Edição provisória

CONCLUSÕES DO ADVOGADO-GERAL
MACIEJ SZPUNAR
apresentadas em 27 de outubro de 2022 (1)

Processo C-470/21

La Quadrature du Net,
Fédération des fournisseurs d'accès à Internet associatifs,
Franciliens.net,
French Data Network
contra
Premier ministre,
Ministère de la Culture

[pedido de decisão prejudicial apresentado pelo Conseil d'État (Conselho de Estado, em formação jurisdicional, França)]

«Reenvio prejudicial – Tratamento de dados pessoais e proteção da privacidade no setor das comunicações eletrónicas – Diretiva 2002/58/CE – Artigo 15.°, n.° 1 – Faculdade dos Estados-Membros de delimitarem o alcance de certos direitos e obrigações – Obrigação de controlo prévio por um órgão jurisdicional ou uma entidade administrativa independente dotada de um poder vinculativo – Dados relativos à identidade civil correspondentes a um endereço IP»

I. Introdução

1. A questão da conservação e do acesso a determinados dados de utilizadores da Internet é uma questão de atualidade permanente e é objeto de uma jurisprudência recente, mas já muito abundante, do Tribunal de Justiça.

2. O presente processo dá ao Tribunal de Justiça a oportunidade de abordar novamente esta questão, no contexto renovado da luta contra as violações dos direitos de propriedade intelectual cometidas exclusivamente em linha.

II. Quadro jurídico

A. Direito da União

3. Os considerandos 2, 6, 7, 11, 22, 26 e 30 da Diretiva 2002/58/CE (2) enunciam:

«(2) A presente diretiva visa assegurar o respeito dos direitos fundamentais e a observância dos princípios reconhecidos, em especial, pela [Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»)]. Visa, em especial, assegurar o pleno respeito pelos direitos consignados nos artigos 7.° e 8.° da citada carta.

[...]

(6) A Internet está a derrubar as tradicionais estruturas do mercado, proporcionando uma infraestrutura mundial para o fornecimento de uma vasta gama de serviços de comunicações eletrónicas. Os serviços de comunicações eletrónicas publicamente disponíveis através da Internet abrem novas possibilidades aos utilizadores, mas suscitam igualmente novos riscos quanto aos seus dados pessoais e à sua privacidade.

(7) No caso das redes de comunicações públicas, é necessário estabelecer disposições legislativas, regulamentares e técnicas específicas para a proteção dos direitos e liberdades fundamentais das pessoas singulares e dos interesses legítimos das pessoas coletivas, em especial no que respeita à capacidade crescente em termos de armazenamento e de processamento informático de dados relativos a assinantes e utilizadores.

[...]

(11) Tal como a [D]iretiva [95/46/CE (3)], a presente diretiva não trata questões relativas à proteção dos direitos e liberdades fundamentais relacionadas com atividades que não são reguladas pelo direito comunitário. Portanto, não altera o equilíbrio existente entre o direito dos indivíduos à privacidade e a possibilidade de os Estados-Membros tomarem medidas como as referidas no n.° 1 do artigo 15.° da presente diretiva, necessárias para a proteção da segurança pública, da defesa, da segurança do Estado (incluindo o bem-estar económico dos Estados quando as atividades digam respeito a questões de segurança do Estado) e a aplicação da legislação penal. Assim sendo, a presente diretiva não afeta a capacidade de os Estados-Membros intercetarem legalmente comunicações eletrónicas ou tomarem outras medidas, se necessário, para quaisquer desses objetivos e em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais[, assinada em Roma em 4 de novembro de 1950], segundo a interpretação da mesma na jurisprudência do Tribunal Europeu dos Direitos do Homem. Essas medidas devem ser adequadas, rigorosamente proporcionais ao objetivo a alcançar e necessárias numa sociedade democrática e devem estar sujeitas, além disso, a salvaguardas adequadas, em conformidade com a Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais.

[...]

(22) A proibição de armazenamento das comunicações e dos dados de tráfego a elas relativos por terceiros que não os utilizadores ou sem o seu consentimento não tem por objetivo proibir qualquer armazenamento automático, intermédio e transitório de informações, desde que esse armazenamento se efetue com o propósito exclusivo de realizar a transmissão através da rede de comunicação eletrónica e desde que as informações não sejam armazenadas por um período de tempo superior ao necessário para a transmissão e para fins de gestão de tráfego e que durante o período de armazenamento se encontre garantida a confidencialidade das informações. [...]

[...]

(26) Os dados relativos aos assinantes tratados em redes de comunicações eletrónicas para estabelecer ligações e para transmitir informações contêm informações sobre a vida privada das pessoas singulares e incidem no direito ao sigilo da sua correspondência ou incidem nos legítimos interesses das pessoas coletivas. Esses dados apenas podem ser armazenados na medida do necessário para a prestação do serviço, para efeitos de faturação e de pagamentos de interligação, e por um período limitado. Qualquer outro tratamento desses dados [...] só é permitido se o assinante tiver dado o seu acordo, com base nas informações exatas e completas que o prestador de serviços de comunicações eletrónicas publicamente disponíveis lhe tiver comunicado relativamente aos tipos de tratamento posterior que pretenda efetuar e sobre o direito do assinante de não dar ou retirar o seu consentimento a esse tratamento. [...]

[...]

(30) Os sistemas de fornecimento de redes e serviços de comunicações eletrónicas devem ser concebidos de modo a limitar ao mínimo o volume necessário de dados pessoais. [...]»

4. Nos termos do artigo 2.° dessa diretiva, sob a epígrafe «Definições»:

«[...]

São também aplicáveis as seguintes definições:

a) “Utilizador” é qualquer pessoa singular que utilize um serviço de comunicações eletrónicas publicamente disponível para fins privados ou comerciais, não sendo necessariamente assinante desse serviço;

b) “Dados de tráfego” são quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma;

c) “Dados de localização” quaisquer dados tratados numa rede de comunicações eletrónicas ou por um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público;

d) “Comunicação” é qualquer informação trocada ou enviada entre um número finito de partes, através de um serviço de comunicações eletrónicas publicamente disponível; não se incluem aqui as informações enviadas no âmbito de um serviço de difusão ao público em geral, através de uma rede de comunicações eletrónicas, exceto na medida em que a informação possa ser relacionada com o assinante ou utilizador identificável que recebe a informação;

[...]»

5. O artigo 3.° da referida diretiva, sob a epígrafe «Serviços abrangidos», dispõe:

«A presente diretiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas na Comunidade, nomeadamente nas redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação.»

6. O artigo 5.° da mesma diretiva, sob a epígrafe «Confidencialidade das comunicações», prevê:

«1. Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, exceto quando legalmente autorizados a fazê-lo, de acordo com o disposto no n.° 1 do artigo 15.° O presente número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade.

[...]

3. Os Estados-Membros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Diretiva [95/46], nomeadamente sobre os objetivos do processamento. Tal não impede o armazenamento técnico ou o acesso que tenha como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, ou que seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador.»

7. Nos termos do artigo 6.° da Diretiva 2002/58, sob a epígrafe «Dados de tráfego»:

«1. Sem prejuízo do disposto nos n.os 2, 3 e 5 do presente artigo e no n.° 1 do artigo 15.°, os dados de tráfego relativos a assinantes e utilizadores tratados e armazenados pelo fornecedor de uma rede pública de comunicações ou de um serviço de comunicações eletrónicas publicamente disponíveis devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação.

2. Podem ser tratados dados de tráfego necessários para efeitos de faturação dos assinantes e de pagamento de interligações. O referido tratamento é lícito apenas até [ao] final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado.

[...]»

8. O artigo 15.°, n.° 1, desta Diretiva 2002/58, sob a epígrafe «Aplicação de determinadas disposições da Diretiva [95/46]», enuncia:

«Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.° e 6.°, nos n.os 1 a 4 do artigo 8.° e no artigo 9.° da presente diretiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa

sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.° 1 do artigo 13.°, da Diretiva [95/46]. Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito [da União], incluindo os mencionados nos n.os 1 e 2 do artigo 6.° [TUE].»

B. Direito francês

1. Code de la propriété intellectuelle (Código da Propriedade Intelectual)

9. O artigo L. 331-12 do Código da Propriedade Intelectual, na versão aplicável ao litígio no processo principal (a seguir «CPI»), dispõe:

«A Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet [Alta Autoridade para a Divulgação das Obras e a Proteção dos Direitos na Internet (a seguir "Hadopi")] é uma autoridade pública independente.»

10. O artigo L. 331-13 do CPI prevê:

«A [Hadopi] deve assegurar:

[...]

2.° A defesa [das obras e de material protegido por um direito de autor ou por um direito conexo nas redes de comunicações eletrónicas] contra a violação desses direitos cometida nas redes de comunicações eletrónicas utilizadas na prestação de serviços de comunicação ao público em linha [...]»

11. Nos termos do artigo L. 331-15 deste código:

«A [Hadopi] é constituída por um órgão colegial e por uma Comissão de Proteção de Direitos. […].

[…]

No exercício das suas funções, os membros do órgão colegial e da Comissão de Proteção de Direitos não recebem instruções de nenhuma autoridade.»

12. O artigo L. 331-17 do referido código dispõe:

«Compete à Comissão de Proteção de Direitos tomar as medidas previstas no artigo L. 331-25.»

13. Nos termos do artigo L. 331-21 do mesmo código:

«Para o exercício, pela Comissão de Proteção de Direitos, das suas funções, a [Hadopi»] dispõe de agentes públicos ajuramentados autorizados pelo [seu] presidente em condições fixadas por decreto adotado em conformidade com o parecer do Conseil d'État (Conselho de Estado, em formação jurisdicional). [...]

Os membros da Comissão de Proteção de Direitos e os agentes mencionados no primeiro parágrafo recebem os pedidos submetidos à referida comissão nas condições previstas no artigo L. 331-24 e procedem à análise dos factos.

