Coletânea da Jurisprudência

CONCLUSÕES DO ADVOGADO-GERAL
MACIEJ SZPUNAR
apresentadas em 4 de junho de 2019[1]

Processo C-18/18

Eva Glawischnig-Piesczek
contra
Facebook Ireland Limited

[pedido de decisão prejudicial apresentado pelo Oberster Gerichtshof (Supremo Tribunal, Áustria)]

«Reenvio prejudicial — Livre prestação de serviços — Diretiva 2000/31/CE — Serviços da sociedade de informação — Responsabilidade dos prestadores intermediários — Obrigação de um prestador de serviços de armazenamento de sítios Internet (Facebook) apagar informações ilegais — Alcance»

I. Introdução

1. *Na Internet não se escreve a lápis mas a tinta*, constata uma personagem de um filme americano lançado em 2010. Refiro-me aqui, e não por acaso, ao filme *The Social Network*.

2. Com efeito, no cerne do presente processo coloca-se a questão de saber se um fornecedor de armazenamento que explora uma plataforma de rede social em linha pode ser obrigado a fazer desaparecer, com ajuda de um apagador de tinta metafórico, certos conteúdos disponibilizados em linha por utilizadores dessa plataforma.

3. Mais especificamente, com as suas questões prejudiciais, o órgão jurisdicional de reenvio convida o Tribunal de Justiça a precisar o alcance pessoal e material das obrigações que podem ser impostas a um fornecedor de armazenamento, sem que isso conduza a impor uma obrigação geral de vigilância, proibida nos termos do artigo 15.º, n.º 1, da Diretiva 2000/31/CE[2]. O órgão jurisdicional de reenvio pergunta igualmente ao Tribunal de Justiça se, no quadro de uma medida inibitória imposta pelo órgão jurisdicional de um Estado-Membro, um fornecedor de armazenamento pode ser obrigado a remover certos conteúdos não só para os internautas desse Estado-Membro mas também a nível mundial.

II. Quadro jurídico

A. Direito da União

4. Os artigos 14.º e 15.º da Diretiva 2000/31 constam da secção 4, intitulada «Responsabilidade dos prestadores intermediários de serviços», do capítulo II dessa diretiva.

1 Língua original: francês.

2 Diretiva 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 178, p. 1).

5. O artigo 14.º, n.ºs 1 e 3, da Diretiva 2000/31, com a epígrafe «Armazenagem em servidor», dispõe:

«1. Em caso de prestação de um serviço da sociedade da informação que consista no armazenamento de informações prestadas por um destinatário do serviço, os Estados-Membros velarão por que a responsabilidade do prestador do serviço não possa ser invocada no que respeita à informação armazenada a pedido de um destinatário do serviço, desde que:

a) O prestador não tenha conhecimento efetivo da atividade ou informação ilegal e, no que se refere a uma ação de indemnização por perdas e danos, não tenha conhecimento de factos ou de circunstâncias que evidenciam a atividade ou informação ilegal,

ou

b) O prestador, a partir do momento em que tenha conhecimento da ilicitude, atue com diligência no sentido de retirar ou impossibilitar o acesso às informações.

[…]

3. O disposto no presente artigo não afeta a faculdade de um tribunal ou autoridade administrativa, de acordo com os sistemas legais dos Estados-Membros, exigir do prestador que previna ou ponha termo a uma infração, nem afeta a faculdade de os Estados-Membros estabelecerem disposições para a remoção ou impossibilitação do acesso à informação.»

6. O artigo 15.º, n.º 1, da Diretiva 2000/31, com a epígrafe «Ausência de obrigação geral de vigilância», dispõe:

«Os Estados-Membros não imporão aos prestadores, para o fornecimento dos serviços mencionados nos artigos 12.º, 13.º e 14.º, uma obrigação geral de vigilância sobre as informações que estes transmitam ou armazenem, ou uma obrigação geral de procurar ativamente factos ou circunstâncias que indiciem ilicitudes.»

