Processo C-340/21

Resumo do pedido de decisão prejudicial em aplicação do artigo 98.°, n.° 1, do Regulamento de Processo do Tribunal de Justiça

Data de entrada:

2 de junho de 2021

Órgão jurisdicional de reenvio:

Varhoven administrativen sad (Supremo Tribunal Administrativo, Bulgária)

Data da decisão de reenvio:

14 de maio de 2021

Recorrente em cassação:

VB

Recorrido em cassação:

Natsionalna agentsia za prihodite (Agência Nacional para as Receitas).

Objeto do processo principal

Recurso contra uma sentença que julgou improcedente uma ação de indemnização por danos imateriais sofridos em resultado do incumprimento ilegal pelo recorrido em cassação, na sua qualidade de responsável pelo tratamento, das suas obrigações por força da Zakon za zashtita na lichnite danni (Lei sobre a proteção de dados pessoais, a seguir «Lei sobre a proteção de dados pessoais») e do Regulamento 2016/679.

Objeto e fundamento jurídico do pedido de decisão prejudicial

Pedido de decisão prejudicial apresentado nos termos do artigo 267.° TFUE, para efeitos da interpretação dos considerandos 74, 85 e 146 e dos artigos 4.°, ponto 12, 5.°, n.° 2, 24.°, 32.° e 82.° do Regulamento 2016/679.

Questões prejudiciais

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

3. Em caso de resposta negativa à primeira questão, deve o princípio da responsabilidade na aceção do artigo 5.°, n.° 2, e do artigo 24.°, 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.°, n.° 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.° 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 caso 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.°, n.° 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.°, ponto 12, do Regulamento (UE) 2016/679, como no presente caso, 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.°, 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 caso como o presente, em que 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?

Disposições e jurisprudência da União Europeia

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). Regulamento: Considerandos 1, 4, 6, 74, 75, 76, 77, 83, 85, 146, Art 4(2) (7) e (12), Art 5, 24, 32, 33, 79, 82.

Acórdão do Tribunal de Justiça de 30 de maio de 2013, Worten (C-342/12, EU:C:2013:355), n.os 24 e 26.

Disposições de direito nacional

Administrativnoprotsesualen kodeks (Código de Processo Administrativo – artigos 144.°, n.° 1, 203.° e 208.°).

Grazhdanski protsesualen kodeks (Código de Processo Civil) – artigo 154.°

Zakon za otgovornostta na darzhavata i obshtinite za vredi (Lei sobre a responsabilidade por danos do Estado e dos municípios).

Zakon za zashtita na lichnite danni (Lei sobre a proteção de dados pessoais) – artigos 39.°, n.os 1 e 2, e 59.°, n.° 1.

Apresentação sucinta dos factos e do processo principal

1 A Natsionalna agentsia za prihodite (Agência Nacional de Receitas Fiscais, a seguir «NAP») é responsável pelo tratamento de dados na aceção do artigo 4.°, ponto 7 do Regulamento 2016/679. Segundo a lei nacional, a NAP é um organismo administrativo sob a autoridade do Ministro das Finanças, responsável pelo apuramento, a proteção e a recuperação de créditos públicos e privados do Estado previamente determinados. No exercício dos poderes públicos que lhe são conferidos, trata dados pessoais.

2 Em 15 de julho de 2019, os meios de comunicação social tornaram público que tinha havido um acesso não autorizado ao sistema de informação da NAP e que as informações das suas bases de dados contendo dados pessoais e informações fiscais e da segurança social tinham sido publicadas na Internet. Foram afetados 4 057 328 cidadãos búlgaros, enquanto o número de todas as pessoas singulares envolvidas, que incluía tanto cidadãos búlgaros como estrangeiros, ascendia a 6 074 140. Entre essas pessoas, está VB.

3 Até à data, não houve nenhuma condenação penal definitiva das pessoas que (supostamente) incorreram no acesso não autorizado referido, definido pelos meios de comunicação social como um «ataque de hacker».