Podem, para a instrução do processo, obter todos os documentos, qualquer que seja o suporte, incluindo os dados conservados e tratados pelos operadores de comunicações eletrónicas nos termos do artigo L. 34-1 do Code des postes et des communications électroniques (Código das Comunicações Postais e Eletrónicas) e pelos prestadores mencionados nos n.os 1 e 2 do ponto I do artigo 6.° da Lei n.° 2004-575 de 21 de junho de 2004 para a Confiança na Economia Digital.

Podem também obter cópia dos documentos referidos no parágrafo anterior.

Podem, nomeadamente, obter dos operadores de comunicações eletrónicas a identidade, o endereço postal, o endereço de correio eletrónico e os dados telefónicos do assinante cujo acesso a serviços de comunicação ao público em linha foi utilizado para fins de reprodução, representação, disponibilização ou comunicação ao público de obras ou de material protegido sem autorização dos titulares dos direitos [...] quando esta última seja for necessária.»

14. O artigo L. 331-24 do CPI dispõe:

«A Comissão de Proteção de Direitos atua mediante requerimento dos agentes ajuramentados e autorizados [...] designados por:

– Organismos de defesa profissional regularmente constituídas;

– Organismos de gestão coletiva;

– Centre national du cinéma et de l'image animée (Centro Nacional do Cinema e da Imagem Animada).

A Comissão de Proteção de Direitos também pode atuar com base em informações que lhe sejam transmitidas pelo Procurador da República.

Não se pode pronunciar sobre factos ocorridos há mais de seis meses.»

15. Nos termos do artigo L. 331-25 deste código, disposição que rege o procedimento designado «Resposta graduada»:

«Quando lhe seja solicitado que se pronuncie sobre a prática de factos suscetíveis de configurar um incumprimento da obrigação definida no artigo L. 336-3 [do CPI], a Comissão de Proteção de Direitos pode enviar ao assinante [...] uma recomendação na qual lhe são indicadas as disposições do artigo L. 336-3, intimando-o a cumprir a obrigação aí estabelecida e advertindo-o das sanções em que incorre por força dos artigos L. 335-7 e L. 335-7-1. Nessa recomendação, o assinante é igualmente informado da oferta legal de conteúdos culturais em linha, sobre a existência de meios de segurança destinados a evitar os incumprimentos da obrigação definida no artigo L. 336-3, bem como sobre as ameaças à renovação da criação artística e à economia do setor da cultura decorrentes de práticas que não respeitam o direito de autor e os direitos conexos.

Em caso de prática reiterada, no prazo de seis meses a contar do envio da recomendação referida no primeiro parágrafo, dos factos suscetíveis de configurar um incumprimento da obrigação definida no artigo L. 336-3, a comissão pode enviar por escrito uma nova recomendação com as mesmas

informações que a anterior enviada por via eletrónica [...], a qual deve ser acompanhada de uma carta com aviso de receção ou qualquer outro meio adequado a fazer prova da data de receção dessa recomendação.

As recomendações enviadas com base no presente artigo devem mencionar a data e hora em que se verificou a prática dos factos suscetíveis de configurar um incumprimento da obrigação definida no artigo L. 336-3. Em contrapartida, não divulgam o conteúdo das obras ou de material protegido a que respeita esse incumprimento. Indicam os dados de contacto telefónico, postal e eletrónico para que o destinatário possa enviar, caso o pretenda, observações à Comissão de Proteção de Direitos e obter, mediante requerimento expresso nesse sentido, informação pormenorizada sobre o conteúdo das obras ou de material protegido a que respeita o incumprimento que lhe é imputado.»

16. O artigo L. 331-29 do referido código dispõe:

«É autorizada a criação, pela [Hadopi], de um tratamento automatizado de dados pessoais das pessoas sujeitas a um processo no âmbito da presente subsecção.

Este tratamento tem por finalidade a execução, pela Comissão de Proteção de Direitos, das medidas previstas na presente subsecção, de todos os atos processuais correspondentes e das modalidades de informação dos organismos de defesa profissional e dos organismos de gestão coletiva dos eventuais pedidos de intervenção junto da autoridade judiciária, bem como das notificações previstas no quinto parágrafo do artigo L. 335-7.

As disposições de aplicação do presente artigo são estabelecidas por decreto [...], que precisa, em especial:

– as categorias de dados registados e o seu prazo de conservação;

– os destinatários habilitados a receber a comunicação desses dados, nomeadamente as pessoas cuja atividade consiste em proporcionar um acesso a serviços de comunicação ao público em linha;

– as condições em que as pessoas interessadas podem exercer, junto da [Hadopi], o seu direito de acesso aos dados respetivos [...].»

17. O artigo R. 331-37 do mesmo código prevê:

«Os operadores de comunicações eletrónicas [...] e os prestadores [...] são obrigados a comunicar, através de interligação com o tratamento automatizado de dados pessoais referido no artigo L. 331-29 ou por recurso a um suporte de registo que garanta a sua integridade e a sua segurança, os dados pessoais e informações mencionados no n.° 2 do anexo ao [Decreto n.° 2010-236, de 5 de março de 2010, relativo ao tratamento automatizado de dados pessoais autorizado pelo artigo L. 331-29 do [CPI] denominado «Sistema de gestão das medidas de proteção das obras na Internet» (4)] [...] no prazo de oito dias após a transmissão pela Comissão de Proteção de Direitos dos dados técnicos necessários para identificar o assinante cujo acesso aos serviços de comunicação ao público em linha tenha sido utilizado para fins de reprodução, representação, disponibilização ou comunicação ao público de obras ou de material protegido sem a autorização dos titulares dos direitos [...] quando tal for necessário.

[...]»

18. O artigo R. 335-5 do CPI dispõe:

«I.- Constitui negligência grave, punida com a coima prevista para as contraordenações de quinto grau, o facto de, sem justificação legítima e estando preenchidas as condições previstas no ponto II, o titular de um acesso a serviços de comunicação ao público em linha:

1° Não ter instalado qualquer meio de segurança desse acesso;

2° Ter revelado falta de diligência na aplicação desse meio.

II.- O disposto no ponto I só é aplicável quando se encontrem cumulativamente preenchidas as seguintes duas condições:

1° Que, em aplicação do artigo L. 331-25 e nos termos previstos neste artigo, a Comissão de Proteção de Direitos tenha recomendado ao titular do acesso a implementação de um meio de segurança do seu acesso que permita evitar a renovação dessa utilização para fins de reprodução, representação, disponibilização ou comunicação ao público de obras ou material protegido por um direito de autor ou por um direito conexo sem a autorização dos titulares desses direitos [...] quando tal for necessário;

2° Que, no ano seguinte à apresentação da referida recomendação, esse acesso tenha sido novamente utilizado para os fins mencionados no n.° 1 do presente ponto II.»

19. O artigo L. 336-3 deste código enuncia:

«O titular do acesso a serviços de comunicação ao público em linha é obrigado a garantir que esse acesso não seja objeto de uma utilização para fins de reprodução, representação, disponibilização ou comunicação ao público de obras ou de material protegido por um direito de autor ou por um direito conexo sem autorização dos titulares [...] quando tal for necessário.

O incumprimento, por parte do titular do acesso, da obrigação definida no primeiro parágrafo não dá origem à responsabilidade penal do interessado [...].»

2. Decreto de 5 de março de 2010

20. O Decreto de 5 de março de 2010, na sua versão aplicável ao litígio no processo principal, prevê, no seu artigo 1.°:

«O tratamento de dados pessoais denominado “Sistema de gestão das medidas para a proteção das obras na Internet” tem por finalidade a execução, pela Comissão de Proteção de Direitos da [Hadopi]:

1.° Das medidas previstas no livro III da parte legislativa do [CPI] (título III, capítulo I, secção 3, subsecção 3) e no livro III da parte regulamentar do mesmo código (título III, capítulo I, secção 2, subsecção 2);

2.° Dos pedidos de consulta submetidos pelo Procurador da República relativos à prática de factos suscetíveis de configurar as infrações previstas nos artigos L. 335-2, L. 335-3, L. 335-4 e R. 335-5 do mesmo código, bem como da informação proveniente dos organismos de defesa profissional e dos organismos de gestão coletiva desses pedidos de consulta submetidos;

[...]»

21. O artigo 4.° deste decreto dispõe:

«I.- Têm acesso direto aos dados pessoais e às informações mencionadas no anexo do presente decreto os agentes públicos ajuramentados autorizados pelo presidente da [Hadopi] nos termos do artigo L. 331-21 do [CPI] e os membros da Comissão de Proteção de Direitos referida no artigo 1.°

II.- Os operadores de comunicações eletrónicas e os prestadores mencionados no n.° 2 do anexo do presente decreto são destinatários:

– dos dados técnicos necessários à identificação do assinante;

– das recomendações previstas no artigo L. 331-25 do [CPI] com vista ao respetivo envio por via eletrónica aos seus assinantes;

– dos elementos necessários à execução das sanções adicionais de suspensão do acesso a um serviço de comunicação ao público em linha comunicadas à Comissão de Proteção de Direitos pelo Procurador da República.

III.- Os organismos de defesa profissional e os organismos de gestão coletiva são destinatários de uma informação relativa ao pedido de consulta submetido pelo Procurador da República.

IV.- As autoridades judiciárias são destinatárias das atas de verificação da prática de factos suscetíveis de configurar as infrações previstas nos artigos L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 e R. 335-5 do [CPI].

A execução da sanção de suspensão é comunicada ao registo criminal automatizado.»