B. Direito austríaco

7. Nos termos do § 18, n.º 1, da E-Commerce-Gesetz (Lei relativa ao comércio eletrónico), através da qual o legislador austríaco transpôs a Diretiva 2000/31, os prestadores de serviços de armazenamento em servidor não têm uma obrigação geral de vigilância sobre as informações que armazenem, transmitam ou tornem acessíveis, nem de procurar por si mesmo factos ou circunstâncias que indiciem atividades ilícitas.

8. Nos termos do § 1330, n.º 1, do Allgemeines Bürgerliches Gesetzbuch (Código Civil Geral, a seguir «ABGB»), quem tiver sofrido um prejuízo efetivo ou lucros cessantes na sequência de uma ofensa à sua honra, tem direito a indemnização. Ao abrigo do n.º 2 desse artigo, o mesmo acontece quando uma pessoa relata factos ofensivos da reputação, da situação material e das perspetivas de futuro de terceiros e de que conhecia ou devia conhecer a falsidade. Neste caso, podem ser exigidas a retratação e a respetiva publicação.

9. Nos termos do § 78. n.º 1, da Urheberrechtsgesetz (Lei sobre os direitos de autor, a seguir «UrhG»), as imagens que representam uma pessoa não devem ser expostas publicamente nem divulgadas de uma outra forma que as torne acessíveis ao público, caso isso viole os interesses legítimos da pessoa em causa ou, se esta tiver falecido sem ter autorizado ou ordenado a publicação, os interesses legítimos de um parente próximo.

III. Factos do litígio no processo principal

10. Eva Glawischnig-Piesczek era deputada no Nationalrat (Conselho Nacional, Áustria), presidente do grupo parlamentar *die Grünen* («Os Verdes») e porta-voz federal desse partido.

11. A Facebook Ireland Limited, sociedade registada na Irlanda com sede em Dublim, é uma filial da sociedade americana Facebook Inc. A Facebook Ireland explora, para os utilizadores situados fora dos Estados Unidos e do Canadá, uma plataforma de rede social em linha, acessível no endereço www.facebook.com. Essa plataforma permite aos utilizadores criar páginas de perfil e publicar comentários.

12. Em 3 de abril de 2016, um utilizador da referida plataforma partilhou na sua página pessoal um artigo da revista austríaca de informação em linha *oe24.at*, intitulado «Os Verdes: a favor da manutenção de um rendimento mínimo para os refugiados». Essa publicação teve por efeito gerar, nessa plataforma, uma «pré-visualização» do sítio de origem, que continha o título e um breve resumo desse artigo, bem como uma fotografia da recorrente. Além disso, esse utilizador publicou, a propósito desse artigo e a acompanhar a partilha, um comentário depreciativo em relação à recorrente, acusando-a de ser uma «vil traidora da pátria», uma «idiota corrupta» e um membro de um «partido de fascistas». Os conteúdos colocados em linha por esse utilizador podiam ser consultados por todos os utilizadores da plataforma em causa.

13. Por carta de 7 de julho de 2016, a recorrente pediu, nomeadamente, à Facebook Ireland que apagasse esse comentário.

14. Não tendo a Facebook Ireland retirado o comentário em causa, a recorrente intentou uma ação no Handelsgericht Wien (Tribunal de Comércio de Viena, Áustria) e pediu que esse tribunal proferisse um despacho de medidas provisórias que obrigasse a Facebook Ireland a cessar de publicar e/ou de divulgar fotos da recorrente, dado que a mensagem que as acompanha divulga afirmações idênticas e/ou de «conteúdo semelhante», a saber, que a recorrente seria uma «vil traidora da pátria» e/ou uma «idiota corrupta» e/ou membro de um «partido de fascistas».

15. Em 7 de dezembro de 2016, o Handelsgericht Wien (Tribunal de Comércio de Viena) proferiu o despacho de medidas provisórias requerido.

