Coletânea da Jurisprudência

CONCLUSÕES DO ADVOGADO-GERAL
MANUEL CAMPOS SÁNCHEZ-BORDONA
apresentadas em 12 de maio de 2016 [1]

Processo C-582/14

Patrick Breyer
contra
Bundesrepublik Deutschland

[pedido de decisão prejudicial apresentado pelo Bundesgerichtshof (Supremo Tribunal Federal, Alemanha)]

«Tratamento de dados pessoais — Diretiva 95/46/CE — Artigos 2.°, alínea a), e 7.°, alínea f) — Conceito de 'dados pessoais' — Endereços IP — Conservação por um fornecedor de serviços relativos a meios de comunicação eletrónicos — Regulamentação nacional que não permite ter em conta o interesse legítimo do responsável pelo tratamento»

1. Um endereço do protocolo IP (a seguir «endereço IP») consiste numa sequência de números binários que é atribuída a um dispositivo (um computador, uma *tablet*, um telefone inteligente), o identifica e lhe permite aceder à rede de comunicações eletrónicas. Para se ligar à Internet, o dispositivo tem que utilizar a sequência numérica disponibilizada pelos fornecedores do serviço de acesso à Internet. O endereço IP é transmitido ao servidor onde está armazenada a página Internet objeto da consulta.

2. Em especial, os fornecedores de acesso à Internet (geralmente, as companhias telefónicas) atribuem aos seus clientes os chamados «endereços IP dinâmicos», de forma temporária, para cada ligação à Internet, e alteram-nos aquando de ligações posteriores. Essas mesmas empresas mantêm um registo, do qual consta o endereço IP que, a cada momento, se encontra atribuído a determinado dispositivo [2].

3. Os titulares dos sítios Internet aos quais o acesso é realizado por meio dos endereços IP dinâmicos também mantêm, habitualmente, registos, dos quais constam as páginas que foram consultadas, quando o foram e a partir de que endereço IP dinâmico. Tecnicamente, estes registos podem ser conservados sem limite de tempo após o termo da ligação à Internet efetuada por cada utilizador.

4. Por si só, um endereço IP dinâmico não basta para que o prestador de serviços identifique o utilizador da sua página Internet. No entanto, se combinar o endereço IP dinâmico com outras informações suplementares que estão na posse do fornecedor de acesso à Internet, poderá fazê-lo.

1 — Língua original: espanhol.

2 — O artigo 5.º da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE (JO L 105, p. 54), impõe, entre outras, a obrigação de conservar, para efeitos de investigação, deteção e punição de infrações graves, «a data e a hora do início (log-in) e do fim (log-off) da ligação ao serviço de acesso à internet [...], juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado».

5. No presente litígio, é debatida a questão de saber se os endereços IP dinâmicos são dados pessoais, na aceção do artigo 2.º, alínea a), da Diretiva 95/46/CE [3]. A resposta exige que se determine, previamente, que relevância tem, para este efeito, o facto de as informações suplementares necessárias para a identificação do utilizador não estarem na posse do titular do sítio Internet, mas na de um terceiro (concretamente, o fornecedor do serviço de acesso à Internet).

6. Trata-se de uma questão inédita para o Tribunal de Justiça, dado que, no n.º 51 do acórdão Scarlet Extended [4], declarou que os endereços IP são «dados pessoais protegidos, uma vez que permitem a identificação precisa dos referidos utilizadores», mas num contexto em que a recolha e identificação dos endereços IP eram realizadas por um fornecedor de acesso à Internet [5], e não por um fornecedor de conteúdos, como no presente caso.

7. Caso os endereços IP dinâmicos sejam dados pessoais para o prestador de serviços de Internet, importa examinar, em seguida, se o seu tratamento está abrangido pelo âmbito de aplicação da Diretiva 95/46.

8. É possível que, mesmo sendo dados pessoais, os referidos endereços não gozem da proteção decorrente da Diretiva 95/46, por exemplo no caso de a finalidade do seu tratamento ser a atuação penal contra os autores de eventuais ataques contra a página Internet. Nesta hipótese, a Diretiva 95/46 não é aplicável, por força do seu artigo 3.º, n.º 2, primeiro travessão.

9. Além disso, há que esclarecer a questão de saber se o prestador de serviços que regista os endereços IP dinâmicos quando um utilizador acede às suas páginas Internet (neste caso, a República Federal da Alemanha) age como poder público ou, antes, como particular.

10. Por último, caso a Diretiva 95/46 seja aplicável, há que precisar até que ponto o seu artigo 7.º, alínea f), é compatível com uma regulamentação nacional que restringe o alcance de uma das condições nele estabelecidas que o tratamento de dados pessoais possa ser considerado justificado.

I – **Quadro normativo**

A – *Direito da União*

11. O considerando 26 da Diretiva 95/46 tem a seguinte redação:

«(26) Considerando que os princípios da proteção devem aplicar-se a qualquer informação relativa a uma pessoa identificada ou identificável; que, para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios suscetíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa; que os princípios da proteção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável; que os códigos de conduta na aceção do artigo 27.º podem ser um instrumento útil para fornecer indicações sobre os meios através dos quais os dados podem ser tornados anónimos e conservados sob uma forma que já não permita a identificação da pessoa em causa».

3 — Diretiva do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281, p. 31).

4 — Acórdão de 24 de novembro de 2011 (C-70/10, EU:C:2011:771, n.º 51).

5 — O mesmo sucedia também no acórdão de 19 de abril de 2012, Bonnier Audio e o. (C-461/10, EU:C:2012:219, n.ºs 51 e 52).

12. De acordo com o artigo 1.º da Diretiva 95/46:

«1. Os Estados-Membros assegurarão, em conformidade com a presente diretiva, a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais.

2. Os Estados-Membros não podem restringir ou proibir a livre circulação de dados pessoais entre Estados-Membros por razões relativas à proteção assegurada por força do n.º 1».

13. Em conformidade com o artigo 2.º da Diretiva 95/46:

«Para efeitos da presente diretiva, entende-se por:

a) 'Dados pessoais', qualquer informação relativa a uma pessoa singular identificada ou identificável ('pessoa em causa'); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;

b) 'Tratamento de dados pessoais' ('tratamento'), qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;

[...]

d) 'Responsável pelo tratamento', a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do tratamento sejam determinadas por disposições legislativas ou regulamentares nacionais ou comunitárias, o responsável pelo tratamento ou os critérios específicos para a sua nomeação podem ser indicados pelo direito nacional ou comunitário;

[...]

f) 'Terceiro', a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que não a pessoa em causa, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão habilitadas a tratar dos dados;

[...]»

14. O artigo 3.º da Diretiva 95/46, sob o título «Âmbito de aplicação», dispõe:

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

2. A presente diretiva não se aplica ao tratamento de dados pessoais:

— efetuado no exercício de atividades não sujeitas à aplicação do direito comunitário, tais como as previstas nos títulos V e VI do Tratado da União Europeia, e, em qualquer caso, ao tratamento de dados que tenha como objeto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse tratamento disser respeito a questões de segurança do Estado), e as atividades do Estado no domínio do direito penal,

[...]»

15. O capítulo II da Diretiva 95/46, referente às «Condições gerais de licitude do tratamento de dados pessoais», inicia-se com o artigo 5.º, segundo o qual «[o]s Estados-Membros especificarão, dentro dos limites do disposto no presente capítulo, as condições em que é lícito o tratamento de dados pessoais».

16. De acordo com o artigo 6.º da Diretiva 95/46:

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

a) Objeto de um tratamento leal e lícito;

b) Recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-Membros estabeleçam garantias adequadas;

c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente;

d) Exatos e, se necessário, atualizados; devem ser tomadas todas as medidas razoáveis para assegurar que os dados inexatos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente, sejam apagados ou retificados;

e) Conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente. Os Estados-Membros estabelecerão garantias apropriadas para os dados pessoais conservados durante períodos mais longos do que o referido, para fins históricos, estatísticos ou científicos.