22. O anexo do Decreto de 5 de março de 2010 prevê:

«Os dados pessoais e informações registadas no tratamento denominado «Sistema de gestão das medidas para a proteção das obras na Internet» são os seguintes:

1 Dados pessoais e informações provenientes de organismos de defesa profissional regularmente constituídos, de organismos de gestão coletiva, do Centre national du cinéma et de l'image animée (Centro Nacional do Cinema e da Imagem Animada), bem como do Procurador da República:

Quanto aos factos suscetíveis de configurar um incumprimento da obrigação definida no artigo L. 336-3 do [CPI]:

Data e hora da prática dos factos;

Endereço IP dos assinantes em causa;

Protocolo descentralizado (*peer-to-peer*) utilizado;

Pseudónimo utilizado pelo assinante;

Informações relativas às obras ou material protegido objeto da prática dos factos;

Nome do ficheiro conforme consta do posto do assinante (se necessário);

Fornecedor de acesso à Internet com o qual foi contratado o acesso ou que forneceu o equipamento técnico IP.

[...]

2 Dados pessoais e informações relativas ao assinante recolhidas junto dos operadores de comunicações eletrónicas [...] e dos prestadores [...]:

Apelido e nome;

Endereço postal e endereços eletrónicos;

Dados telefónicos;

Endereço do equipamento telefónico do assinante;

Fornecedor de acesso à Internet, que utiliza os meios técnicos do fornecedor de acesso referido no n.° 1, com o qual o assinante celebrou o seu contrato; número de processo;

Data do início da suspensão do acesso a um serviço de comunicação ao público em linha.

[...]»

3. Code des postes et des télécommunications (Código das Comunicações Postais e Eletrónicas)

23. O artigo L. 34-1 do Code des postes et des communications électroniques (Código das Comunicações Postais e Eletrónicas), conforme alterado pelo artigo 17.° da Lei n.° 2021-998 de 30 de julho de 2021 (5) (a seguir «CPCE»), dispõe, no ponto II-A, que «os operadores de comunicações eletrónicas devem conservar:

1.° Para efeitos do processo penal, da prevenção de ameaças contra a segurança pública e da salvaguarda da segurança nacional, as informações relativas à identidade civil do utilizador, até ao final do prazo de cinco anos a contar do termo do seu contrato;

2.° Para as mesmas finalidades que as enunciadas no n.° 1 do presente ponto II-A, as outras informações fornecidas pelo utilizador no momento da subscrição de um contrato ou da criação de uma conta, bem como as informações relativas ao pagamento, até ao final do prazo de um ano a contar do termo do seu contrato ou do encerramento da sua conta;

3.° Para efeitos da luta contra a criminalidade e criminalidade grave, da prevenção de ameaças graves contra a segurança pública e da salvaguarda da segurança nacional, os dados técnicos que permitam identificar a fonte da ligação ou os dados relativos aos equipamentos terminais utilizados, até ao final do prazo de um ano a contar da ligação ou da utilização dos equipamentos terminais.»

III. Litígio no processo principal, questões prejudiciais e tramitação processual no Tribunal de Justiça

24. Por petição inicial de 12 de agosto de 2019 e dois articulados complementares de 12 de novembro de 2019 e de 6 de maio de 2021, a La Quadrature du Net, a Fédération des fournisseurs d'accès à Internet associatifs, a Franciliens.net e a French Data Network apresentaram no Conseil d'État (Conselho de Estado, em formação jurisdicional, França) um pedido de anulação da decisão de indeferimento tácito do Primeiro-Ministro sobre o pedido que tinham apresentado de revogação do Decreto de 5 de março de 2010 quando este decreto e as disposições que constituem a sua base jurídica não só lesariam excessivamente os direitos garantidos pela Constitution française (Constituição Francesa), mas seriam também contrários ao artigo 15.° da Diretiva 2002/58 e aos artigos 7.°, 8.°, 11.° e 52.° da Carta.

25. Em particular, os recorrentes no processo principal alegam que o Decreto de 5 de março de 2010 e as disposições que constituem a sua base jurídica autorizam o acesso a dados de ligação de forma desproporcionada relativamente a infrações aos direitos de autor cometidas na Internet e desprovidas de gravidade, sem que haja um controlo prévio por parte de um juiz ou de uma autoridade que dê garantias de independência e imparcialidade.

26. A este respeito, o órgão jurisdicional de reenvio começa por sublinha que o Tribunal de Justiça, no seu último Acórdão La Quadrature du Net e o. (6), declarou que o artigo 15.°, n.° 1, da Diretiva 2002/58, lido em conjugação com os artigos 7.°, 8.°, 11.°, e com o artigo 52.°, n.° 1, da Carta, não se opõe a medidas legislativas que prevejam, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública, uma conservação generalizada e indiferenciada *de dados relativos à identidade civil* dos utilizadores de meios de comunicações eletrónicos. Assim, a conservação desses dados seria possível, sem um determinado prazo, para efeitos de investigação, deteção e repressão de infrações penais no geral.

27. O órgão jurisdicional de reenvio deduz daqui que o fundamento invocado pelos recorrentes no processo principal relativo à ilegalidade do Decreto de 5 de março de 2010, por ter sido adotado no âmbito da luta contra infrações sem gravidade, só pode ser julgado improcedente.

28. O órgão jurisdicional de reenvio refere, em seguida, que o Tribunal de Justiça, no seu Acórdão Tele2 Sverige e Watson (7), declarou que o artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.°, 11.° e do artigo 52.°, n.° 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial o acesso das autoridades nacionais competentes aos dados conservados, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente.

29. Salienta que o Tribunal de Justiça, no Acórdão Tele2 (8), esclareceu que, para garantir, na prática, o pleno cumprimento dessas condições, é essencial que o acesso das autoridades nacionais competentes aos dados conservados seja, em princípio, salvo em casos de urgência devidamente justificados, sujeito à exigência de um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente, e que a decisão desse órgão jurisdicional ou dessa entidade ocorra na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, deteção ou ação penal.

30. O órgão jurisdicional de reenvio sublinha que o Tribunal de Justiça referiu essa exigência no Acórdão La Quadrature du Net e o. (9), quanto à recolha em tempo real de dados de ligação pelos serviços de informação, bem como no Acórdão Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas) (10), quanto ao acesso das autoridades nacionais aos dados de ligação.

31. Por último, o órgão jurisdicional de reenvio observa que, desde a sua criação em 2009, a Hadopi enviou mais de 12, 7 milhões de recomendações a titulares de assinaturas, em aplicação do procedimento de resposta graduada previsto no artigo L 331-25 do CPI, das quais 827 791 apenas durante o ano de 2019. Para este efeito, os agentes da Comissão de Proteção de Direitos da Hadopi devem poder recolher, todos os anos, um número considerável de dados relativos à identidade civil dos utilizadores em causa. Considera que, atendendo ao volume dessas recomendações, o facto de submeter essa recolha a um controlo prévio implica o risco de tornar impossível a execução das recomendações.

32. Nestas circunstâncias, o Conseil d'État (Conselho de Estado, em formação jurisdicional, França) decidiu suspender a instância e submeter ao Tribuna de Justiça as seguintes questões prejudiciais:

«1) Os dados [relativos à identidade civil] correspondentes a um endereço IP fazem parte [d]os dados relativos ao tráfego ou de localização sujeitos, em princípio, a um controlo prévio obrigatório por um órgão jurisdicional ou uma entidade administrativa independente dotada de um poder vinculativo?

2) Em caso de resposta afirmativa à primeira questão, e tendo em conta a reduzida sensibilidade dos dados relativos à identidade civil dos utilizadores, incluindo os seus dados telefónicos, a Diretiva [2002/58], [lida em conjugação] com a [Carta], deve ser interpretada no sentido de que se opõe a uma legislação nacional que prevê a recolha desses dados correspondentes ao endereço IP dos utilizadores por uma autoridade administrativa, sem controlo prévio por um órgão jurisdicional ou uma entidade administrativa independente com poderes vinculativos?

3) Em caso de resposta afirmativa à segunda questão, e tendo em conta a reduzida sensibilidade dos dados relativos à identidade civil, a circunstância de que só esses dados podem ser recolhidos, e apenas para as necessidades de prevenção de violação de obrigações definidas de forma precisa, limitativa e restritiva pelo direito nacional, e a circunstância de que um controlo sistemático do acesso aos dados de cada utilizador por um órgão jurisdicional ou por uma entidade administrativa terceira com poder vinculativo é suscetível de comprometer o cumprimento da missão de serviço público confiada à própria autoridade administrativa independente que procede à recolha, a Diretiva [2002/58] opõe-se a que esse controlo seja efetuado de acordo com modalidades adaptadas, como um controlo automatizado, no caso em apreço sob a supervisão de um serviço interno do organismo que dê garantias de independência e imparcialidade em relação aos agentes responsáveis por essa recolha?»

33. Os recorrentes no processo principal, os Governos francês, estónio, sueco e norueguês, bem como a Comissão Europeia apresentaram observações escritas. Essas mesmas partes, com exceção dos Governos estónio, dinamarquês e finlandês, estiveram representadas na audiência realizada em 5 de julho de 2022.

IV. Análise

A. Quanto à primeira e segunda questões prejudiciais

34. Com a sua primeira e segunda questões prejudiciais, que, na minha opinião, devem ser analisadas em conjunto, o órgão jurisdicional de reenvio pretende saber, em substância, se o artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta, deve ser interpretado no sentido de que se opõe a uma legislação nacional que permite o acesso, de uma autoridade administrativa encarregada da proteção dos direitos de autor e direitos conexos contra violações desses direitos cometidas na Internet, a dados relativos à identidade civil correspondentes a endereços IP, para que essa autoridade possa identificar os titulares desses endereços suspeitos de serem responsáveis pela prática dessas violações e possa

tomar, se necessário, medidas contra esses mesmos titulares, sem que esse acesso esteja sujeito a um controlo prévio por parte de um órgão jurisdicional ou uma entidade administrativa independente.