16. Em seguida, a Facebook Ireland impossibilitou, na Áustria, o acesso ao conteúdo inicialmente publicado.

17. Em sede de recurso, o Oberlandesgericht Wien (Tribunal Regional Superior de Viena, Áustria) confirmou o despacho de medidas provisórias proferido em primeira instância a respeito das afirmações idênticas. Ao fazê-lo, esse tribunal indeferiu o pedido da Facebook Ireland destinado a limitar o despacho de medidas provisórias à República da Áustria. Em contrapartida, o referido tribunal decidiu que a obrigação de cessar a divulgação de afirmações de conteúdo semelhante visava unicamente as levadas ao conhecimento da Facebook Ireland pela recorrente no processo principal, por terceiros ou por outra forma.

18. Os tribunais de primeira e de segunda instância fundamentaram as suas decisões com base no § 78 da UrhG e no § 1330 do ABGB, considerando, nomeadamente, que o comentário publicado continha declarações que ofendiam excessivamente a honra da recorrente e que dava a entender que a mesma teria tido um comportamento criminoso, sem fornecer a mínima prova a esse respeito. Além disso, segundo esses tribunais, em matéria de declarações proferidas contra uma personalidade política, sem relação com um debate político ou de interesse geral, qualquer referência ao direito à liberdade de expressão era igualmente inaceitável.

19. As duas partes no processo principal interpuseram recursos para o Oberster Gerichtshof (Supremo Tribunal, Áustria), que considerou que as declarações em causa se destinavam a ofender a honra da recorrente, a injuriá-la e a difamá-la.

20. O órgão jurisdicional de reenvio é chamado a pronunciar-se sobre a questão de saber se a ordem de cessação, dada a um fornecedor de armazenamento que explora uma rede social com inúmeros utilizadores, também pode ser alargada, a nível mundial, às declarações literalmente idênticas e/ou de conteúdo semelhante de que aquele não tem conhecimento.

21. A este respeito, o Oberster Gerichtshof (Supremo Tribunal) refere que, de acordo com a sua própria jurisprudência, essa obrigação deve ser considerada proporcionada quando o prestador já teve conhecimento de, pelo menos, uma ofensa aos interesses da pessoa em causa causada pela atuação de um utilizador do serviço e que, assim sendo, o risco de serem cometidas outras violações é real.

IV. Questões prejudiciais e tramitação processual no Tribunal de Justiça

22. Foi nessas circunstâncias que o Oberster Gerichtshof (Supremo Tribunal), por decisão de 25 de outubro de 2017, que deu entrada no Tribunal de Justiça em 10 de janeiro de 2018, decidiu suspender a instância e submeter as seguintes questões à apreciação do Tribunal de Justiça:

«1) O artigo 15.º, n.º 1, da Diretiva [2000/31] opõe-se, em termos gerais, a uma das seguintes obrigações impostas a um fornecedor de *web hosting* que não removeu imediatamente informações ilegais, no sentido de remover não apenas a informação ilegal em causa na aceção do artigo 14.º, n.º 1, alínea a), [desta] diretiva, mas também outras informações de conteúdo idêntico:

   a) a nível mundial?

   b) no respetivo Estado-Membro?

   c) do respetivo utilizador a nível mundial?

   d) do respetivo utilizador no Estado-Membro?

2) Em caso de resposta negativa à primeira questão: o mesmo se aplica a informações de conteúdo semelhante?

3) O mesmo se aplica a informações de conteúdo semelhante, a partir do momento em que o operador tenha tido conhecimento desta circunstância?»

23. Foram apresentadas observações escritas pela recorrente, pela Facebook Ireland, pelos Governos austríaco, letão, português e finlandês e pela Comissão Europeia. Os mesmos interessados, com exceção do Governo português, fizeram-se representar na audiência de 13 de fevereiro de 2019.