4 Após o acesso, centenas de cidadãos processaram a NAP a fim de obterem uma compensação por danos imateriais.

5 Em 16 de setembro de 2019, VB intentou uma ação contra a NAP no Administrativen sad Sofia-grad (Tribunal Administrativo de Sófia, a seguir ASSG) para pagamento de danos no montante de 1 000 leva (BGN) (aproximadamente 511 euros) por força do artigo 82.°, n.° 1, do Regulamento 2016/679, do artigo 1.°, n.° 1, da Lei sobre a responsabilidade por danos do Estado e dos municípios (Zakon za otgovornostta na darzhavata i obshtinite za vredi) e do artigo 39.°, n.° 1, da Lei sobre a proteção de dados pessoais (Zakon za zashtita na lichnite danni).

6 Na sua ação em primeira instância, VB alegou que a NAP não tinha «cumprido da melhor forma possível» a sua obrigação de «garantir adequadamente a sua cibersegurança» e de «garantir o mais eficazmente possível a segurança dos dados pessoais dos cidadãos da República da Bulgária». Em consequência, ocorreu uma violação de dados pessoais na aceção do artigo 4.°, ponto 12, do regulamento e dados pessoais foram ilicitamente divulgados.

7 Segundo VB, «a falta de diligência e a não aplicação de medidas eficazes de proteção de dados» constituía um incumprimento por parte da NAP das suas obrigações de proteção dos dados dos cidadãos e, em sua opinião, isso constituía uma violação dos artigos 24.° e 32.° do Regulamento 2016/679. Como responsável pelo tratamento, a NAP tinha a obrigação de processar os dados pessoais de modo a «garantir níveis de segurança adequados» através da adoção de medidas técnicas e organizativas apropriadas.

8 VB alegou que a violação das obrigações por parte da NAP lhe tinha causado danos imateriais, sob a forma de preocupações e receios de uma futura utilização indevida dos seus dados pessoais, tais como expropriação dos seus bens, utilização indevida das suas contas bancárias, conclusão de empréstimos em seu nome, alteração do seu estado civil ou usurpação da sua identidade. Sente-se indignada com a «grande intrusão no sistema de informação da NAP» e sente que o Estado não a protegeu. Receia ser chantageada, agredida ou raptada.

9 A NAP considerou a alegação infundada. VB não tinha pedido informações à NAP sobre a questão de saber quais tinham sido exatamente os dados pessoais aos se tinha tido acesso.

10 Depois de os dados terem sido acedidos, a NAP tinha tomado medidas imediatas para proteger os direitos e os interesses dos cidadãos. Tinham sido realizadas reuniões com representantes e peritos dos serviços de segurança, a Notarialna kamara (Câmara dos Notários), a Agentsia po vpisvaniata (Agência do Registo), a Asotsiatsia na targovskite banki (Associação dos Bancos Comerciais), etc., a fim de coordenar as medidas para limitar as consequências do acesso. Foram criadas secções especiais sobre o ataque informático no website da NAP, onde foram publicadas informações atualizadas.

11 Segundo a NAP, não existe nenhuma ligação causal entre os pretensos danos imateriais e o acesso não autorizado aos dados pessoais. A NAP tinha sido vítima de um ataque intencional de terceiros que não são seus funcionários. Por conseguinte, não foi responsável pelos danos ocorridos.

12 A NAP argumentou que tinha tomado numerosas medidas. Concretamente, implementou sistemas de gestão de processos e sistemas de gestão para a segurança das informações, aprovou procedimentos que cumpriam as normas internacionais de qualidade ISSO 9000 e ISSO 9001, e aplicou políticas, regras, procedimentos, instruções e métodos de gestão da segurança das informações.

13 A NAP apresentou provas, nomeadamente vários documentos internos de janeiro de 2013 a maio de 2019, sobre o conteúdo, o procedimento para o estabelecimento, a manutenção e o acesso às bases de dados; a implementação de sistemas de gestão da segurança das informações; procedimentos de prevenção; regras internas sobre segurança das redes e das informações; instruções sobre o tratamento das informações; diretrizes sobre a proteção de dados pessoais; medidas e meios para a proteção de dados pessoais; métodos e procedimentos de avaliação dos riscos.

14 Por Sentença de 27 de novembro de 2020, o ASSG julgou a pretensão de VB infundada.

15 O ASSG argumentou que o acesso não autorizado à base de dados da NAP tinha tido lugar através de um «ataque de hacker» por parte de pessoas contra as quais tinha sido aberta uma investigação, que ainda não tinha terminado.