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

17. Segundo o artigo 7.º da Diretiva 95/46:

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

a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento; ou

b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa; ou

c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou

d) O tratamento for necessário para a proteção de interesses vitais da pessoa em causa; ou

e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ou

f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do n.º 1 do artigo 1.º»

18. Nos termos do artigo 13.º da Diretiva 95/46:

«1. Os Estados-Membros podem tomar medidas legislativas destinadas a restringir o alcance das obrigações e direitos referidos no n.º 1 do artigo 6.º, no artigo 10.º, no n.º 1 do artigo 11.º e nos artigos 12.° e 21.°, sempre que tal restrição constitua uma medida necessária à proteção:

a) Da segurança do Estado;

b) Da defesa;

c) Da segurança pública;

d) Da prevenção, investigação, deteção e repressão de infrações penais e de violações da deontologia das profissões regulamentadas;

e) De um interesse económico ou financeiro importante de um Estado-[M]embro ou da União Europeia, incluindo nos domínios monetário, orçamental ou fiscal;

f) De missões de controlo, de inspeção ou de regulamentação associadas, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas c), d) e e);

g) De pessoa em causa ou dos direitos e liberdades de outrem.

[...]»

B – *Direito nacional*

19. O § 12 da lei alemã das telecomunicações (Telemediengesetz, a seguir «TMG»)[6] dispõe:

«(1) O prestador de serviços só pode recolher e utilizar dados pessoais para efeitos de disponibilização de meios de comunicação eletrónicos no caso de a presente lei ou outra disposição que diga expressamente respeito a meios de comunicação eletrónicos o permitir ou no caso de o utilizador ter prestado o seu consentimento.

(2) O prestador de serviços só pode utilizar os dados pessoais recolhidos para efeitos de disponibilização de meios de comunicação eletrónicos para outras finalidades no caso de a presente lei ou outra disposição que diga expressamente respeito a meios de comunicação eletrónicos o permitir ou no caso de o utilizador ter prestado o seu consentimento.

(3) Salvo disposição em contrário, são aplicáveis as disposições sobre proteção de dados pessoais, mesmo que os dados não sejam tratados de forma automática.»

6 — Lei de 26 de fevereiro de 2007 (*BGBl* 2007 I, p. 179).

20. De acordo com o § 15 da TMG:

«(1) O prestador de serviços só pode recolher e utilizar dados pessoais de um utilizador, desde que tal se torne necessário para possibilitar, e faturar, a utilização do meio de comunicação eletrónico (dados de utilização). Constituem dados de utilização, nomeadamente:

1. As características que permitem a identificação do utilizador,

2. As informações sobre o início e o termo, bem como o volume, da respetiva utilização e

3. As informações sobre os meios de comunicação eletrónicos a que o utilizador acedeu.

(2) O prestador de serviços pode reunir os dados de utilização de um utilizador relacionados com a utilização de vários meios de comunicação eletrónicos, desde que tal seja necessário para efeitos de faturação com o utilizador.

[...]

(4) O prestador de serviços pode utilizar os dados de utilização após o termo do processo de utilização, desde que os mesmos sejam necessários para efeitos de faturação com o utilizador (dados de faturação). O prestador de serviços pode bloquear os dados para cumprimento de prazos de conservação legais, estatutários ou contratuais. [...]»

21. De acordo com o § 3, n.º 1, da lei federal alemã relativa à proteção de bases de dados (Bundesdatenschutzgesetz, a seguir «BDSG»)[7], «[d]ados pessoais são informações individualizadas sobre as circunstâncias pessoais ou materiais de uma pessoa singular identificada ou identificável ('pessoa em causa'). [...]».

II – **Matéria de facto**

22. P. Breyer intentou uma ação inibitória contra a República Federal da Alemanha por registo de endereços IP.

23. Vários organismos públicos alemães disponibilizam portais da Internet acessíveis ao público, nos quais prestam informações atualizadas. Para evitar ataques e permitir uma atuação penal contra os responsáveis pelos referidos ataques, na maioria destes portais, todos os acessos são gravados em ficheiros de registo. Aí conservam, após o termo do processo de utilização, o nome do ficheiro ou do sítio acedido, os termos inseridos nos campos de pesquisa, a data do acesso, a quantidade de dados transferida, a comunicação de que o acesso foi bem sucedido e o endereço IP do computador a partir do qual o mesmo foi realizado.

24. Com o seu pedido, P. Breyer, que consultou vários dos referidos sítios Internet, pretende que a República Federal da Alemanha seja condenada a abster-se de armazenar, ou de mandar armazenar por terceiros, o endereço IP do sistema de *host* a partir do qual acedeu aos sítios em causa, desde que o armazenamento não seja necessário para restabelecer a disponibilidade do meio de comunicação eletrónico em caso de avaria.

7 — Lei de 20 de dezembro de 1990 (*BGBl* 1990 I, p. 2954).

25. A ação intentada por P. Breyer foi julgada improcedente em primeira instância. No entanto, o seu recurso foi parcialmente deferido, tendo a República Federal da Alemanha sido condenada a abster-se de registar o endereço IP, após o termo de cada sessão. A ordem de inibição foi subordinada à condição de, no âmbito de uma sessão, o demandante ter fornecido os seus dados pessoais, incluindo sob a forma de um endereço de correio eletrónico, e o armazenamento não ser necessário para restabelecer a disponibilidade do meio de comunicação eletrónico.

III – **Pedido de decisão prejudicial submetido**

26. Tendo ambas as partes interposto recurso de «Revista», a sexta secção cível do Bundesgerichtshof (supremo tribunal federal alemão) submeteu ao Tribunal de Justiça o presente pedido de decisão prejudicial, que deu entrada na Secretaria em 17 de dezembro de 2014, com as seguintes questões:

«1) Deve o artigo 2.º, alínea a), da Diretiva 95/46/CE [...] ser interpretado no sentido de que um endereço do protocolo IP (endereço IP), armazenado por um prestador de serviços no contexto de um acesso ao seu sítio Internet, constitui para este um dado pessoal quando um terceiro (neste caso: o fornecedor de acesso à Internet) dispõe das informações suplementares necessárias para a identificação da pessoa em causa?

2) [Opõe-se o] artigo 7.º, alínea f), da diretiva relativa à proteção de dados [...] a uma disposição nacional nos termos da qual o prestador de serviços apenas pode recolher e utilizar dados pessoais de um utilizador sem o consentimento do mesmo na medida em que tal seja necessário para disponibilizar e faturar a utilização concreta do meio de comunicação eletrónico por parte desse utilizador e nos termos da qual a finalidade [que consiste em] garantir o funcionamento [...] do meio de comunicação eletrónico não pode justificar a sua utilização após o termo [da sessão]?»

27. Segundo explica o tribunal de reenvio, de acordo com o direito alemão, o recorrente poderia exigir da recorrida que se abstivesse de armazenar os endereços IP, se, à luz da legislação relativa à proteção de dados, a sua conservação constituísse uma ingerência inadmissível nos seus direitos gerais de personalidade, em especial, no seu «direito de autodeterminação em relação à informação» [§§ 1004, n.º 1, e 823, n.º 1, do Código Civil alemão (Bürgerliches Gesetzbuch), em conjugação com os artigos 1.º e 2.º da Lei Fundamental alemã (Grundgesetz)].

28. Assim seria, caso: a) o endereço IP — pelo menos associado ao período de acesso à Internet — pudesse ser qualificado como «dados pessoais» na aceção do artigo 2.º, alínea a), em conjugação com a última parte do considerando 26, ambos da Diretiva 95/46 ou do § 12, n.os 1 e 3, da TMG, em conjugação com o § 3, n.º 1, da BDSG, e, b) não se verificasse nenhum pressuposto de autorização na aceção do artigo 7.º, alínea f), da Diretiva 95/46 ou dos §§ 12, n.os 1 e 3, e 15, n.os 1 e 4, da TMG.

29. Segundo o Bundesgerichtshof, para a interpretação do direito nacional (§ 12, n.º 1, da TMG), é fundamental a questão de saber de que forma deve ser entendida a referência pessoal prevista no artigo 2.º, alínea a), da Diretiva 95/46.