1. Delimitação das questões prejudiciais

a) Recolha prévia de endereços IP pelos organismos de titulares de direitos

35. Resulta da decisão de reenvio que o mecanismo de resposta graduada em causa no processo principal comporta dois tratamentos de dados sucessivos que consistem, o primeiro, na recolha prévia, pelos organismos de titulares de direitos, dos endereços IP nas redes descentralizadas (*peer-to-peer*) de infratores do direito de autor e, o segundo, na associação desses endereços IP à identidade civil das pessoas pela Hadopi na sequência da intervenção que lhe é solicitada, para efeitos do envio de uma recomendação às pessoas cujo acesso a serviços de comunicação ao público em linha foi utilizado em violação das normas relativas ao direito de autor.

36. A primeira e segunda questões prejudiciais têm apenas por objeto o segundo tratamento efetuado pela Hadopi.

37. Todavia, as recorrentes no processo principal alegam que o primeiro tratamento deve ser objeto de análise pelo Tribunal de Justiça, na medida em que, se esses endereços IP forem obtidos em violação das disposições da Diretiva 2002/58, a sua exploração no âmbito do segundo tratamento é necessariamente contrária a essas disposições.

38. Este raciocínio não é convincente. O artigo 3.°, n.° 1, da Diretiva 2002/58 limita o seu âmbito de aplicação ao «tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas». Ora, tal como especificou o Governo francês na audiência, os organismos de titulares de direitos obtêm os endereços IP em causa não através dos prestadores de serviços de comunicações eletrónicas, mas diretamente em linha, pela consulta dos dados disponíveis ao público em geral.

39. Assim, só se pode concluir que a recolha prévia dos endereços IP pelos organismos de titulares de direitos não é abrangida pelas disposições da Diretiva 2002/58 e, como refere a Comissão, pode, por conseguinte, ser analisada à luz das disposições do Regulamento (UE) 2016/679 (11). Deste modo, afigura-se-me que essa análise ultrapassa assim o âmbito das questões prejudiciais submetidas ao Tribunal de Justiça, tanto mais que o órgão jurisdicional de reenvio não apresenta pormenores relativos à recolha prévia que permitiriam ao Tribunal de Justiça dar-lhe uma resposta útil.

40. Neste contexto, a minha análise centrar-se-á na questão do acesso da Hadopi aos dados relativos à identidade civil correspondentes a um endereço IP.

b) Associação dos endereços IP e dos dados relativos à identidade civil

41. A primeira e segunda questões prejudiciais têm por objeto «os dados relativos à identidade civil correspondentes a um endereço IP», que são, segundo o órgão jurisdicional de reenvio, de reduzida sensibilidade. Esse órgão jurisdicional refere-se exclusivamente, na sua decisão, aos números do Acórdão La Quadrature du Net e o. relativos à conservação dos dados relativos à identidade civil.

42. É certo que a jurisprudência do Tribunal de Justiça efetua uma distinção entre o regime de conservação e de acesso dos endereços IP e o regime de conservação e de acesso dos dados relativos à identidade civil dos utilizadores dos meios de comunicações eletrónicos, sendo este segundo regime menos estrito do que o primeiro (12).

43. No entanto, afigura-se-me que, no presente caso, apesar da formulação dessas duas questões prejudiciais, não está em causa a questão do mero acesso aos dados relativos à identidade civil dos utilizadores dos meios de comunicações eletrónicos, mas sim a associação desses dados aos endereços IP de que a Hadopi dispõe na sequência da recolha e da transmissão destes pelos organismos de titulares de direitos. Com efeito, como salienta a Comissão, o acesso aos dados relativos à identidade civil pela Hadopi visa desbloquear um conjunto mais amplo de dados, designadamente os endereços IP e os extratos de ficheiros consultados, e permitir a sua exploração, não tendo os dados relativos à identidade civil e os endereços IP, isoladamente, interesse para as autoridades nacionais, uma vez que nem a identidade civil nem o endereço IP, por si sós, podem dar informações sobre as atividades em linha das pessoas singulares se não forem associados.

44. Daqui resulta que, a meu ver, há que entender a primeira e segunda questões prejudiciais como tendo por objeto não só os dados relativos à identidade civil dos utilizadores de um meio de comunicação eletrónico, mas também o acesso aos endereços IP que permitam identificar a fonte de uma ligação.

c) Conservação dos endereços IP pelos prestadores de serviços de comunicação

45. É certo que, como referem o Governo francês e a Comissão, as questões prejudiciais submetidas ao Tribunal de Justiça não têm por objeto, em termos formais, a conservação dos dados pelos prestadores de serviços de comunicações eletrónicas, mas apenas o acesso da Hadopi a dados relativos à identidade civil correspondentes a endereços IP.

46. Todavia, a questão do acesso da Hadopi a esses dados afigura-se efetivamente indissociável da questão, prévia, da sua conservação pelos prestadores de serviços de comunicações. Tal como sublinhou o Tribunal de Justiça, a conservação de dados só é feita, sendo caso disso, para tornar os dados acessíveis às autoridades nacionais competentes (13). Por outras palavras, a conservação e o acesso aos dados não podem ser considerados isoladamente, até mesmo porque o segundo está dependente da primeira.

47. É certo que o Tribunal de Justiça já analisou a compatibilidade com o artigo 15.°, n.° 1, da Diretiva 2002/58 de uma legislação nacional relativa ao mero acesso das autoridades nacionais competentes a determinados dados pessoais independentemente da questão da compatibilidade da conservação dos dados em causa com esta mesma disposição (14). Por conseguinte, pode responder-se às presentes questões prejudiciais sem considerar a questão de saber se os dados em causa foram conservados em conformidade com as disposições do direito da União.

48. No entanto, devo observar, antes de mais, que, no Acórdão Ministerio Fiscal (15), a análise efetuada pelo Tribunal de Justiça no que se refere à compatibilidade com o direito da União do acesso das autoridades nacionais a determinados dados pessoais responde estritamente aos mesmos princípios que a efetuada para avaliar a compatibilidade da conservação desses dados com o direito da União. Com efeito, o Tribunal de Justiça refere-se exclusivamente à jurisprudência desenvolvida quanto a este último aspeto para a aplicar à questão do acesso a dados pessoais. Por outras palavras, não sendo analisada a compatibilidade da conservação de determinados dados com o direito da União, esta análise reporta-se à fase da questão do acesso a esses dados, de modo que a compatibilidade desse acesso depende *in fine* da questão da conservação.

49. Em seguida, o Tribunal de Justiça indicou claramente que o acesso a dados pessoais só pode ser concedido se esses dados tiverem sido conservados pelos prestadores de serviços de comunicações eletrónicas em conformidade com o artigo 15.°, n.° 1, da Diretiva 2002/58 (16) e que o acesso a dados pessoais por entidades privadas para permitir instaurar o processo judicial, em instâncias cíveis, contra violações do direito de autor só é compatível com o direito da União na condição de esses dados serem conservados de forma compatível com esta disposição (17).

50. Por último, é jurisprudência constante do Tribunal de Justiça que o acesso a dados de tráfego e a dados de localização conservados pelos prestadores em aplicação de uma medida adotada ao abrigo do artigo 15.°, n.° 1, da Diretiva 2002/58, que deve ser efetuado no pleno respeito das condições resultantes da jurisprudência que interpretou a Diretiva 2002/58, apenas pode, em princípio, ser justificado pelo objetivo de interesse geral através do qual essa conservação foi imposta a esses prestadores (18). Por outras palavras, a compatibilidade com o direito da União do acesso das autoridades nacionais a determinados dados pessoais depende inteiramente da compatibilidade da conservação desses dados com o direito da União.

51. Daí resulta, na minha opinião, que a análise da compatibilidade com o direito da União de uma legislação nacional que preveja o acesso de uma autoridade nacional a dados pessoais pressupõe que tenha sido previamente demonstrada a compatibilidade da conservação desses mesmos dados com o direito da União.

52. Nestas circunstâncias, iniciarei a minha análise recordando a jurisprudência do Tribunal de Justiça relativa à questão da conservação dos endereços IP atribuídos à fonte de uma ligação, para demonstrar os respetivos limites e propor um quadro analítico adaptado da legislação em causa.

2. Jurisprudência do Tribunal de Justiça relativa à interpretação do artigo 15.°, n.° 1, da Diretiva 2002/58 quanto às medidas que visam a conservação dos endereços IP atribuídos à fonte de uma ligação

53. O artigo 5.°, n.° 1, da Diretiva 2002/58 consagra o princípio da confidencialidade tanto das comunicações eletrónicas como dos respetivos dados de tráfego e impõe, nomeadamente, que, em princípio, pessoas que não os utilizadores estejam proibidas de armazenar, sem o consentimento destes, essas comunicações e esses dados (19).

54. No que respeita ao tratamento e ao armazenamento pelos prestadores de serviços de comunicações eletrónicas dos dados de tráfego relativos a assinantes e utilizadores, a Diretiva 2002/58 prevê, no seu artigo 6.°, n.° 1, que esses dados devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação e precisa, no n.° 2 do mesmo artigo, que os dados de tráfego necessários para efeitos de faturação dos assinantes e de pagamento de interligações só podem ser tratados até final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado. No que se refere aos dados de localização para além dos dados de tráfego, o artigo 9.°, n.° 1, desta diretiva estabelece que esses dados só podem ser tratados em determinadas condições e depois serem tornados anónimos ou com o consentimento dos utilizadores ou assinantes (20).

55. Assim, ao adotar a Diretiva 2002/58, o legislador da União concretizou os direitos consagrados nos artigos 7.° e 8.° da Carta, pelo que os utilizadores de meios de comunicação eletrónicos têm o direito de esperar, em princípio, que, caso não tenham dado consentimento, as suas comunicações e respetivos dados permaneçam anónimos e não possam ser objeto de registo (21). Por conseguinte, essa diretiva não se limita a enquadrar o acesso a esses dados através de garantias destinadas a prevenir abusos, mas consagra também, em especial, o princípio da proibição do seu armazenamento por terceiros.