16 O resultado ilícito não permite concluir que o responsável pelo tratamento não tenha cumprido as suas obrigações de tomar as medidas técnicas e organizativas adequadas para assegurar a proteção da base de dados, de modo a que ninguém pudesse ter acesso à mesma de nenhum modo e através de nenhum meio.

17 O ASSG considerou que cabia ao recorrente demonstrar quais os atos (técnicos) que a NAP deveria ter efetivamente realizado mas que não realizou ou realizou de forma deficiente, levando assim ao acesso não autorizado e à divulgação de dados pessoais ou contribuindo para a ocorrência desse resultado.

18 Na opinião do ASSG, tendo em conta as provas apresentadas, não era possível constatar nenhuma falha por parte do responsável pelo tratamento. VB não tinha sofrido danos imateriais suscetíveis de ser compensados. O sofrimento psicológico, desencadeado pela notícia do acesso não autorizado às bases de dados de informação da NAP, é uma consequência mas não constitui um dano efetivamente sofrido em sentido jurídico. VB não tinha manifestado interesse em saber exatamente a quais dos seus dados pessoais se tinha acedido. Este comportamento não revela uma angústia emocional forte.

19 O ASSG constatou que a divulgação pública do acesso ilegal à base de dados da NAP não tinha afetado a vida de VB do ponto de vista da sua autoconfiança, da

sua autoestima, do seu trabalho, das suas relações ou do seu estado de saúde. Não há uma relação causal com as emoções negativas sofridas, uma vez que estas não são o resultado da conduta da NAP.

20 VB recorreu do acórdão do ASSG para o órgão jurisdicional de reenvio, o Varhoven administrativen saden (Supremo Tribunal Administrativo, a seguir VAS).

Argumentos essenciais das partes no processo principal

21 No recurso de cassação, VB alega que o ASSG repartiu incorretamente o ónus da prova no que respeita à demonstração de um facto negativo, ou seja, a não adoção pelo responsável pelo tratamento das medidas técnicas e organizativas adequadas.

22 VB considera que a aplicação de medidas eficazes se enquadra no âmbito dos poderes discricionários da NAP, de modo que não é possível determinar quais as obrigações específicas que os funcionários da NAP deveriam ter cumprido, mas não cumpriram. As provas apresentadas pela NAP não demonstraram que as medidas técnicas e organizativas tomadas eram adequadas.

23 VB sustenta que as preocupações sobre uma possível utilização indevida futura dos dados pessoais não constituem um dano hipotético, mas um dano imaterial efetivo, que deve ser ressarcido. Não é necessário provar danos imateriais comuns.

24 A NAP alega que o ASSG teve razão ao considerar que não tinha incorrido numa omissão na sua qualidade de responsável pelo tratamento, mas que tinha adotado numerosas medidas técnicas e organizativas para assegurar a proteção no tratamento de dados pessoais. A ocorrência real de danos não tinha sido provada. A preocupação e o receio de acontecimentos futuros não são suscetíveis de ressarcimento.

Apresentação sucinta da fundamentação do pedido de decisão prejudicial

25 Processos judiciais semelhantes contra a NAP terminaram com resultados contraditórios em primeira instância. As ações foram julgadas improcedentes ou procedentes, no todo ou em parte. A legislação foi interpretada e aplicada de forma não coerente em relação a todos os elementos da responsabilidade do responsável pelo tratamento.

26 Segundo o VAS, os elementos constitutivos da responsabilidade ao abrigo do artigo 82.° do regulamento são: i) uma violação do regulamento pelo responsável pelo tratamento; ii) danos materiais ou imateriais sofridos pela pessoa em causa; e iii) um nexo de causalidade entre os danos sofridos e a violação específica.

Quanto à primeira questão

27 Nos termos do artigo 24.°, n.° 1, do regulamento, 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 regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

28 O artigo 32.° do regulamento estabelece as obrigações do responsável pelo tratamento em relação à segurança do tratamento, relevantes para desencadear a sua responsabilidade por força do artigo 24.°, enumerando os critérios segundo os quais devem ser aplicadas as medidas técnicas e organizativas adequadas para assegurar um nível de proteção adequado ao risco. Tais critérios incluem «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».

29 O Regulamento 2016/679 não define o conceito de «medidas técnicas e organizativas adequadas». No considerando 74 indica-se que 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 regulamento, incluindo a eficácia das medidas.