30. Além disso, o tribunal de reenvio assinala que, dado que, segundo o § 15, n.º 1, da TMG, o prestador de serviços apenas pode recolher e utilizar os dados pessoais de um utilizador desde que tal se torne imprescindível para possibilitar, e faturar, a utilização do meio de comunicação eletrónico (dados de utilização) [8], a interpretação dessa disposição de direito interno está ligada à interpretação que for feita do artigo 7.º, alínea f), da Diretiva 95/46.

8 — Segundo o Bundesgerichtshof, os dados de utilização são constituídos pelas características que permitem a identificação do utilizador, as informações sobre o início, o termo e o volume da respetiva utilização, bem como pelas informações sobre os meios de comunicação eletrónicos a que o utilizador acedeu.

IV – **Tramitação processual no Tribunal de Justiça. Alegações das partes**

31. Apresentaram observações escritas os Governos alemão, austríaco e português, bem como a Comissão. Apenas esta instituição e P. Breyer compareceram na audiência realizada em 25 de fevereiro de 2016, na qual o Governo alemão declinou participar.

A – *Alegações das partes quanto à primeira questão*

32. Segundo P. Breyer, são dados pessoais, inclusive, os dados cuja reunião só é possível do ponto de vista teórico, ou seja, partindo da base de um perigo potencial abstrato, pouco importando se, na prática, essa reunião é efetivamente levada a cabo. Em seu entender, o facto de um organismo poder ser relativamente incapaz de identificar uma pessoa servindo-se do endereço IP não significa que não exista um perigo para essa pessoa. Além disso, na sua opinião, é relevante o facto de a Alemanha conservar os seus dados de IP para, sendo esse o caso, identificar eventuais ataques ou intentar ações penais, ao abrigo da autorização do § 113 da TMG, como aconteceu em diversas ocasiões.

33. Para o Governo alemão, deve ser dada resposta negativa à primeira questão. Em seu entender, os endereços IP dinâmicos não revelam uma pessoa «identificada», na aceção do artigo 2.º, alínea a), da Diretiva 95/46. Para determinar se os referidos endereços fornecem informações sobre uma pessoa «identificável», na aceção dessa mesma disposição, o exame da *identificabilidade* deve ser realizado com base num critério «relativo». Em seu entender, é o que resulta do considerando 26 da Diretiva 95/46, segundo o qual devem ser tidos em consideração apenas os meios suscetíveis de serem «razoavelmente» utilizados, seja pelo responsável pelo tratamento, seja por terceiro, para a identificação de uma pessoa. Esta especificação indicaria que o legislador da União não quis incluir no âmbito de aplicação da Diretiva 95/46 as situações nas quais é objetivamente possível uma identificação por parte de um terceiro.

34. O Governo alemão entende também que o conceito de «dados pessoais», na aceção do artigo 2.º, alínea a), da Diretiva 95/46, deve ser interpretado à luz da finalidade desta diretiva, a saber, assegurar o respeito dos direitos fundamentais. A necessidade de proteção das pessoas singulares pode ser vista de forma diferente, em função de quem está na posse dos dados e do facto de dispor, ou não, de meios para se servir deles para efeitos de identificação.

35. O Governo alemão sustenta que P. Breyer não é identificável com base nos endereços IP combinados com os outros dados que os fornecedores de conteúdos conservam. Para isso, seria necessário manipular a informação que está na posse dos fornecedores de acesso à Internet, os quais, na inexistência de uma base legal, não a podem disponibilizar aos fornecedores de conteúdos.

36. Para o Governo austríaco, pelo contrário, a resposta deve ser afirmativa. De acordo com o considerando 26 da Diretiva 95/46, para que uma pessoa seja considerada identificável não é necessário que todos os seus dados de identificação se encontrem em poder de uma única entidade. Assim, se um terceiro (como, por exemplo, o fornecedor de acesso à Internet) dispuser de meios para identificar o titular desse endereço, sem ter de empreender esforços excessivos, um endereço IP pode ser um dado pessoal.

37. O Governo português inclina-se igualmente para uma resposta afirmativa, por considerar que o endereço IP, combinado com a data da sessão de consulta, constitui um dado pessoal, na medida em que pode conduzir à identificação do utilizador por um organismo diferente daquele que guardou o endereço IP.

38. A Comissão também propõe uma resposta afirmativa, apoiando-se na solução adotada pelo Tribunal de Justiça no processo Scarlet Extended[9]. Para a Comissão, uma vez que armazenar os endereços IP serve precisamente para identificar os utilizadores em caso de ataques cibernéticos, o uso dos dados suplementares registados pelos fornecedores de acesso à Internet constitui um meio suscetível de ser «razoavelmente» utilizado, na aceção do considerando 26 da Diretiva 95/46. Em conclusão, no entender da Comissão, tanto o objetivo prosseguido por esta diretiva como os artigos 7.° e 8.° da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta») militam a favor de uma interpretação lata do artigo 2.º, alínea a), da Diretiva 95/46.

B – *Alegações das partes quanto à segunda questão*

39. P. Breyer entende que o artigo 7.º, alínea f), da Diretiva 95/46 constitui uma cláusula geral, cuja aplicação exige uma concretização. De acordo com a jurisprudência do Tribunal de Justiça, tratar-se-ia, portanto, de proceder à apreciação das circunstâncias do caso concreto e determinar se há grupos com um interesse legítimo, na aceção daquela disposição, sendo que, por conseguinte, para efeitos da aplicação desse artigo, não só está permitida, como é indispensável a previsão de regras especiais para esses grupos. Para P. Breyer, nesse caso, a regulamentação nacional é compatível com o artigo 7.º, alínea f), da Diretiva 95/46, na medida em que não existe um interesse do portal público na conservação de dados pessoais, ou porque o interesse em proteger o anonimato tem maior peso. Em seu entender, porém, uma conservação sistemática e de caráter pessoal dos dados não é compatível com uma sociedade democrática, nem necessária ou proporcionada para garantir o funcionamento dos meios eletrónicos, que é perfeitamente possível sem o registo destes dados pessoais, como demonstram os sítios Internet de alguns ministérios federais.

40. O Governo alemão sustenta que não há lugar para a abordagem da segunda questão, apresentada apenas no caso de a primeira vir a ter resposta afirmativa, o que, na sua opinião, não deve acontecer, pelas razões anteriormente expostas.

41. O Governo austríaco propõe responder que a Diretiva 95/46 não se opõe, de modo geral, à conservação de dados como os que estão em causa no processo principal, nos casos em que isso seja imprescindível para assegurar o bom funcionamento dos meios eletrónicos. Para esse governo, uma conservação limitada do endereço IP, para além do tempo de duração da consulta de uma página Internet, pode ser lícita, no que diz respeito à obrigação do responsável pelo tratamento dos dados pessoais de aplicar as medidas de proteção destes dados impostas no artigo 17.º, n.º 1, da Diretiva 95/46. A luta contra os ataques cibernéticos pode legitimar a análise dos dados relativos a ataques anteriores e que o acesso à página Internet seja negado a alguns endereços IP. A proporcionalidade da conservação de dados como os que estão em causa no processo principal, do ponto de vista do objetivo da garantia do bom funcionamento dos meios eletrónicos, deveria ser apreciada caso a caso, tendo em conta os princípios enunciados no artigo 6.º, n.º 1, da Diretiva 95/46.

42. O Governo português defende que o artigo 7.º, alínea f), da Diretiva 95/46 não se opõe às normas nacionais que estão em causa no processo principal, porque o legislador alemão já tinha procedido à ponderação, imposta nessa disposição, entre os interesses legítimos do responsável pelo tratamento dos dados pessoais, por um lado, e os direitos e liberdades dos titulares desses dados, por outro.

43. Para a Comissão, a regulamentação nacional que transpõe o artigo 7.º, alínea f), da Diretiva 95/46 deve definir os objetivos do tratamento de dados pessoais de forma a que sejam previsíveis para o particular afetado. Em seu entender, a regulamentação alemã não respeita esta exigência, ao prever, no § 15, n.º 1, da TMG, que é autorizada a conservação dos endereços IP, «desde que tal se torne necessário para possibilitar [...] a utilização do meio de comunicação eletrónico».

9 — Acórdão de 24 de novembro de 2011 (C-70/10, EU:C:2011:771, n.º 51).