56. Nestas circunstâncias, na medida em que o artigo 15.°, n.° 1, da Diretiva 2002/58 permite aos Estados-Membros adotar medidas legislativas para «restringir o âmbito» dos direitos e obrigações previstos, nomeadamente, nos artigos 5.°, 6.° e 9.° desta diretiva, como os que decorrem dos princípios da confidencialidade das comunicações e da proibição do armazenamento dos respetivos dados, esta disposição enuncia uma exceção à regra geral prevista, nomeadamente, nestes artigos 5.°, 6.° e 9.° e deve, assim, em conformidade com jurisprudência constante, ser objeto de interpretação estrita. Por conseguinte, tal disposição não pode justificar que a derrogação à obrigação de princípio de garantir a confidencialidade das comunicações eletrónicas e dos respetivos dados e, em especial, a proibição de armazenar esses dados, prevista no artigo 5.° da referida diretiva, se converta na regra, sob pena de esvaziar esta última disposição do seu alcance (22).

57. Quanto aos objetivos suscetíveis de justificar uma limitação dos direitos e das obrigações previstos, nomeadamente, nos artigos 5.°, 6.° e 9.° da Diretiva 2002/58, o Tribunal de Justiça já declarou que a enumeração dos objetivos que figuram no artigo 15.°, n.° 1, primeira frase, dessa diretiva tem caráter taxativo, de modo que uma medida legislativa adotada ao abrigo desta disposição tem que responder efetiva e estritamente a um desses objetivos (23).

58. Além disso, resulta do artigo 15.°, n.° 1, terceira frase, da Diretiva 2002/58 que as medidas tomadas pelos Estados-Membros ao abrigo desta disposição devem respeitar os princípios gerais do direito da União, entre os quais figura o princípio da proporcionalidade, e assegurar o respeito dos direitos fundamentais garantidos pela Carta. A este respeito, o Tribunal de Justiça já declarou que a obrigação imposta por um Estado-Membro aos prestadores de serviços de comunicações eletrónicas, através de uma legislação nacional, de conservarem os dados de tráfego para, se for caso disso, os disponibilizarem às autoridades nacionais competentes levanta questões não apenas quanto ao respeito dos artigos 7.° e 8.° da Carta, relativos, respetivamente ao respeito pela vida privada e à proteção dos dados pessoais, mas igualmente do artigo 11.° da Carta, relativo à liberdade de expressão, que constitui um dos fundamentos essenciais de uma sociedade democrática e pluralista, fazendo parte dos valores nos quais, em conformidade com o artigo 2.° TUE, se baseia a União (24).

59. Não obstante, na medida em que o artigo 15.°, n.° 1, da Diretiva 2002/58 permite aos Estados-Membros restringir os direitos e obrigações previstos nos artigos 5.°, 6.°, e 9.° desta diretiva, esta disposição reflete a circunstância de os direitos consagrados nos artigos 7.°, 8.° e 11.° da Carta não serem prerrogativas absolutas, mas deverem ser tomados em consideração relativamente à sua função na sociedade. Com efeito, conforme resulta do seu artigo 52.°, n.° 1, a Carta admite restrições ao exercício desses direitos, desde que essas restrições estejam previstas por lei, respeitem o conteúdo essencial desses direitos e, na observância do princípio da proporcionalidade, sejam necessárias e correspondam efetivamente a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros. Assim, a interpretação do artigo 15.°, n.° 1, da Diretiva 2002/58, à luz da Carta, exige que se tenha igualmente em conta a importância dos objetivos de proteção da segurança nacional e de luta contra a criminalidade grave, contribuindo para a proteção dos direitos e liberdades de terceiros, e a dos direitos consagrados nos artigos 3.°, 4.°, 6.° e 7.° da Carta (25), de que podem resultar obrigações positivas que incumbem aos poderes públicos (26).

60. Face a estas diferentes obrigações positivas, há, portanto, que proceder a uma conciliação dos diferentes interesses legítimos e direitos em causa. Neste quadro, decorre dos próprios termos do artigo 15.°, n.° 1, primeira frase, da Diretiva 2002/58 que os Estados-Membros podem adotar uma medida derrogatória do princípio da confidencialidade quando tal medida seja «necessária, adequada e proporcionada numa sociedade democrática», indicando o considerando 11 desta diretiva, a este respeito, que uma medida desta natureza deve ser «rigorosamente» proporcionada ao objetivo a alcançar (27).

61. A este respeito, decorre da jurisprudência do Tribunal de Justiça que a possibilidade de os Estados-Membros justificarem uma limitação aos direitos e obrigações previstos, nomeadamente, nos artigos 5.°, 6.° e 9.° da Diretiva 2002/58 deve ser apreciada através da medição da gravidade da ingerência que tal limitação implica e da verificação de que a importância do objetivo de interesse geral prosseguido por tal limitação está relacionada com essa gravidade (28).

62. Refira-se, além disso, que o Tribunal de Justiça distingue, na sua jurisprudência, por um lado, as ingerências que resultam do acesso a dados que, enquanto tais, fornecem informações precisas sobre as comunicações em causa e, portanto, sobre a vida privada da pessoa, e para as quais o regime de conservação é estrito, e, por outro, as ingerências que resultam do acesso a esses dados, que só podem fornecer essas informações quando associados a outros dados, como os endereços IP (29).

63. Em especial, no que respeita aos endereços IP, o Tribunal de Justiça referiu que são gerados sem estarem ligados a uma comunicação específica e servem principalmente para identificar, por intermédio dos prestadores de serviços de comunicações eletrónicas, a pessoa singular proprietária de um equipamento terminal a partir do qual é efetuada uma comunicação através da Internet. Por conseguinte, desde que apenas sejam conservados os endereços IP da fonte da comunicação e não os do seu destinatário, esta categoria de dados tem um grau de sensibilidade menor que o dos outros dados de tráfego (30).

64. O Tribunal de Justiça sublinha ao mesmo tempo que, uma vez que os endereços IP podem ser utilizados para efetuar, nomeadamente, um rastreio exaustivo do percurso de navegação de um internauta e, por conseguinte, da sua atividade em linha, esses dados permitem estabelecer o perfil pormenorizado deste último e tirar conclusões precisas sobre a vida privada do utilizador. A conservação e a análise desses endereços IP constituem, deste modo, ingerências *graves* nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta e podem ter efeitos dissuasivos no exercício da liberdade de expressão garantida no artigo 11.° da mesma (31).

65. No entanto, segundo jurisprudência constante, para efeitos da necessária conciliação dos direitos e dos interesses legítimos em causa exigida pela jurisprudência, há que ter em conta o facto de, no caso de uma infração cometida em linha, o endereço IP poder constituir o único meio de investigação que permite a identificação da pessoa à qual esse endereço estava atribuído no momento da prática dessa infração (32).

66. Por conseguinte, o Tribunal de Justiça declara que uma medida legislativa que prevê a conservação generalizada e indiferenciada unicamente dos endereços IP atribuídos à fonte de uma ligação não se afigura, em princípio, contrária ao artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta, desde que essa possibilidade esteja sujeita ao estrito respeito das condições materiais e processuais que devem reger a utilização desses dados e entendendo-se que, atendendo ao caráter grave da ingerência que esta conservação comporta, só a luta contra a *criminalidade grave* e a prevenção das ameaças graves contra a segurança pública são suscetíveis, tal como a salvaguarda da segurança nacional, de justificar essa ingerência (33).

67. Por outro lado, o Tribunal de Justiça precisa que o período de conservação não pode exceder o estritamente necessário à luz do objetivo prosseguido e que uma medida desta natureza deve prever requisitos e garantias estritas quanto à exploração desses dados (34).

3. Limites da jurisprudência relativa à interpretação do artigo 15.°, n.° 1, da Diretiva 2002/58 no que respeita às medidas que visam a conservação dos endereços IP atribuídos à fonte de uma ligação

68. A solução encontrada pelo Tribunal de Justiça no que respeita às medidas nacionais que visam a conservação dos endereços IP atribuídos à fonte de uma ligação, interpretadas à luz do artigo 15.°, n.° 1, da Diretiva 2002/58, parece apresentar duas dificuldades principais.

a) Conciliação com a jurisprudência relativa à comunicação dos endereços IP atribuídos à fonte de uma ligação no âmbito de ações em matéria de proteção dos direitos de propriedade intelectual.

69. Em primeiro lugar, tal como evoquei nas minhas conclusões no processo M.I.C.M. (35), existe uma certa tensão entre esta linha de jurisprudência e a relativa à comunicação dos endereços IP no âmbito de ações em matéria de proteção dos direitos de propriedade intelectual aos titulares desses direitos, que põe o acento tónico na obrigação de os Estados-Membros assegurarem aos titulares dos direitos de propriedade intelectual possibilidades reais de obterem uma indemnização pelos prejuízos resultantes da violação desses direitos (36).

70. Com efeito, no que respeita a esta segunda linha de jurisprudência, o Tribunal de Justiça declara reiteradamente que o direito da União não se opõe a que os Estados-Membros estabeleçam uma obrigação de transmitir a entidades privadas dados pessoais para permitir instaurar o processo judicial, em instâncias cíveis, contra violações do direito de autor (37).

71. O Tribunal de Justiça salienta, a este respeito, que a possibilidade de os Estados-Membros preverem a obrigação de transmitir, no âmbito de uma ação cível, dados pessoais decorre, antes de mais, da possibilidade de prever essa transmissão no âmbito do processo por infrações penais (38), que foi, por sua vez, estendida aos processos civis.

72. Contudo, ao mesmo tempo, no que respeita aos endereços IP, o Tribunal de Justiça exige que esses dados só possam ser conservados no âmbito da luta contra a criminalidade grave e da prevenção das ameaças graves contra a segurança pública (39).