30 O que precede leva a concluir que o responsável pelo tratamento deve efetuar uma avaliação de risco de acordo com os critérios estabelecidos no artigo 32.° do Regulamento 2016/679, com base na qual deve adotar medidas técnicas e organizativas adequadas ao nível de proteção dos dados pessoais exigido e proporcionadas ao risco. Ao implementar medidas técnicas e organizativas adequadas, o responsável pelo tratamento assegura o tratamento dos dados pessoais em conformidade com o Regulamento 2016/679.

31 Decorre destas disposições que a escolha das medidas técnicas e organizativas adequadas é uma questão de conveniência. Contudo, a avaliação da conveniência pelo responsável pelo tratamento não está sujeita a fiscalização jurisdicional, uma vez que a verificação efetuada pelo tribunal é uma fiscalização da legalidade. Ao mesmo tempo, quando existe uma margem de discricionariedade quanto à escolha das medidas técnicas e organizativas, o tratamento de dados pessoais deve ser efetuado no âmbito do Regulamento 2016/679 e em conformidade com o objetivo de salvaguardar o direito fundamental à proteção dos dados pessoais das pessoas.

32 À luz do acima exposto, o VAS pede ao Tribunal de Justiça que esclareça se os artigos 24.° e 32.° do Regulamento 2016/679 devem ser interpretados no sentido de que a mera ocorrência de um resultado ilícito sob a forma de divulgação ou acesso não autorizados a dados pessoais na aceção do artigo 4.°, ponto 12, do regulamento prova que as medidas técnicas e organizativas tomadas pelo responsável pelo tratamento não foram adequadas.

Segunda questão (em caso de resposta negativa à primeira questão)

33 Uma vez que a seleção e a aplicação de medidas técnicas e organizativas são deixadas à apreciação subjetiva do responsável pelo tratamento e são da sua competência, segundo o VAS, a questão que se coloca é saber 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 e cumprem o disposto nos artigos 24.° e 32.° do Regulamento 2016/679.

34 O VAS tem dúvidas sobre a questão de saber se é suficiente que o tribunal determine o modo como o responsável pelo tratamento cumpriu as suas obrigações decorrentes das disposições acima mencionadas, ou se deve examinar a substância das medidas técnicas e organizativas tomadas e implementadas, que, no entanto, são mencionadas no regulamento a título meramente exemplificativo e são implementadas em função da sua oportunidade.

Terceira questão (em caso de resposta negativa à primeira questão)

35 Por força do artigo 5.°, n.° 2, do Regulamento 2016/679, o responsável pelo tratamento é responsável pelo cumprimento do disposto no n.° 1, relativo aos princípios em matéria de tratamento de dados pessoais, e tem de poder comprová-lo. O artigo 24.°, n.° 1, do regulamento obriga o responsável pelo tratamento a aplicar «as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o ([…]) regulamento».

36 O artigo 82.°, n.° 3, do Regulamento 2016/679 prevê que o responsável pelo tratamento ou o subcontratante fica isento da responsabilidade nos termos do n.° 2 «se provar que não é de modo algum responsável pelo evento que deu origem aos danos». Segundo o referido n.° 2, o responsável pelo tratamento é responsável pelos danos causados por um tratamento viole o regulamento.

37 Nos termos da legislação nacional, cada parte num processo judicial é obrigada a provar as circunstâncias em que se fundam os seus pedidos e contestações. Em processos análogos, os tribunais de primeira instância repartiram o ónus da prova de maneira diferente entre o recorrente e o recorrido.

38 No presente caso, a questão relevante é saber se o princípio da responsabilidade na aceção do artigo 5.°, n.° 2, em conjugação com o considerando 74 e com o artigo 24.°, n.° 1, do Regulamento 2016/679, deve ser interpretado no sentido de que inverte o ónus da prova e de que o responsável pelo tratamento contra o qual foi intentada uma ação de indemnização por violação do regulamento, enquanto demandado, tem a obrigação de provar que as medidas técnicas e organizativas por ele aplicadas são adequadas.

39 Além da questão do objeto e do alcance da fiscalização jurisdicional do cumprimento das obrigações decorrentes do regulamento, é igualmente necessário clarificar como e com base em que provas se deve verificar se todas as medidas técnicas e organizativas adequadas foram cumpridas e, em especial, se foram aplicadas.