44. A Comissão propõe, pois, que se responda à segunda questão no sentido de que se opõe à interpretação de uma disposição nacional segundo a qual uma autoridade pública que age como fornecedor de serviços pode recolher e utilizar os dados pessoais de um utilizador sem o seu consentimento, mesmo que o objetivo prosseguido seja assegurar o bom funcionamento geral do meio eletrónico, desde que a referida disposição nacional não estabeleça esse objetivo de modo suficientemente claro e preciso.

V – **Apreciação**

A – *Primeira questão*

1. Delimitação da questão submetida

45. Nos termos em que o Bundesgerichtshof a formulou, a primeira a primeira questão prejudicial visa esclarecer se um endereço IP, através do qual se acede a uma página Internet, constitui um dado pessoal [na aceção do artigo 2.º, alínea a), da Diretiva 95/46/CE] para o organismo público titular dessa página, caso o fornecedor de acesso à Internet esteja na posse de informações suplementares que permitam a identificação da pessoa em causa.

46. Com esta redação, a questão é suficientemente precisa para afastar, à partida, outras que poderiam ser suscitadas *in abstrato* a respeito da natureza jurídica dos endereços IP, no contexto da proteção de dados pessoais.

47. Em primeiro lugar, o Bundesgerichtshof faz exclusivamente referência aos «endereços IP dinâmicos», ou seja, os que são atribuídos de forma temporária a cada ligação à Internet e são alterados aquando de ligações posteriores. Distinguem-se, pois, dos «endereços IP fixos ou estáticos», que se caracterizam por serem imutáveis e permitirem a identificação permanente do dispositivo ligado à Internet.

48. Em segundo lugar, o tribunal de reenvio parte da presunção de que, no processo principal, o fornecedor da página Internet não está em condições de identificar, através do endereço IP dinâmico, as pessoas que visitam as suas páginas, nem está na posse, por si só, de informações suplementares que, combinados com aquele endereço IP, permitam essa identificação. O Bundesgerichtshof parece entender que, neste contexto, *para o fornecedor da página Internet*, o endereço IP dinâmico não é um dado pessoal, na aceção do artigo 2.º, alínea a), da Diretiva 95/46.

49. A dúvida do tribunal de reenvio é relativa à possibilidade de o endereço IP dinâmico ser qualificado como dado pessoal para o fornecedor da página Internet, *quando um terceiro dispõe de informações suplementares* que, combinadas com aquele endereço, permitem identificar as pessoas que consultam as suas páginas. Mas, e esta é uma observação mais relevante, o Bundesgerichtshof não se refere a qualquer terceiro que esteja na posse de informações suplementares, mas apenas ao fornecedor de acesso à Internet (portanto, exclui outros possíveis detentores desse tipo de dados).

50. Ficam, assim, à margem do debate, entre outros, os seguintes aspetos: a) se os endereços IP estáticos são dados de caráter pessoal, à luz da Diretiva 95/46 [10]; b) se os endereços IP dinâmicos são, sempre e em qualquer circunstância, dados pessoais, na aceção dessa diretiva e, por último, c) se a qualificação dos endereços IP dinâmicos como dados pessoais é inevitável sempre que exista um terceiro, independentemente de quem seja, capaz de os utilizar para a identificação dos utilizadores da Internet.

51. Trata-se, pois, unicamente, de decidir se um endereço IP dinâmico é um dado pessoal para o fornecedor de serviços de Internet, quando a empresa de comunicações eletrónicas que disponibiliza o acesso à Internet (o fornecedor de acesso) dispõe de informações suplementares que, combinados com aquele endereço, permitem a identificação das pessoas que acedem à página Internet gerida pelo primeiro.

2. Quanto ao mérito

52. A questão que este reenvio prejudicial suscita tem sido objeto de intenso debate, polarizado em duas correntes de opinião, na doutrina e na jurisprudência alemãs [11]. De acordo com uma das correntes (que opta por um critério «objetivo» ou «absoluto») um utilizador é identificável — e, por conseguinte, o endereço IP é um dado pessoal suscetível de proteção — quando, independentemente das capacidades e de meios do fornecedor do serviço de Internet, é possível identificá-lo, bastando, para isso, combinar esse endereço IP dinâmico com os dados fornecidos por um terceiro (por exemplo, o fornecedor de acesso à Internet).

53. Para os defensores da outra corrente (que propõem um critério «relativo»), para atribuir caráter pessoal ao endereço IP dinâmico não basta a possibilidade de dispor do auxílio de um terceiro na identificação final do utilizador. O que é relevante é a capacidade de, através dos seus próprios meios, quem tem acesso ao dado se servir do mesmo para identificar, desse modo, uma pessoa.

54. Independentemente do teor desta polémica no direito interno, a resposta do Tribunal de Justiça deve limitar-se à interpretação das disposições da Diretiva 95/46 a que tanto o tribunal de reenvio como as partes no processo fizeram referência, ou seja, o artigo 2.º, alínea a) [12], e o considerando 26 [13] da mesma.

10 — Problema que o Tribunal de Justiça decidiu, de forma definitiva, nos acórdãos de 24 de novembro de 2011, Scarlet Extended (C-70/10, EU:C:2011:771, n.º 51), e de 19 de abril de 2012, Bonnier Audio e o. (C-461/10, EU:C:2012:219). Nos n.ºs 51 e 52 desse último acórdão, o Tribunal de Justiça concluiu que a comunicação, «tendo em vista a sua identificação, do nome e do endereço de um [...] utilizador de Internet que usou o endereço de IP a partir do qual se presume que foram ilicitamente trocados ficheiros contendo obras protegidas [...] constitui um tratamento de dados pessoais na aceção do artigo 2.º, primeiro parágrafo, da Diretiva 2002/58, lido em conjugação com o artigo 2.º, alínea b), da Diretiva 95/46».

11 — Sobre as duas posições doutrinárias, podem ver-se, por exemplo, Schreibauer, M., en *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P., e von Lewinski, K. (eds.), Carl Heymanns Verlag/Wolters Kluwer, Colonia, 2014, 4.ª ed., § 11 Telemediengesetz (4 a 10). Nink, J. e Pohle, J.: «Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze», *Multimedia und Recht*, 9/2015, pp. 563 a 567. Heidrich, J. e Wegener, C.: «Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging», *Multimedia und Recht*, 8/2015, pp. 487 a 492. Leisterer, H.: «Die neuen Pflichten zur Netz— und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr», *Computer und Recht*, 10/2015, pp. 665 a 670.

12 — Transcrito no n.º 13.

13 — Transcrito no n.º 11.

55. Pelo simples facto de fornecerem informação sobre a data e a hora do acesso a uma página Internet a partir de um computador (ou de outro dispositivo), os endereços IP dinâmicos revelam certos padrões do comportamento de um utilizador na Internet e, por conseguinte, pressupõem uma potencial ingerência no direito à vida privada [14], consagrado no artigo 8.º da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais e no artigo 7.º da Carta, à luz dos quais, bem como do artigo 8.º da mesma, a Diretiva 95/46 deve ser interpretada [15]. De facto, as partes no litígio não põem em causa esta premissa, que também não é, em si mesma, objeto da questão prejudicial.

56. A pessoa à qual esses elementos dizem respeito não é uma «pessoa singular identificada». A data e a hora de uma ligação, bem como o seu número de origem, não revelam, direta ou imediatamente, quem é a pessoa singular à qual pertence o dispositivo a partir do qual a visita à página Internet é realizada, nem a identidade do utilizador que o usa (pode ser qualquer pessoa singular).

57. Contudo, na medida em que um endereço IP dinâmico ajuda a determinar — por si só, ou em conjunto com outros dados — quem é o proprietário do dispositivo utilizado para o acesso à página Internet, pode ser qualificado como uma informação relativa a uma «pessoa identificável» [16].