73. As tentativas de conciliação destas duas linhas de jurisprudência conduzem, na minha opinião, a resultados inadequados e não são convincentes.

74. Por um lado, contrariamente ao alegado pelo Governo francês na audiência, a luta contra as violações dos direitos de propriedade intelectual não pode integrar a luta contra a criminalidade grave. O conceito de «criminalidade grave» deve, a meu ver, ser objeto de uma interpretação autónoma. Não pode depender das conceções de cada Estado-Membro sob pena de permitir contornar os requisitos do artigo 15.°, n.° 1, da Diretiva 2002/58 consoante os Estados-Membros adotem ou não uma conceção extensiva da luta contra a criminalidade grave. Ora, como já referi, os interesses associados à proteção dos direitos de propriedade intelectual não podem confundir-se com os subjacentes à luta contra a criminalidade grave (40).

75. Por outro lado, admitir a transmissão de endereços IP aos titulares de direitos de propriedade intelectual no âmbito de processos que tenham por objeto a respetiva proteção, ainda que a sua conservação só se tenha tornado possível no âmbito da luta contra a criminalidade grave, estaria claramente em contradição com a jurisprudência do Tribunal de Justiça relativa à conservação dos dados de ligação e acabaria por privar de efeito útil os requisitos exigidos para a conservação desses dados, uma vez que, em todo o caso, o acesso aos mesmos seria possível com fundamentos diferentes.

76. Daqui resulta, na minha opinião, que a conservação dos endereços IP para efeitos da proteção de direitos de propriedade intelectual, bem como a respetiva comunicação aos titulares desses direitos no âmbito de procedimentos relativos a essa proteção, poderiam ser contrárias ao artigo 15.°, n.° 1, da Diretiva 2002/58, tal como foi interpretado na jurisprudência do Tribunal de Justiça. A obrigação de transmissão de dados pessoais a entidades privadas para permitir a instauração do processo judicial em instâncias cíveis, contra violações do direito de autor, e possibilitada pelo próprio Tribunal de Justiça, é, deste modo, simultaneamente neutralizada pelo papel da sua própria jurisprudência relativa à conservação dos endereços IP pelos prestadores de serviços de comunicações eletrónicas.

77. Essa solução não é, todavia, satisfatória, na medida em que põe em causa o equilíbrio entre os diferentes interesses em jogo que o Tribunal de Justiça procurou demonstrar, privando os titulares de direitos de propriedade intelectual do principal, senão único, meio de identificar os autores das violações em linha desses direitos. Esta consideração leva-me a expor a segunda dificuldade que pode resultar, sob o meu ponto de vista, da jurisprudência do Tribunal de Justiça, no que respeita a medidas nacionais que visam a conservação dos endereços IP atribuídos à fonte de uma ligação interpretada à luz do artigo 15.°, n.° 1, da Diretiva 2002/58.

b) Risco de impunidade sistémica das infrações cometidas exclusivamente em linha

78. Assim, em segundo lugar, considero que essa solução é uma fonte de dificuldades práticas. Como salienta o próprio Tribunal de Justiça, no caso de uma infração cometida exclusivamente em linha, o endereço IP pode constituir o único meio de investigação que permite a identificação da pessoa à qual esse endereço estava atribuído no momento da prática dessa infração.

79. Porém, afigura-se-me que este facto não foi inteiramente tido em consideração na ponderação dos interesses em causa. Embora o Tribunal de Justiça restrinja a possibilidade de conservação dos endereços IP ao âmbito da luta contra a criminalidade grave, ao mesmo tempo impede que esses dados possam ser conservados a fim de lutar contra infrações penais em geral, embora algumas destas infrações só possam ser prevenidas, detetadas ou punidas graças aos referidos dados.

80. Por outras palavras, a jurisprudência do Tribunal de Justiça pode levar a que as autoridades nacionais sejam privadas do único meio de identificação dos autores de infrações em linha que, todavia, não são abrangidas pela criminalidade grave, como é o caso das infrações aos direitos de propriedade intelectual. Daí resultaria, efetivamente, uma impunidade sistémica relativamente às infrações cometidas exclusivamente em linha, para além das simples infrações aos direitos de propriedade intelectual. Penso, nomeadamente, nos casos de difamação cometidos em linha. O direito da União prevê efetivamente medidas inibitórias contra os intermediários cujos serviços sejam utilizados para a prática desse tipo de infrações (41), mas poderia resultar da jurisprudência do Tribunal de Justiça que os próprios autores desses atos nunca fossem objeto de ação penal.

81. Sob pena de se admitir que uma série de infrações penais nunca possam ser sujeitas a ação penal, considero que o equilíbrio entre os diferentes interesses em causa deve ser objeto de uma nova análise.

82. Estas diferentes considerações levam-me a propor ao Tribunal de Justiça uma certa adaptação da jurisprudência relativa às medidas nacionais que visam a conservação dos endereços IP interpretadas à luz do artigo 15.°, n.° 1, da Diretiva 2002/58.

4. Proposta de adaptação da jurisprudência do Tribunal de Justiça relativa à interpretação do artigo 15.°, n.° 1, da Diretiva 2002/58 no que respeita às medidas que visam a conservação dos endereços IP atribuídos à fonte de uma ligação

83. Atendendo às considerações precedentes, considero que o artigo 15.°, n.° 1, da Diretiva 2002/58 deve ser interpretado no sentido de que não se opõe a medidas que preveem uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período de tempo limitado ao estritamente necessário, a fim de assegurar a prevenção, investigação, deteção e repressão de infrações penais em linha em relação às quais o endereço IP constitui *o único meio* de investigação que permite a identificação da pessoa à qual esse endereço estava atribuído no momento da prática da infração.

84. Devo sublinhar, a este respeito, que essa proposta não põe em causa, na minha opinião, o requisito da proporcionalidade exigido para a conservação dos dados, atendendo à gravidade da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta que a mesma implica (42). Pelo contrário, cumpre plenamente esse requisito.

85. Por um lado, a limitação aos direitos e obrigações previstos nos artigos 5.°, 6.° e 9.° da Diretiva 2002/58 constituída pela conservação dos endereços IP prossegue um objetivo de interesse geral relacionado com essa gravidade, a saber, a prevenção, investigação, deteção e repressão de infrações penais previstas em atos legislativos que, de outro modo, ficariam desprovidos de efeitos.

86. Por outro lado, essa limitação deve efetuar-se dentro dos limites do estritamente necessário. Com efeito, essa conservação é limitada a situações específicas, a saber, às infrações penais cometidas em linha e em relação às quais só é possível identificar o seu autor graças ao endereço IP que lhe é atribuído. Por outras palavras, não se trata de autorizar uma conservação generalizada e indiferenciada de dados sem outros requisitos, mas apenas de permitir a repressão de infrações penais bem determinadas e não como regra geral.

87. Todavia, embora o artigo 15.°, n.° 1, da Diretiva 2002/58 não se oponha a uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação para efeitos de assegurar a prevenção, investigação, deteção e repressão de infrações penais em linha em relação às quais o endereço IP constitui o único meio de investigação que permite a identificação da pessoa à qual esse endereço estava atribuído no momento da prática da infração, há que precisar ainda que, segundo a jurisprudência, essa possibilidade deve estar sujeita «ao estrito respeito das condições materiais e processuais *que devem reger a utilização desses dados*» (43). O Tribunal de Justiça especifica igualmente que essa medida «deve prever requisitos e garantias estritas quanto à *exploração desses dados*» (44).

88. Por outras palavras, como já sublinhei, a conservação dos dados e o acesso aos mesmos não podem ser considerados isoladamente. Nestas circunstâncias, embora a possibilidade de a Hadopi aceder aos endereços IP não seja à partida contrária ao artigo 15.°, n.° 1, da Diretiva 2002/58, na medida em que esses dados foram conservados em conformidade com os requisitos previstos nesta disposição, é ainda necessário, a fim de responder às questões prejudiciais submetidas ao Tribunal de Justiça, verificar se as condições de acesso aos endereços IP atribuídos à fonte de uma ligação pela Hadopi estão, por si sós, em conformidade com a referida disposição, designadamente quanto à eventual necessidade de um controlo prévio desse acesso por um órgão jurisdicional ou uma autoridade administrativa independente.

89. Tendo sido analisada a questão preliminar da conservação dos endereços IP atribuídos à fonte de uma ligação, procederei agora à análise do acesso da Hadopi a esses dados, à luz do artigo 15.°, n.° 1, da Diretiva 2002/58.

5. O acesso da Hadopi aos dados relativos à identidade civil correspondentes aos endereços IP

90. Resulta da jurisprudência do Tribunal de Justiça, no que se refere aos objetivos suscetíveis de justificar uma medida nacional que derrogue o princípio da confidencialidade das comunicações eletrónicas, que o acesso aos dados deve responder estrita e objetivamente a um desses objetivos, e que o objetivo prosseguido por essa medida deve estar relacionado com a gravidade da ingerência nos direitos fundamentais que esse acesso gera (45).

91. Além disso, conforme já exposto (46), o acesso a dados conservados pelos prestadores em aplicação de uma medida adotada ao abrigo do artigo 15.°, n.° 1, da Diretiva 2002/58 apenas pode, em princípio, ser justificado pelo objetivo de interesse geral através do qual essa conservação foi imposta a tais prestadores (47).

92. O Tribunal de Justiça declarou, assim, em conformidade com o princípio da proporcionalidade, que uma ingerência grave só pode ser justificada, em matéria de prevenção, investigação, deteção e repressão de infrações penais, por um objetivo de luta contra a criminalidade, devendo também este ser qualificado de grave (48).

93. A este respeito, saliento, contrariamente ao que alegam o Governo francês e a Comissão, que o acesso da Hadopi aos dados relativos à identidade civil correspondentes a um endereço IP configura efetivamente uma ingerência grave nos direitos fundamentais. Com efeito, não se trata apenas de aceder aos dados relativos à identidade civil, que são, por si sós, de reduzida sensibilidade, mas sim de associar esses dados a um conjunto mais amplo de dados, ou seja, o endereço IP, e ainda, como sublinham as recorrentes no processo principal, a um extrato do ficheiro carregado em violação dos direitos de autor.