40 No decurso do processo, a NAP apresentou provas relativas à garantia da proteção das redes de informação em conformidade com as normas especificadas nos documentos, mas não foi requerido um parecer técnico forense para determinar se as medidas técnicas e organizativas eram adequadas na aceção do regulamento. O VAS está consciente de que um responsável pelo tratamento como a NAP é obrigado a aplicar medidas organizativas, tecnológicas e técnicas de segurança das redes e das informações que sejam proporcionadas às ameaças colocadas pela criminalidade informática, a fim de minimizar o risco da sua concretização. Contudo, o acesso de peritos forenses em qualquer processo cuja base jurídica seja o artigo 82.° do regulamento poderá acarretar novas consequências negativas para a proteção dos dados pessoais.

41 Tendo em conta o estado da técnica, as normas existentes para a proteção dos sistemas de redes de informação e o acesso não autorizado através de um «ataque de hacker» por pessoas externas à administração do responsável pelo tratamento, o VAS interroga-se se a obtenção de um parecer técnico forense pelo tribunal pode ser considerada um meio de prova necessário e suficiente para determinar se as medidas técnicas e organizativas tomadas e aplicadas foram adequadas para assegurar a proteção dos dados pessoais.

Quanto à quarta questão

42 Como responsável pelo tratamento envolvido numa operação de tratamento, a NAP é responsável, mas pode ficar isenta de responsabilidade ao abrigo do artigo 82.°, n.° 3, do Regulamento 2016/679, se provar que não é de modo algum responsável pelo evento que deu origem aos danos.

43 É indiscutível no presente processo que o acesso aos dados pessoais teve lugar por meio de um «ataque de hacker» contra a NAP. Em contrapartida, o acesso não autorizado e a divulgação de dados pessoais não ocorreu durante ou por ocasião do tratamento de dados pessoais por funcionários da NAP.

44 O VAS pede ao Tribunal de Justiça que esclareça se, no presente caso, é possível presumir que existe uma circunstância pela qual o responsável pelo tratamento não é de modo algum responsável e se, consequentemente, esta circunstância o isenta de responsabilidade.

Quinta questão

45 A pessoa em causa pede o ressarcimento de danos imateriais que se manifestaram sob a forma de preocupação, ansiedade, stress, sentimentos de insegurança e receios de uma futura utilização indevida dos seus dados pessoais das várias maneiras por ela descritas. Não há provas de que os dados pessoais de VB tenham sido utilizados indevidamente.

46 Como resulta dos considerandos 75 e 85 do Regulamento, a enumeração de exemplos de danos materiais ou imateriais tem em conta a natureza dos dados pessoais e os efeitos adversos sobre as pessoas em causa, e não apenas a sua perceção subjetiva.

47 O considerando 146 do regulamento estabelece o alcance da responsabilidade. Esta última abrange «os danos» causados a uma pessoa que possa ter sido vítima de um tratamento que viole o regulamento.

48 Na sequência de um acesso já ocorrido, os dados pessoais da pessoa em causa podem ser objeto de numerosas utilizações indevidas, de natureza imaterial e material, com consequências significativas. Tais abusos tornaram-se do conhecimento público, o que pode justificar um maior nível de preocupação para as pessoas vítima do «hacking». No presente caso, atendendo à falta de informação quanto à existência de um abuso já cometido, um abuso futuro é uma mera presunção, uma hipótese que apresenta um risco potencial mas incerto para os direitos do titular dos dados.

49 Pelas razões acima expostas, coloca-se a questão de saber se as perceções negativas da pessoa em causa neste contexto, ou seja, se o simples facto de ter surgido o risco de uma eventual futura utilização indevida dos dados pessoais, se enquadra no conceito de dano imaterial, que deve ser interpretado em sentido amplo, e dá direito a indemnização ao abrigo do artigo 82.°, n.° 1, em conjugação com o considerando 146, do regulamento.

50 Contudo, é possível que o artigo 82.°, n.° 1, em conjugação com o considerando 146, não possa ser interpretado no sentido de que qualquer sentimento negativo, receio ou ansiedade da pessoa em causa lhe dá direito a uma indemnização pelos danos imateriais sofridos, quando não tenha havido uma utilização ilícita anterior, como, por exemplo, uma expropriação de propriedade, a contração de empréstimos em nome da pessoa em causa ou a usurpação de identidade.