58. Segundo indica o Bundesgerichtshof, o endereço IP dinâmico não basta, por si só, para identificar o utilizador que acedeu a uma página Internet através dele. Se, pelo contrário, o fornecedor do serviço de Internet pudesse identificar o utilizador através do endereço IP dinâmico, tratar-se-ia, sem qualquer dúvida, de um dado pessoal, na aceção da Diretiva 95/46. Porém, não parece ser este o sentido da questão prejudicial, à qual está subjacente a ideia de que não é possível aos fornecedores de serviços de Internet envolvidos no litígio do processo principal identificar o utilizador exclusivamente com base no endereço IP dinâmico.

59. É pacífico que o endereço IP dinâmico, quando combinado com outros dados, permite a identificação «indireta» do utilizador. Será que a possibilidade de, eventualmente, existirem essas informações suplementares, associáveis ao endereço IP dinâmico, autoriza, por si só, que este seja qualificado como um dado pessoal à luz da Diretiva? Ter-se-á de determinar se, para esse efeito, a mera possibilidade, em abstrato, de dispor desses dados é suficiente ou se, pelo contrário, é necessário que os mesmos estejam à disposição de quem já sabe o endereço IP dinâmico, ou de um terceiro.

60. As partes centraram as suas observações na interpretação do considerando 26 da Diretiva 95/46, de cujo conteúdo destacam a expressão «meios suscetíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa». A questão submetida pelo tribunal de reenvio não diz respeito a informações suplementares detidas pelos fornecedores do serviço em causa no processo principal. Também não faz referência a qualquer terceiro que esteja na posse dessas informações suplementares (cujo cruzamento com o endereço IP dinâmico permita a identificação do utilizador), mas sim ao fornecedor de acesso à Internet.

14 — Como recordou o advogado-geral P. Cruz Villalón nas conclusões que apresentou no processo Scarlet Extended (C-70/10, EU:C:2011:255, n.º 76), e como também entende a Autoridade Europeia para a Proteção de Dados, nos seus Pareceres de 22 de fevereiro de 2010, sobre as negociações em curso na União Europeia sobre um Acordo Comercial Anticontrafação (ATA) (JO C 147, p. 1, n.º 24), e de 10 de maio de 2010, sobre a proposta de Diretiva do Parlamento Europeu e do Conselho relativa à luta contra o abuso e a exploração sexual de crianças e a pornografia infantil e que revoga a Decisão-Quadro 2004/68/JAI (JO C 323, p. 6, n.º 11).

15 — V., neste sentido, acórdão de 20 de maio de 2003, Österreichischer Rundfunk (C-465/00, C-138/01 e C-139/01, EU:C:2003:294, n.º 68), e conclusões apresentadas pela advogada-geral J. Kokott no processo Promusicae (C-275/06, EU:C:2007:454, n.ºs 51 e segs.).

16 — Cabe presumir que, salvo prova em contrário, essa pessoa é a que navegou na Internet e acedeu à página Internet em causa. No entanto, mesmo sem esta presunção, a informação acerca da data, da hora e do número de origem do acesso a uma página Internet, permitiria relacionar esse acesso com o proprietário do dispositivo e associá-lo indiretamente aos padrões do seu comportamento na Internet. A única exceção possível seria constituída pelos endereços IP atribuídos a computadores de estabelecimentos comerciais, como os *cibercafés*, cujos utilizadores anónimos não são identificáveis e sobre cujos proprietários o tráfego gerado no estabelecimento não fornece qualquer informação pessoal relevante. Esta é, aliás, a única exceção ao princípio segundo o qual os endereços IP são dados pessoais, admitida pelo Grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais, criado pela Diretiva 95/46 (o denominado «Grupo do artigo 29.º»). O seu Parecer 4/2007, de 20 de junho de 2007, sobre o conceito de dados pessoais, WP 136, pode ser lido em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

61. Neste caso, não é, pois, necessário que o Tribunal de Justiça examine todos os meios que a demandada no processo principal poderia «razoavelmente» utilizar para que os endereços IP dinâmicos de que dispõe possam ser qualificados como dados pessoais. Como o Bundesgerichtshof apenas faz referência a informações suplementares em poder de um terceiro, pode inferir-se: a) ou que a demandada não dispõe de informações suplementares próprias, que permitam a identificação do utilizador, b) ou que, se os tem à sua disposição, não está em condições de razoavelmente os utilizar com esse objetivo, enquanto responsável pelo seu tratamento, de acordo com o considerando 26 da Diretiva 95/46.

62. Ambas as hipóteses dependem de uma verificação de natureza factual, que é da competência exclusiva do órgão jurisdicional de reenvio. Caso o Bundesgerichtshof tivesse alguma dúvida quanto à capacidade de a demandada razoavelmente fazer uso de informações suplementares próprias, o Tribunal de Justiça poderia fornecer-lhe critérios gerais de interpretação da expressão «meios suscetíveis de serem razoavelmente utilizados [...] pelo responsável pelo tratamento». Não sendo esse o caso, em meu entender, seria deslocado o Tribunal de Justiça fixar agora critérios de interpretação que não são imprescindíveis ao tribunal de reenvio, e que o mesmo não solicitou.

63. Por conseguinte, o núcleo da questão submetida circunscreve-se a resolver se, para qualificar os endereços IP dinâmicos como dados pessoais, é relevante o facto de um terceiro muito específico — o fornecedor de acesso à Internet — dispor de informações suplementares que, combinadas com esses endereços, são suscetíveis de identificar o utilizador que visitou uma determinada página Internet.

64. Uma vez mais, impõe-se fazer referência ao considerando 26 da Diretiva 95/46. A expressão «meios suscetíveis de serem razoavelmente utilizados [...] *por qualquer outra pessoa*» [17] poderia dar azo a uma interpretação segundo a qual bastaria que um terceiro pudesse obter informações suplementares (suscetíveis de serem combinadas com um endereço IP dinâmico com vista a identificar uma pessoa) para se poder considerar que esse endereço constitui *eo ipso* um dado pessoal.

65. Na prática, essa interpretação maximalista levaria a qualificar como dado pessoal qualquer tipo de informação, por mais insuficiente que fosse, para, por si só, permitir a identificação de um utilizador. Nunca se poderá excluir, com absoluta certeza, que não haja um terceiro que esteja na posse de informações suplementares suscetíveis de serem combinadas com aquela informação e, consequentemente, capazes de revelar a identidade de uma pessoa.

66. Na minha opinião, a possibilidade de, num futuro mais ou menos imediato, o avanço dos meios técnicos facilitar, de forma considerável, o caminho de acesso a instrumentos de obtenção e tratamento da informação cada vez mais sofisticados justifica as cautelas com que se pretende antecipar a defesa da intimidade. Ao definir as categorias jurídicas relevantes no âmbito da proteção de dados, procurou-se que fossem incluídas hipóteses de comportamento suficientemente amplas e flexíveis para abranger qualquer caso imaginável [18].

67. No entanto, penso que essa preocupação — de resto, perfeitamente legítima — não pode levar a que se ignorem os termos da vontade normativa do legislador e que a interpretação sistemática do considerando 26 da Diretiva 95/46 se circunscreva aos «meios suscetíveis de serem razoavelmente utilizados» *por determinados terceiros*.

17 — O sublinhado é meu.

18 — Esta vocação cautelar e preventiva subjaz à posição mantida pelo Grupo do artigo 29.º, para o qual, como indiquei, se deve partir do princípio de que os endereços IP constituem dados pessoais, admitindo como única exceção a hipótese de o prestador do serviço estar em condições de determinar, com absoluta certeza, que os endereços correspondem a pessoas que não são identificáveis, como, por exemplo, os utilizadores de um *cibercafé*. V. nota 16 *in fine*.

68. Assim como o considerando 26 não se refere a quaisquer meios utilizáveis pelo responsável do tratamento (neste caso, o prestador de serviços de Internet), mas apenas aos que este possa «razoavelmente» utilizar, também se deve entender que o legislador se refere aos «terceiros» aos quais pode recorrer, *também de modo razoável*, um responsável pelo tratamento que pretenda obter as informações suplementares para a identificação. Assim não será quando o contacto com esses terceiros for, de facto, muito oneroso em termos humanos e económicos, inexequível na prática ou proibido por lei. De outro modo, como acima observei, seria praticamente impossível distinguir entre uns e outros meios, uma vez que seria sempre possível imaginar a eventualidade de um terceiro, mesmo inacessível para o prestador de serviços de Internet, poder dispor — atualmente ou no futuro — de informações suplementares pertinentes para a identificação de um utilizador.

