simples sentimento de desconforto face à falta de respeito de outrem pela lei confunde-se facilmente com uma indemnização sem dano que, como já referimos, não parece possível na situação prevista no artigo 82.º do regulamento.

82. O facto de, em circunstâncias como as do processo principal, a utilização abusiva dos dados pessoais ser apenas potencial, e não efetiva, é suficiente para considerar que o titular dos dados pode ter sofrido um dano moral causado pela violação do regulamento, desde que este demonstre que o receio dessa utilização abusiva lhe causou concreta e especificamente um dano emocional real e certo [39].

83. A fronteira entre os simples descontentamentos (não indemnizáveis) e os verdadeiros danos morais (indemnizáveis) é ténue, mas os órgãos jurisdicionais nacionais, aos quais cabe a função de delimitar caso a caso essa fronteira, devem proceder a uma avaliação atenta de todos os elementos fornecidos pelo titular dos dados que pede a indemnização, a quem caberá o ónus de alegar com precisão, e não de modo genérico, elementos concretos suscetíveis de conduzir à existência de um «dano moral efetivamente sofrido» devido à violação de dados pessoais, sem que, no entanto, esse dano atinja um limiar específico de gravidade predeterminado: o que importa é que não se trate da simples perceção subjetiva, variável e dependente igualmente de elementos de caráter e pessoais, mas de uma inquietação objetiva, mesmo que ligeira mas demonstrável, na sua esfera física ou psíquica ou na sua vida pessoal, da natureza dos dados pessoais em causa e da importância que revestem para a vida do titular dos dados e talvez também da perceção que a sociedade tem, nesse momento, dessa inquietação específica decorrente da violação dos dados [40].

IV. Conclusão

84. Tendo em conta todas as considerações precedentes, proponho ao Tribunal de Justiça que responda às questões prejudiciais submetidas do seguinte modo:

«Os artigos 5.º, 24.º, 32.º e 82.º do Regulamento 2016/679 devem ser interpretados no sentido de que:

a mera existência de uma "violação de dados pessoais", conforme definida no artigo 4.º, ponto 12, não basta, por si só, para concluir que as medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento não são "adequadas" para assegurar a proteção dos dados em causa;

ao examinar se as medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento são adequadas, o órgão jurisdicional nacional chamado a pronunciar-se deve efetuar uma fiscalização que abrange uma análise concreta quer do conteúdo dessas medidas, quer do modo como foram aplicadas e dos seus efeitos práticos;

[39] Segundo a Irlanda, estas considerações são particularmente importantes na prática, no contexto da criminalidade informática, uma vez que, se qualquer pessoa afetada, ainda que minimamente, por uma violação tiver direito a uma indemnização por danos morais, isso terá um forte impacto, especialmente nos responsáveis pelo tratamento de dados do setor público, que são financiados por fundos públicos limitados e devem antes servir interesses coletivos, incluindo a melhoria da segurança dos dados pessoais (observações escritas, n.º 72).

[40] V. Conclusões do advogado-geral M. Campos Sánchez-Bordona, supramencionadas, n.º 116.

no âmbito de uma ação de indemnização ao abrigo do artigo 82.º do RGPD, o responsável pelo tratamento dos dados pessoais tem o ónus de provar que as medidas técnicas e organizativas são adequadas nos termos do artigo 32.º do referido regulamento;

em conformidade com o princípio da autonomia processual, compete ao ordenamento jurídico interno de cada Estado-Membro determinar os meios de prova admissíveis e a sua força probatória, incluindo as medidas de instrução que os órgãos jurisdicionais nacionais podem ou devem ordenar para avaliar se um responsável pelo tratamento de dados pessoais aplicou as medidas adequadas nos termos deste regulamento, no respeito dos princípios da equivalência e da eficácia definidos pelo direito da União;

o facto de a violação deste regulamento que causou os danos em causa ter sido cometida por um terceiro não constitui, em si mesmo, um motivo para isentar de responsabilidade o responsável pelo tratamento e, para beneficiar da isenção prevista nesta disposição, o responsável pelo tratamento tem de provar que não é de modo algum responsável pela violação;

o prejuízo consistente no receio de uma eventual futura utilização abusiva dos seus dados pessoais, cuja existência tenha sido demonstrada pelo titular dos dados, pode constituir um dano moral que confere direito a uma indemnização, desde que o titular dos dados demonstre ter sofrido individualmente um dano emocional, real e certo, circunstância que cabe ao órgão jurisdicional nacional chamado a pronunciar-se verificar em cada caso concreto.»