Por conseguinte, trata-se de associar a identidade civil de uma pessoa ao conteúdo do ficheiro consultado e ao endereço IP por intermédio do qual foi feita essa consulta.

94. No entanto, tal como considero dever permitir-se também a conservação de dados que configura uma ingerência grave nos direitos fundamentais para efeitos de assegurar a prevenção, a investigação, a deteção e a repressão de infrações penais em linha em relação às quais o endereço IP constitui o único meio de investigação que permite a identificação da pessoa à qual esse endereço estava atribuído no momento da pratica da infração (49), considero que o acesso a esses dados deve ser tornado possível para prosseguir o mesmo objetivo, sob pena de se admitir a impunidade geral das infrações cometidas exclusivamente em linha.

95. Por conseguinte, o acesso da Hadopi aos dados relativos à identidade civil associados a um endereço IP afigura-se-me justificado pelo objetivo de interesse geral através do qual essa conservação foi imposta aos prestadores de serviços de comunicações eletrónicas.

96. A jurisprudência do Tribunal de Justiça precisa, todavia, que uma legislação nacional que regula o acesso das autoridades competentes a dados de tráfego e a dados de localização conservados não se pode limitar a exigir que o acesso responda à finalidade prosseguida por essa legislação, mas deve igualmente prever as condições materiais e processuais que regem o acesso das autoridades nacionais competentes aos dados em causa (50).

97. Em particular, o Tribunal de Justiça considera que, uma vez que um acesso generalizado a todos os dados conservados, independentemente de uma qualquer relação com o objetivo prosseguido, não pode ser considerado limitado ao estritamente necessário, a regulamentação nacional deve basear-se em critérios objetivos para definir as circunstâncias e as condições nas quais deve ser concedido às autoridades nacionais competentes o acesso aos dados dos utilizadores, de modo a verificar que o acesso só é concedido aos dados de pessoas suspeitas de planear, cometer ou terem cometido uma infração grave ou estarem envolvidas de uma maneira ou outra nessa infração (51).

98. Assim, segundo a jurisprudência, a fim de garantir, na prática, o pleno respeito destes requisitos, é essencial que o acesso das autoridades nacionais competentes aos dados conservados esteja, em princípio, sujeito a um controlo prévio, efetuado por um órgão jurisdicional ou por uma entidade administrativa independente (52).

99. Todavia, refira-se que o Tribunal de Justiça estabeleceu essa necessidade de um controlo prévio do acesso aos dados pessoais em circunstâncias específicas diferentes das do presente caso, que envolvam intromissões *especialmente graves* e na vida privada dos utilizadores de serviços de comunicações eletrónicas.

100. Com efeito, tratava-se, em cada um dos acórdãos que salientaram essa exigência, de medidas nacionais que autorizam o acesso ao conjunto dos dados de tráfego e à localização dos utilizadores relativos a todos os meios de comunicação eletrónica (53) ou, pelo menos, à telefonia fixa e móvel (54). Mais concretamente, estava em causa o acesso a um «conjunto de dados [...] suscetíveis de fornecer informações sobre as comunicações efetuadas por um utilizador de um meio de comunicação eletrónica ou sobre a localização dos equipamentos terminais por ele utilizados e de permitir tirar conclusões precisas sobre a sua vida privada» (55), de modo que a exigência de um controlo prévio do acesso a esses dados por um órgão jurisdicional ou uma entidade administrativa independente só existe, na minha opinião, nesse contexto.

101. Ora, por um lado, o acesso da Hadopi fica limitado à associação dos dados relativos à identidade civil ao endereço IP utilizado e ao ficheiro consultado num momento específico, sem que tal tenha como resultado permitir às autoridades competentes reconstituir o percurso de navegação em linha

do utilizador visado, nem, por conseguinte, tirar conclusões precisas sobre a sua vida privada para além do conhecimento do ficheiro específico consultado no momento da infração. Não se trata, portanto, de permitir o rastreio do conjunto das atividades em linha do utilizador em causa.

102. Por outro lado, esses dados dizem respeito apenas a dados de pessoas que, como foi constatado nas atas elaboradas pelos organismos de titulares de direitos, praticaram factos suscetíveis de configurar um incumprimento da obrigação prevista no artigo L.336-3 do CPI. O acesso da Hadopi aos dados relativos à identidade civil associados aos endereços IP é, assim, estritamente limitado ao necessário para alcançar o objetivo prosseguido, ou seja, permitir a prevenção, investigação, deteção e repressão de infrações penais em linha relativamente às quais o endereço IP constitui o único meio de investigação que permite a identificação da pessoa à qual esse endereço estava atribuído no momento da prática da infração, no qual se insere o mecanismo de resposta graduada.

103. Neste contexto, considero que o artigo 15.°, n.° 1, da Diretiva 2002/58 não impõe a existência de um controlo prévio, por um órgão jurisdicional ou uma entidade administrativa independente, do acesso da Hadopi aos dados relativos à identidade civil associados aos endereços IP dos utilizadores.

104. Quanto ao restante, refira-se, como sublinha o Governo francês, que o acesso da Hadopi a esses dados, se não estiver sujeito a um controlo prévio por um órgão jurisdicional ou uma entidade independente, não está, contudo, isento de controlo, uma vez que o ficheiro enviado pela Hadopi aos operadores de comunicações eletrónicas é elaborado diariamente por um agente ajuramentado com base nos pedidos de intervenção recebidos e validados, de forma aleatória por amostra, antes do seu aditamento ao ficheiro (56). Importa sobretudo observar que o procedimento de resposta graduada continua sujeito às disposições da Diretiva (UE) 2016/680 (57). A este título, as pessoas singulares visadas pela Hadopi beneficiam de um conjunto de garantias materiais e processuais previstas nesta diretiva. Estas englobam o direito de acesso, retificação e apagamento dos dados pessoais tratados pela Hadopi, bem como a possibilidade de apresentar uma reclamação a uma autoridade de controlo independente, eventualmente seguida de um recurso judicial intentado nos termos do direito comum (58).

105. Por conseguinte, proponho responder à primeira e segunda questões prejudiciais, que o artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta, deve ser interpretado no sentido de que não se opõe a uma legislação nacional que permite a conservação pelos prestadores de serviços de comunicações eletrónicas e o acesso de uma autoridade administrativa, responsável pela proteção dos direitos de autor e direitos conexos contra violações desses direitos cometidas na Internet, limitado a dados relativos à identidade civil correspondentes a endereços IP a fim de que essa autoridade possa identificar os titulares desses endereços suspeitos de serem responsáveis pela prática dessas violações e possa tomar, se necessário, medidas contra esses mesmos titulares, sem que esse acesso esteja subordinado a um controlo prévio por um órgão jurisdicional ou uma entidade administrativa independente, quando esses dados constituam o único meio de investigação que permite a identificação da pessoa à qual esse endereço estava atribuído no momento da prática da infração.

B. Quanto à terceira questão prejudicial

106. Com a sua terceira questão prejudicial, o órgão jurisdicional de reenvio pretende saber se, em caso de resposta afirmativa à primeira e segunda questões, e atendendo à reduzida sensibilidade dos dados relativos à identidade civil, ao enquadramento estrito do acesso aos dados e ao imperativo de não comprometer a missão de serviço público confiada à autoridade administrativa em causa, o artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta, deve ser interpretado no sentido de que se opõe a que o controlo prévio do acesso seja efetuado de acordo com modalidades adaptadas, como um controlo automatizado, no caso em apreço sob a supervisão de um serviço interno do organismo que dê garantias de independência e de imparcialidade em relação aos agentes responsáveis por essa recolha.

107. Decorre da redação da terceira questão prejudicial, bem como da resposta escrita do Governo francês às questões do Tribunal de Justiça que as modalidades de controlo adaptadas às quais se faz referência nesta questão não têm por objeto um sistema de controlo existente no direito nacional, mas as hipóteses que podem ser exploradas e destinadas, se necessário, a adequar o sistema francês ao cumprimento do direito da União.

108. Ora, é jurisprudência constante que um pedido de decisão prejudicial consiste, não na formulação de opiniões consultivas sobre questões gerais e hipotéticas, mas na necessidade inerente à solução efetiva de um litígio a respeito do direito da União (59).

109. Por conseguinte, uma vez que a terceira questão prejudicial tem, na minha opinião, caráter hipotético, deve ser julgada inadmissível.

110. Em todo o caso, atendendo à resposta que proponho dar à primeira e segunda questões prejudiciais, não há que responder à terceira questão.

V. Conclusão

111. À luz de todas as considerações precedentes, proponho que o Tribunal de Justiça responda às questões prejudiciais submetidas pelo Conseil d'État (Conselho de Estado, em formação jurisdicional, França) da seguinte forma:

O artigo 15.°, n.° 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta dos Direitos Fundamentais da União Europeia

deve ser interpretado no sentido de que:

não se opõe a uma legislação nacional que permite a conservação pelos prestadores de serviços de comunicações eletrónicas e o acesso de uma autoridade administrativa, responsável pela proteção dos direitos de autor e direitos conexos contra violações desses direitos cometidas na Internet, limitado a dados relativos à identidade civil correspondentes a endereços IP a fim de que essa autoridade possa identificar os titulares desses endereços suspeitos de serem responsáveis pela prática dessas violações e possa tomar, se necessário, medidas contra esses mesmos titulares, sem que esse acesso esteja subordinado a um controlo prévio por um órgão jurisdicional ou uma entidade administrativa independente, quando esses dados constituam o único meio de investigação que permite a identificação da pessoa à qual esse endereço estava atribuído no momento da prática da infração.