69. Como acima indiquei, o terceiro a que o Bundesgerichtshof se refere é um fornecedor de acesso à Internet. Seguramente, é a este terceiro que é mais razoável pensar que o prestador de serviços se dirige a fim de obter as informações suplementares necessárias, caso pretenda identificar, da forma mais eficaz, prática e direta, o utilizador que acedeu à sua página Internet através do endereço IP dinâmico. Não é, de modo algum, um terceiro hipotético, desconhecido e inacessível, mas sim um protagonista, na rede da Internet, do qual se sabe seguramente que está na posse dos dados de que o prestador de serviços necessita para identificar um utilizador. Com efeito, como o tribunal de reenvio indica, é a este terceiro, em concreto, que a demandada no processo principal tem intenção de se dirigir para obter as informações suplementares que lhe são imprescindíveis.

70. O fornecedor de acesso à Internet é, tipicamente, o terceiro a que o considerando 26 da Diretiva 95/46 faz referência e ao qual o prestador de serviços do processo principal pode recorrer do modo mais «razoável». Contudo, resta esclarecer se a obtenção das informações suplementares que estão na posse desse terceiro pode ser qualificada de «razoavelmente» viável ou exequível.

71. O Governo alemão sustenta que, visto a informação que está na posse do fornecedor de acesso à Internet ser um dado pessoal, este não a pode ceder, pura e simplesmente, mas apenas em conformidade com a legislação que regula o tratamento destes dados [19].

72. Não há dúvida de que assim é, uma vez que, para utilizar essa informação, há que respeitar a legislação aplicável aos dados pessoais. Uma informação só pode ser «razoavelmente» obtida se forem cumpridas as condições que regulam o acesso a esse tipo de dados, sendo a primeira a possibilidade, legalmente prevista, da sua conservação e transmissão a outros. É certo que o fornecedor de acesso à Internet está autorizado a recusar a entrega dos dados solicitados, mas também é admissível o contrário. Tendo em conta o teor do considerando 26 da Diretiva 95/46, a possibilidade de transmissão de dados, perfeitamente «razoável», converte, por si só, o endereço IP dinâmico num dado pessoal para o prestador de serviços de Internet.

73. Trata-se de uma possibilidade exequível *dentro do quadro da lei* e, portanto, «razoável». Os meios de acesso razoáveis a que a Diretiva 95/46 faz referência devem ser, por definição, meios lícitos [20]. Como recorda o Governo alemão [21], esta é a premissa de que, naturalmente, parte o tribunal de reenvio. Assim se reduzem consideravelmente as vias de acesso juridicamente relevantes, uma vez que terão de ser, exclusivamente, as de natureza lícita. Mas enquanto estas existirem, por mais restritivas que possam ser na sua aplicação prática, constituem um «meio razoável», na aceção da Diretiva 95/46.

19 — N.os 40 e 45 das suas observações escritas.

20 — Neste contexto, é irrelevante que o acesso aos dados pessoais seja possível *de facto* através de uma violação da legislação em matéria de proteção de dados.

21 — N.os 47 e 48 das suas observações escritas.

74. Por conseguinte, considero que a primeira questão do Bundesgerichtshof, tal como este a formulou, tem resposta afirmativa. Do ponto de vista do fornecedor de serviços de Internet, o endereço IP dinâmico deve ser qualificado como um dado pessoal, tendo em conta a existência de um terceiro (o fornecedor de acesso à Internet) ao qual aquele pode razoavelmente recorrer para obter outras informações suplementares que, cruzadas com o mesmo, permitam a identificação de um utilizador.

75. Penso que a solução que defendo é reforçada pelo resultado a que a solução contrária conduziria. Se os endereços IP dinâmicos não constituíssem dados pessoais para o prestador de serviços na Internet, este poderia conservá-los de indefinidamente e solicitar, a qualquer momento, ao fornecedor de acesso à Internet as informações suplementares a fim de as conjugar com esses endereços e identificar o respetivo utilizador. Nestas circunstâncias, como o Governo alemão admite [22], o endereço IP dinâmico converter-se-ia num dado pessoal, uma vez que já disporia das informações suplementares válidas para identificar o utilizador, sendo aplicável, a este respeito, a legislação em matéria de proteção de dados.

76. Mas, tratar-se-ia de um dado cuja conservação só teria sido possível na medida em que, até então, não havia sido considerado um dado pessoal para o prestador de serviços. Ficaria, assim, nas mãos deste a qualificação jurídica do endereço IP dinâmico como dado pessoal, sujeita à eventualidade de, num momento futuro, o mesmo decidir utilizá-lo para identificar o utilizador através da sua combinação com as informações suplementares que deveria obter de um terceiro. No entanto, em meu entender, o que é determinante à luz da Diretiva 95/46 é a possibilidade — razoável — da existência de um terceiro «acessível», que disponha dos meios necessários para permitir a identificação de uma pessoa, e não que a possibilidade de recorrer a esse terceiro se concretize.

77. Poder-se-ia inclusivamente admitir, como fez o Governo alemão, que o endereço IP dinâmico só se converte num dado pessoal quando o fornecedor de acesso à Internet o recebe. Contudo, ter-se-ia então de reconhecer que essa qualificação revestia efeitos retroativos no que diz respeito ao prazo de conservação do endereço IP, e, consequentemente, considerá-la inexistente, caso já tivesse expirado o prazo durante o qual o dado poderia ter sido conservado se tivesse sido qualificado, desde o início, como dado pessoal. Nesta situação, produzir-se-ia um resultado contrário ao espírito da legislação relativa à proteção de dados pessoais. A razão que justifica a conservação apenas temporária destes dados seria defraudada perante um eventual atraso da relevância de uma qualidade que lhes é inerente desde o início: a sua potencialidade como meio de identificação — por si só, ou conjuntamente com outros dados — de uma pessoa singular. Também por esta razão, de pura economia, é mais razoável atribuir-lhe esse caráter desde o início.

78. Portanto, como primeira conclusão, entendo que o artigo 2.º, alínea a), da Diretiva 95/46 deve ser interpretado no sentido de que um endereço IP armazenado por um prestador de serviços no contexto de um acesso ao seu sítio Internet constitui para este um dado pessoal, na medida em que um fornecedor de acesso à Internet disponha das informações suplementares necessárias para a identificação da pessoa em causa.

B – *Segunda questão*

79. Com a segunda questão prejudicial, o Bundesgerichtshof pretende saber se o artigo 7.º, alínea f), da Diretiva 95/46 se opõe a uma regulamentação nacional que só admite a recolha e utilização dos dados pessoais de um utilizador sem o consentimento do mesmo na medida em que tal seja necessário para disponibilizar e faturar a utilização concreta do meio de comunicação eletrónico por parte desse utilizador, sem que a finalidade de garantir o funcionamento geral do meio de comunicação possa justificar a sua utilização após o termo do respetivo processo de utilização.

22 — N.º 36 das suas observações escritas.

80. A resposta deve ser precedida de um esclarecimento acerca da informação fornecida pelo Bundesgerichtshof segundo a qual os dados controvertidos são conservados para assegurar o bom funcionamento dos sítios Internet em causa no processo principal, possibilitando, se for esse o caso, uma atuação penal contra os responsáveis pelos ataques cibernéticos de que possam ser objeto.

81. Antes de mais, coloca-se, pois, a questão de saber se o tratamento dos endereços IP a que o despacho de reenvio faz alusão está incluído na exceção prevista no artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46 [23].

1. Quanto à aplicabilidade da Diretiva 95/46 ao tratamento dos dados controvertidos

82. Segundo parece, no processo principal, a República Federal da Alemanha age como mero prestador de serviços de Internet, ou seja, como particular (e, por conseguinte, *sine imperio*). Deste facto deduz-se que, em princípio, o tratamento dos dados objeto do presente litígio não está excluído do âmbito de aplicação da Diretiva 95/46.