V. Análise

A. Quanto à primeira e segunda questões prejudiciais

24. Com a sua primeira e segunda questões, que devem ser examinadas conjuntamente, o órgão jurisdicional de reenvio pede que o Tribunal de Justiça determine o alcance material e pessoal de uma obrigação de vigilância que pode ser imposta, no quadro de uma medida inibitória, ao prestador de um serviço da sociedade de informação que consiste no armazenamento de informações fornecidas por um utilizador desse serviço (concretamente, a um fornecedor de armazenamento), sem que tal conduza à imposição de uma obrigação geral de vigilância, proibida pelo artigo 15.º, n.º 1, da Diretiva 2000/31.

25. É certo que estas duas primeiras questões visam mais a remoção das informações divulgadas através de uma plataforma de rede social em linha do que a vigilância ou a filtragem dessas informações. Contudo, há que referir que as plataformas de rede social constituem meios de comunicação cujo conteúdo é principalmente criado não pelas suas sociedades fundadoras e gerentes, mas pelos seus utilizadores. Além disso, esse conteúdo, reproduzido e entretanto alterado, é objeto de trocas constantes entre os utilizadores.

26. Para poder suprimir uma informação difundida através dessa plataforma ou tornar o acesso à mesma impossível, seja qual for o autor dessa informação e o seu conteúdo, um fornecedor de armazenamento deve previamente identificar essa informação de entre as informações armazenadas nos seus servidores. Para tal, deve, de uma forma ou de outra, vigiar ou filtrar essas informações. Ora, nos termos do artigo 15.º, n.º 1, da Diretiva 2000/31, referido nas questões prejudiciais, um Estado-Membro não pode impor uma obrigação geral de vigilância a um fornecedor de armazenamento. Tudo isto sugere que, com as suas duas primeiras questões, o órgão jurisdicional de reenvio se interroga, em substância, sobre o alcance pessoal e material dessa obrigação, que é conforme às exigências da Diretiva 2000/31.

27. Com a sua primeira questão, o órgão jurisdicional de reenvio pede igualmente ao Tribunal de Justiça que precise se um fornecedor de armazenamento pode ser obrigado a remover, a nível mundial, informações divulgadas através de uma plataforma de rede social.

28. Para responder a estas duas questões, analisarei em primeiro lugar, por um lado, o regime da Diretiva 2000/31 aplicável à Facebook Ireland enquanto fornecedor de armazenamento e, por outro, as implicações da sua qualificação como fornecedor de armazenamento no que respeita às medidas inibitórias impostas a esse prestador. Em segundo lugar, procederei à análise das exigências previstas pelo direito da União no que diz respeito ao alcance material e pessoal da obrigação de vigilância que pode ser imposta a um fornecedor de armazenamento no quadro de uma medida inibitória, sem que isso conduza à imposição de uma obrigação geral nessa matéria. Por último, em terceiro lugar, abordarei a questão do alcance territorial da obrigação de remoção.

1. Medidas inibitórias impostas aos fornecedores de armazenamento à luz da Diretiva 2000/31

29. Importa recordar que, para que a armazenagem efetuada pelo prestador de um serviço da sociedade de informação seja abrangida pelo artigo 14.º da Diretiva 2000/31, o comportamento desse prestador deve limitar-se ao de um «prestador intermediário» na aceção pretendida pelo legislador no contexto da secção 4 dessa diretiva. Além disso, segundo o considerando 42 da referida diretiva, o seu comportamento é puramente técnico, automático e passivo, o que implica a falta de conhecimento ou de controlo dos dados que armazena e que o papel por ele desempenhado deva, portanto, ser neutro [3].

3 V., nomeadamente, Acórdão de 23 de março de 2010, Google France e Google (C-236/08 a C-238/08, EU:C:2010:159, n.os 112 e 113).

30. O Tribunal de Justiça já teve oportunidade de esclarecer que quem explora uma plataforma de rede social, armazenando nos seus servidores informações fornecidas por utilizadores dessa plataforma, relativas ao seu perfil, é um prestador de serviços de armazenamento na aceção do artigo 14.º da Diretiva 2000/31 [4]. Independentemente das dúvidas que se possa ter a este respeito, resulta do pedido de decisão prejudicial que, para o órgão jurisdicional de reenvio, é ponto assente que a Facebook Ireland é um fornecedor de armazenamento cujo comportamento se limita ao de um prestador intermediário.