---

1 Língua original: francês.

---

2 Diretiva do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO 2002, L 201, p. 37).

---

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 1995, L 281, p. 31).

---

4 JORF de 7 de março de 2010, texto n.° 19.

5 JORF de 31 de julho de 2021, texto n.° 1. Esta versão do artigo L. 34-1 do CPCE, em vigor desde 31 de julho de 2021, foi adotada na sequência da decisão do Conseil d'État (Conselho de Estado, em formação jurisdicional, França) de 21 de abril de 2021, n.° 393099 (JORF de 25 de abril de 2021) que revogou a versão anterior dessa disposição que incluía uma obrigação de conservação de dados pessoais «para efeitos de investigação, deteção e repressão de infrações penais ou do incumprimento da obrigação definida no artigo L. 336-3 [do CPI]» com o único objetivo de permitir, se necessário, a disponibilização, nomeadamente, à Hadopi. Pela Decisão n.° 2021-976-977 QPC, de 25 de fevereiro de 2022 (M. Habib A. e o.), o Conseil constitutionnel (Tribunal Constitucional, França) declarou a inconstitucionalidade da versão anterior do artigo L. 34-1 do CPCE pelo facto essencial de que, «ao autorizar a conservação geral e indiferenciada dos dados de ligação, as disposições impugnadas violam de forma desproporcionada o direito à vida privada» (n.° 13). Com efeito, esse órgão jurisdicional considerou que os dados de ligação que devem ser conservados por força dessas disposições são relativos, não só à identificação dos utilizadores dos serviços de comunicações eletrónicas, mas também a outros dados que, «atendendo à respetiva diversidade e aos tratamentos de que podem ser objeto, fornecem, sobre esses utilizadores e, eventualmente, sobre terceiros, informações diversas e precisas, especialmente lesivas da sua privacidade» (n.° 11).

6 V. Acórdão de 6 de outubro de 2020 (C-511/18, C-512/18 e C-520/18, a seguir «Acórdão La Quadrature du Net e o. », EU:C:2020:791, dispositivo).

7 V. Acórdão de 21 de dezembro de 2016 (C-203/15 e C-698/15, a seguir «Acórdão Tele2», EU:C:2016:970, dispositivo).

8 N.° 120 deste acórdão.

9 N.° 189 deste acórdão.

10 Acórdão de 2 de março de 2021 (C-746/18, a seguir «Acórdão Prokuratuur», EU:C:2021:152).

11 Regulamento do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO 2016, L 119, p. 1).

12 V. Acórdão La Quadrature du Net e o. (n.os 155 e 159).

13 V. Acórdão Tele2 (n.° 79).

14 V. Acórdão de 2 de outubro de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, n.° 49).

15 Acórdão de 2 de outubro de 2018 (C-207/16, EU:C:2018:788).

16 V. Acórdão Prokuratuur (n.° 29)

17 V. Acórdão de 17 de junho de 2021, M.I.C.M. (C-597/19, EU:C:2021:492, n.os 127 a 130).

18 V. Acórdãos La Quadrature du Net e o., n.° 166), de 5 de abril de 2022, Commissioner of An Garda Síochána e o. (C-140/20, a seguir «Acórdão Commissioner of An Garda Síochána e o.» EU:C:2022:258, n.° 98), e de 20 de setembro de 2022, SpaceNet (C-793/19 e C-794/19, a seguir «Acórdão SpaceNet», EUC:2002:702, n.° 131).

19 V. Acórdãos La Quadrature du Net e o. (n.° 107); Commissioner of An Garda Síochána e o. (n.° 35), e SpaceNet (n.° 52).

20 V. Acórdãos Tele2 (n.° 86), La Quadrature du Net e o. (n.° 108), Commissioner of An Garda Síochána e o. (n.° 38), e SpaceNet (n.° 55).

21 V. Acórdãos La Quadrature du Net e o. (n.° 109), Commissioner of An Garda Síochána e o. (n.° 37), e SpaceNet (n.° 54).

22 V. Acórdãos La Quadrature du Net e o. (n.os 110 e 111), Commissioner of An Garda Síochána e o. (n.° 40), e SpaceNet (n.° 57).

23 V. Acórdãos La Quadrature du Net e o. (n.° 112), Commissioner of An Garda Síochána e o. (n.° 41), e SpaceNet (n.° 58).

24 V. Acórdãos La Quadrature du Net e o. (n.os 113 e 114); Commissioner of An Garda Síochána e o. (n.° 42), e SpaceNet (n.° 60).

25 V. Acórdãos La Quadrature du Net e o. (n.os 120 a 122), Commissioner of An Garda Síochána e o. (n.° 48), e SpaceNet (n.° 63).

26 V. Acórdãos La Quadrature du Net e o. (n.os 120 a 122), Commissioner of An Garda Síochána e o. (n.° 49), e SpaceNet (n.° 64).

27 V. Acórdãos La Quadrature du Net e o. (n.os 127 a 129), Commissioner of An Garda Síochána e o. (n.os 50 e 51) e SpaceNet (n.os 65 e 66).

28 V. Acórdãos La Quadrature du Net e o. (n.° 131), Commissioner of An Garda Síochána e o. (n.° 53) e SpaceNet (n.° 68).

29 V. n.os 41 e segs. das presentes conclusões.

30 V. Acórdão La Quadrature du Net e o. (n.° 152).

31 V. Acórdãos La Quadrature du Net e o. (n.° 153), Commissioner of An Garda Síochána e o. (n.° 73), e SpaceNet (n.° 103). O sublinhado é meu.

32 V. Acórdãos La Quadrature du Net e o. (n.° 154), Commissioner of An Garda Síochána e o. (n.° 73), e SpaceNet (n.° 103).

33 V. Acórdãos La Quadrature du Net e o. (n.os 155 e 156), Commissioner of An Garda Síochána e o. (n.° 74), e SpaceNet (n.os 104 e 105).

34 V. Acórdãos La Quadrature du Net e o. (n.° 156), e SpaceNet (n.° 105).

35 C-597/19, EU:C:2020:1063, n.° 98.

36 V. as minhas conclusões no processo M.I.C.M. (C-597/19, EU:C:2020:1063, n.° 97).

37 V. Acórdãos de 19 de abril de 2012, Bonnier Audio e o. (C-461/10, EU:C:2012:219, n.° 55), de 4 de maio de 2017, Rīgas satiksme (C-13/16, EU:C:2017:336, n.° 34), e de 17 de junho de 2021, M.I.C.M. (C-597/19, EU:C:2021:492, n.os 47 a 54).

38 V., neste sentido, Acórdão de 29 de janeiro de 2008, Promusicae (C-275/06, EU:C:2008:54, n.os 50 a 52).

39 V. n.° 65 das presentes conclusões.

40 V. as minhas conclusões no processo M.I.C.M. (C-597/19, EU:C:2020:1063, n.° 103).

41 V. artigo 15.°, n.° 1, da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o Comércio Eletrónico») (JO 2000, L 78, p. 1).

42 V. n.os 60 e 61 das presentes conclusões.

43 V. Acórdão La Quadrature du Net e o. (n.° 155) (o sublinhado é meu).

44 V. Acórdão La Quadrature du Net e o. (n.° 156) (O sublinhado é meu).

45 V. Acórdãos de 2 de outubro de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, n.° 55), e Prokuratuur (n.° 32).

46 N.° 47 das presentes conclusões.

47 V. Acórdãos SpaceNet, (n.° 131), La Quadrature du Net e o. (n.° 166) e Commissioner of An Garda Síochána e o. (n.° 98).

48 V. Acórdãos Tele2 (n.° 115), de 2 de outubro de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, n.° 56), e Prokuratuur (n.° 33).

49 V. n.os 65 e segs. das presentes conclusões.

50 V. Acórdãos Tele2 (n.° 118), Prokuratuur (n.° 49), e Commissioner of An Garda Síochána e o. (n.° 104).

51 V. Acórdãos Tele2 (n.° 119), Prokuratuur (n.° 50), e Commissioner of An Garda Síochána e o. (n.° 105).

52 V. Acórdãos Tele2 (n.° 119), Prokuratuur (n.° 50) e Commissioner of An Garda Síochána e o. (n.° 105).

53 V. Acórdãos Tele2 e Commissioner of An Garda Síochána e o.

---

54 V. Acórdão Prokuratuur.

---

55 V. Acórdão Prokuratuur (n.° 45).

---

56 A título acessório, refira-se que contra a obrigação de um controlo prévio sistemático também militam argumentos de viabilidade. A existência de um sistema organizado de luta contra as infrações aos direitos de autor cometidas em linha, como o que está em causa no processo principal, pressupõe a necessidade de tratar quantidades significativas de dados pessoais, que refletem o número de infrações processadas, a saber, a título de exemplo em relação ao ano de 2019, segundo as observações do Governo francês, 33 465 pedidos de identificação do endereço IP efetuados pela Hadopi diariamente. Neste contexto, a obrigação de um controlo prévio do acesso a esses dados poderia comprometer, na prática, o funcionamento dos mecanismos de luta organizada contra a contrafação em linha, pondo em causa o equilíbrio entre os direitos dos utilizadores e os dos autores.

---

57 Diretiva do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO 2016, L 119, p. 89).

---

58 Todas essas garantias se encontram previstas nas disposições do capítulo III, título III, da Lei n.° 78-17 relativa à informática, aos ficheiros e às liberdades, de 6 de janeiro de 1978 (JORF de 7 de janeiro de 1978).

---

59 V. Acórdãos de 26 de outubro de 2017, Balgarska energiyna borsa (C-347/16, EU:C:2017:816, n.° 31), de 31 de maio de 2018, Confetra e o. (C-259/16 e C-260/16, EU:C:2018:370, n.° 63), e de 17 de outubro de 2019, Elektrorazpredelenie Yug (C-31/18, EU:C:2019:868, n.° 32).