83. Nas palavras utilizadas pelo Tribunal de Justiça, no acórdão Lindqvist [24], as atividades referidas no artigo 3.º, n.º 2, da Diretiva 95/46 «são, em todos os casos, atividades próprias aos Estados ou às autoridades estatais e alheias aos domínios de atividade dos particulares» [25]. Na medida em que o responsável pelo tratamento dos dados controvertidos seja uma pessoa que, apesar da sua qualidade de autoridade pública, age, de facto, como um sujeito privado, a Diretiva 95/46 é aplicável.

84. O tribunal de reenvio, ao destacar a finalidade principal que a Administração alemã prossegue com o armazenamento dos endereços IP dinâmicos, sublinha que pretende «assegurar e manter a segurança e o funcionamento dos seus meios de comunicação eletrónicos»; em especial, promover o «reconhecimento e [a] proteção contra os denominados ataques 'Denial-of-Service' ('de negação de serviço'), muito frequentes, no âmbito dos quais a infraestrutura de telecomunicações é paralisada de forma propositada e coordenada, através do envio de uma grande quantidade de pedidos de acesso a vários servidores *web*» [26]. A conservação dos endereços IP dinâmicos com este objetivo é comum a qualquer titular de sítios Internet de certa importância e não implica, direta ou indiretamente, o exercício de um poder público, pelo que a sua inclusão no âmbito da Diretiva 95/46 não se reveste de excessiva dificuldade.

85. No entanto, o Bundesgerichtshof assegura que a conservação dos endereços IP dinâmicos pelos prestadores de serviços em causa no processo principal corresponde também ao objetivo da atuação penal, quando necessária, contra os autores de eventuais ataques cibernéticos. É este objetivo suficiente para excluir o tratamento desses dados do âmbito de aplicação da Diretiva 95/46?

86. Na minha opinião, se, por «atuação penal», se entender o exercício, pelos prestadores de serviços demandados no processo principal, do *ius puniendi* do Estado, estaremos perante uma «atividade do Estado no domínio do direito penal» e, por conseguinte, perante uma das exceções previstas no artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46.

23 — Não está abrangido no âmbito de aplicação da Diretiva 95/46 o «tratamento de dados que tenha como objeto a segurança pública, a defesa, a segurança do Estado […] e *as atividades do Estado no domínio do direito penal*» (o sublinhado é meu).

24 — Acórdão de 6 de novembro de 2003 (C-101/01, EU:C:2003:596, n.º 43).

25 — V., nos mesmos termos, acórdão de 16 de dezembro de 2008, Satakunnan Markkinapörssi e Satamedia (C-73/07, EU:C:2008:727, n.º 41).

26 — N.º 36 do despacho de reenvio do pedido de decisão prejudicial.

87. Nestas circunstâncias, de acordo com a jurisprudência estabelecida pelo Tribunal de Justiça no processo Huber [27], o tratamento de dados pessoais pelos prestadores de serviço, a fim de garantir a segurança e o funcionamento técnico dos seus serviços de comunicação eletrónicos, está abrangido pelo âmbito de aplicação da Diretiva 95/46, ao passo que o tratamento de dados destinado à atividade do Estado no domínio do direito penal não está.

88. De igual modo, mesmo que a atuação penal, propiamente dita, não competisse à República Federal da Alemanha enquanto mero prestador de serviços desprovido de *jus imperium*, mas esta se limitasse, como qualquer particular, a transferir os endereços IP controvertidos para um órgão do Estado, com vista ao exercício de uma ação repressiva, o tratamento dos endereços IP dinâmicos teria igualmente por objeto uma atividade excluída do âmbito da Diretiva 95/46.

89. Isto resulta da jurisprudência estabelecida no processo Parlamento/Conselho e Comissão [28], na qual o Tribunal de Justiça declarou que o facto de determinados dados pessoais «terem sido recolhidos por operadores privados para fins comerciais e de serem eles a organizar a sua transferência para um Estado terceiro» não implica que a transferência em causa «não se enquadre no âmbito de aplicação» do artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46, quando a transferência tem por objeto as atividades do Estado no domínio penal, uma vez que, nesse caso, a mesma «[se] integra num quadro instituído pelos poderes públicos e que tem em vista a segurança pública» [29].

90. Pelo contrário, se, como penso e pode ser deduzido do despacho de reenvio, por «atuação penal» se deve entender a que é própria de um particular enquanto sujeito com legitimidade para requerer a atuação do *ius puniendi* do Estado através da ação correspondente, então, não é possível defender que o tratamento dos endereços IP dinâmicos tem por objeto a atividade do Estado no domínio penal, que está excluída do âmbito de aplicação da Diretiva 95/46.

91. Com efeito, a conservação e o registo desses dados serviriam como um meio de prova adicional em apoio do pedido, dirigido pelo titular da página Internet ao Estado, com vista a obter a repressão de um comportamento ilícito. Em conclusão, seria um instrumento de defesa, por via penal, dos direitos reconhecidos aos particulares (neste caso, um organismo público que age como sujeito de direito privado) pelo ordenamento jurídico. Desta perspetiva, não se distingue da iniciativa de qualquer outro fornecedor de serviço de Internet que pretenda a tutela do Estado em conformidade com as regras de exercício da ação penal estabelecidas no ordenamento jurídico.

92. Por conseguinte, na medida em que a Administração alemã se comporte como um prestador de serviços de Internet desprovido de poder público, o que compete ao tribunal de reenvio examinar, o tratamento que faça dos endereços IP dinâmicos, como dados pessoais, está abrangido pelo âmbito de aplicação da Diretiva 95/46.

2. Quanto ao mérito

93. O § 15, n.º 1, da TMG só autoriza a recolha e utilização de dados pessoais de um utilizador desde que tal se torne imprescindível para facultar, e faturar, uma utilização concreta do meio de comunicação eletrónico. Mais exatamente, o prestador de serviços só pode recolher e utilizar os chamados «dados de utilização», ou seja, os dados pessoais de um utilizador indispensáveis «para

27 — Acórdão de 16 de dezembro de 2008 (C-524/06, EU:C:2008:725, n.º 45).

28 — Acórdão de 30 de maio de 2006 (C-317/04 e C-318/04, EU:C:2006:346, n.os 54 a 59).

29 — *Ibidem*, n.º 59. Esse processo tinha por objeto dados pessoais cujo tratamento não era necessário para a prestação de serviços que constituía o negócio dos operadores privados em causa (transportadoras aéreas), mas que estes eram obrigados a transferir para as autoridades dos Estados Unidos, para impedir e combater o terrorismo.

possibilitar, e faturar, a utilização do meio de comunicação eletrónico». Estes dados devem ser eliminados quando o processo termina (ou seja, quando cessa a utilização concreta do meio de comunicação eletrónico), exceto quando devam ser gravados «para efeitos de faturação», de acordo com o disposto no n.º 4 do mesmo § 15 da TMG.

94. Uma vez terminada a ligação, o § 15 da TMG parece excluir que os dados de utilização possam ser armazenados por outros motivos, nem sequer para assegurar «a utilização do meio de comunicação eletrónico», em geral. Ao fazer referência, exclusivamente, à finalidade de faturação, como justificação para a conservação dos dados, aquela disposição da TMG poderia ser interpretada (embora a sua interpretação final seja da competência do órgão jurisdicional de reenvio) no sentido de que exige que os dados de utilização só sejam usados para possibilitar uma relação concreta, e sejam eliminados quando a mesma termine.

95. O artigo 7.º, alínea f), da Diretiva 95/46 [30] legitima o tratamento de dados pessoais em termos que qualificaria de mais generosos (para o responsável pelo tratamento) do que os utilizados na redação do § 15 da TMG. Neste aspeto, a norma alemã pode ser qualificada de mais restritiva do que a da União, uma vez que, em princípio, não contempla a prossecução de outros interesses legítimos que não sejam o interesse relacionado com a faturação do serviço, sendo que a República Federal da Alemanha, enquanto prestador de serviços na Internet, poderia ter também um interesse legítimo em assegurar o bom funcionamento das suas páginas Internet, para além de cada relação de utilização [31].

96. A doutrina adotada pelo Tribunal de Justiça no acórdão ASNEF e FECEMD [32] fornece as orientações pelas quais se deve pautar a resposta à segunda questão prejudicial. O Tribunal de Justiça declarou, então, que, do objetivo prosseguido pela Diretiva 95/46 «decorre [...] que o artigo 7.º da Diretiva 95/46 prevê uma lista exaustiva e taxativa dos casos em que um tratamento de dados pessoais pode ser considerado lícito» [33]. Daí que «os Estados-Membros não podem acrescentar novos princípios relativos à legitimação dos tratamentos de dados pessoais ao artigo 7.º da Diretiva 95/46 nem prever exigências suplementares que venham alterar o alcance de um dos seis princípios previstos nesse artigo» [34].

97. O § 15 da TMG não acrescenta qualquer requisito suplementar aos requisitos de licitude do tratamento de dados previstos no artigo 7.º da Diretiva 95/46 — ao contrário do que acontecia nos processos ASNEF e FECEMD [35] —, mas, se o mesmo for interpretado no sentido restritivo a que o tribunal de reenvio faz alusão, reduz o conteúdo da condição prevista na alínea f) da referida disposição: enquanto o legislador da União refere a prossecução de «[...] interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados», em geral, o § 15 da TMG atende unicamente à necessidade de «possibilitar, e faturar, a utilização [concreta] do meio de comunicação eletrónico».

98. À semelhança do que acontecia nos processos ASNEF e FECEMD [36], também no presente processo, uma medida nacional — de novo, caso fosse interpretada no sentido restritivo anteriormente descrito —, alteraria o alcance de um princípio previsto no artigo 7.º da Diretiva 95/46, mais do que se limitaria a especificá-lo, que é o único fim para o qual as autoridades de cada Estado-Membro dispõem de certa margem de apreciação, de acordo com o artigo 5.º da Diretiva 95/46.

30 — Transcrito no n.º 17.

31 — V. n.º 84. É certo que os titulares de páginas Internet têm um interesse legítimo em prevenir e combater as negações de serviço («Denial-of-Service»), a que o tribunal de reenvio faz referência, ou seja, os ataques massivos que, por vezes, são lançados de modo concertado contra alguns sítios Internet, a fim de os saturar e os tornar inoperantes.

32 — Acórdão de 24 de novembro de 2011 (C-468/10 e C-469/10, EU:C:2011:777).

33 — *Ibidem*, n.º 30.

34 — *Ibidem*, n.º 32.

35 — Nesse caso, a legislação nacional acrescentava às exigências previstas no artigo 7.º, alínea f), da Diretiva 95/46 a de que os dados objeto de tratamento constassem de fontes acessíveis ao público.

36 — Acórdão de 24 de novembro de 2011 (C-468/10 e C-469/10, EU:C:2011:777).

99. Com efeito, de acordo com esta última disposição, «[o]s Estados-[M]embros especificarão, dentro dos limites do disposto no presente capítulo [37], as condições em que é lícito o tratamento de dados pessoais». Contudo, como o Tribunal de Justiça declarou no processo ASNEF e FECEMD[38], «nos termos [da referida disposição], os Estados-Membros também não podem introduzir outros princípios relativos à legitimação de tratamentos de dados pessoais além dos enunciados no artigo 7.º dessa diretiva nem alterar, através de exigências suplementares, o alcance dos seis princípios previstos no referido artigo 7.º».

100. O § 15 da TMG reduziria substancialmente, em relação ao artigo 7.º, alínea f), da Diretiva 95/46, o perímetro dos interesses legítimos relevantes para a justificação do tratamento de dados, sem se limitar a esclarecê-lo ou a precisá-lo dentro das margens da autorização conferida pelo artigo 5.º dessa diretiva. Além disso, fá-lo-ia de uma forma categórica e absoluta, sem consentir que a proteção e a garantia da utilização geral do meio de comunicação eletrónico pudessem ser objeto de ponderação com «os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do n.º 1 do artigo 1.º» da Diretiva 95/46, de acordo com o disposto no artigo 7.º, alínea f), da mesma.

101. Em conclusão, à semelhança do que acontecia no processo ASNEF e FECEMD[39], o legislador federal alemão teria prescrito, «para [algumas categorias de dados pessoais], de forma definitiva o resultado da ponderação dos direitos e interesses opostos, sem permitir um resultado diferente devido a circunstâncias particulares de um caso concreto», de forma que «já não [estaria] em causa uma precisão na aceção do [...] artigo 5.º» da Diretiva 95/46.

102. Nestas circunstâncias, entendo que o Bundesgerichtshof tem a obrigação de interpretar a legislação nacional em conformidade com a Diretiva 95/46, o que implica que: a) entre as razões justificativas para o tratamento dos chamados «dados de utilização» possa ser incluído o interesse legítimo do prestador de serviços de telecomunicações em proteger a utilização geral dos mesmos e b) esse interesse do prestador do serviço possa ser ponderado, *ad casum*, com os interesses ou os direitos e liberdades fundamentais do utilizador, a fim de determinar qual deve ser protegido, de acordo com o artigo 1.º, n.º 1, da Diretiva 95/46[40].

103. Em meu entender, nada mais há a acrescentar quanto ao modo como, no caso que deu origem ao presente reenvio prejudicial, esta ponderação deva ser realizada. O Bundesgerichtshof nada pergunta sobre este aspeto, preocupando-se com a solução a dar a uma questão prévia a esse juízo de ponderação, ou seja, a questão de saber se esse juízo pode ser levado a cabo.

104. Por último, parece supérfluo assinalar que o tribunal de reenvio poderá ter em conta eventuais disposições legais que o Estado-Membro tenha adotado ao abrigo da autorização prevista no artigo 13.º, n.º 1, alínea d), da Diretiva 95/46, destinadas a restringir o alcance das obrigações e dos direitos referidos no artigo 6.º da mesma, sempre que for necessário à proteção, entre outros bens, «[d]a prevenção, investigação, deteção e repressão de infrações penais [...]». O tribunal de reenvio, seguramente consciente da existência de ambos os artigos, também não faz referência a este ponto.

37 — Capítulo II, intitulado «Condições gerais de licitude do tratamento de dados pessoais», que compreende os artigos 5.° a 21.° da Diretiva 95/46.

38 — Acórdão de 24 de novembro de 2011 (C-468/10 e C-469/10, EU:C:2011:777, n.º 36).

39 — *Ibidem*, n.º 47.

40 — Na audiência, a defesa de P. Breyer negou que o registo dos endereços IP dinâmicos fosse necessário para proteger o bom funcionamento dos serviços de Internet face a eventuais ataques. Penso que não é possível dar resposta em termos absolutos a esse problema, cuja solução, pelo contrário, deverá ser precedida de uma comparação, em cada caso concreto, entre o interesse do titular do sítio Internet e os direitos e interesses dos utilizadores.

105. Por conseguinte, proponho que se responda à segunda questão prejudicial no sentido de que o artigo 7.º, alínea f), da Diretiva 95/46 se opõe a uma norma nacional cuja interpretação impeça que um prestador de serviços possa recolher e tratar dados pessoais de um utilizador sem o consentimento do mesmo, com a finalidade de garantir o funcionamento geral do meio de comunicação eletrónico, após o termo do respetivo processo de utilização.

VI – **Conclusão**

106. À luz do que foi exposto, proponho que o Tribunal de Justiça responda às questões submetidas, nos seguintes termos:

«1) De acordo com o artigo 2.º, alínea a), da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, um endereço IP dinâmico por meio do qual um utilizador tenha acedido à página Internet de um fornecedor de um meio de comunicação eletrónico constitui para este um 'dado pessoal' na medida em que um fornecedor de acesso à Internet disponha de outras informações suplementares que, associadas ao endereço IP dinâmico, permitam a identificação do utilizador.

2) O artigo 7.º, alínea f), da Diretiva 95/46 deve ser interpretado no sentido de que, em princípio, o objetivo de garantir o funcionamento do meio de comunicação eletrónico pode ser considerado um interesse legítimo, cuja prossecução justifica o tratamento desse dado pessoal, desde que prevaleça sobre os interesses ou os direitos fundamentais da pessoa em causa. Uma disposição nacional que não permita tomar em consideração esse interesse legítimo é incompatível com o referido artigo.»