31. Ao abrigo da Diretiva 2000/31, um fornecedor de armazenamento cujo comportamento se limita ao de um prestador intermediário beneficia de uma imunidade relativa em matéria de responsabilidade pelas informações que armazena. Com efeito, essa imunidade apenas é concedida quando esse fornecedor de armazenamento não teve conhecimento do caráter ilegal das informações armazenadas ou da atividade desenvolvida através dessas informações e na condição de, uma vez advertido dessa ilegalidade, agir prontamente com vista a retirar as informações em causa ou impossibilitar o acesso às mesmas. Em contrapartida, se esse fornecedor de armazenamento não preencher esses requisitos, isto é, se tinha conhecimento da ilegalidade das informações armazenadas, mas não agiu no sentido de as retirar ou impossibilitar o acesso às mesmas, a Diretiva 2000/31 não se opõe a que possa ser considerado indiretamente responsável por essas informações [5].

32. Por outro lado, resulta do artigo 14.º, n.º 3, da Diretiva 2000/31 que a imunidade concedida a um prestador intermediário não obsta a que um órgão jurisdicional ou uma autoridade administrativa, de acordo com os sistemas legais dos Estados-Membros, exija do prestador que previna uma violação ou ponha termo a uma violação. Decorre dessa disposição que um prestador intermediário pode ser destinatário de medidas inibitórias, mesmo que, segundo os requisitos enunciados no artigo 14.º, n.º 1, dessa diretiva, esse prestador não seja ele próprio responsável pelas informações armazenadas nos seus servidores [6].

33. As condições e as modalidades dessas medidas inibitórias impostas aos prestadores intermediários relevam do direito nacional [7]. Todavia, as regras instituídas pelos Estados-Membros devem respeitar as exigências estabelecidas pelo direito da União, nomeadamente pela Diretiva 2000/31.

34. Tudo isto reflete a vontade do legislador da União de ponderar, através dessa diretiva, os diferentes interesses dos fornecedores de armazenamento cujo comportamento se limite ao de um prestador intermediário, dos utilizadores dos seus serviços e das pessoas lesadas por qualquer infração cometida durante a utilização desses serviços. Por conseguinte, incumbe aos Estados-Membros, na execução das medidas de transposição da Diretiva 2000/31, não só respeitar as exigências estabelecidas por essa diretiva, mas também zelar por não se basear numa interpretação que entre em conflito com os direitos fundamentais em causa ou com os outros princípios gerais do direito da União, tais como o princípio da proporcionalidade [8].

4 V. Acórdão de 16 de fevereiro de 2012, SABAM (C-360/10, EU:C:2012:85, n.º 27).

5 V. artigo 14.º da Diretiva 2000/31. V., igualmente, as minhas Conclusões no processo Stichting Brein (C-610/15, EU:C:2017:99, n.ºs 67 e 68).

6 V. Acórdão de 7 de agosto de 2018, SNB-REACT (C-521/17, EU:C:2018:639, n.º 51). V., igualmente, neste sentido, Lodder, A. R., Polter, P., «ISP blocking and filtering: on the shallow justifications in case law regarding effectiveness of measures», *European Journal of Law and Technology*, 2017, vol. 8, n.º 2, p. 5.

7 V. as minhas Conclusões no processo Mc Fadden (C-484/14, EU:C:2016:170). V., igualmente, Husovec, M., *Injunctions Against Intermediaires in the European Union. Accountable But Not Liable*?, Cambridge University Press, Cambridge, 2017, pp. 57 e 58.

8 V., neste sentido, sobre o respeito dos direitos fundamentais e do princípio da proporcionalidade, Acórdão de 29 de janeiro de 2008, Promusicae (C-275/06, EU:C:2008:54, n.º 68).

2. Exigências quanto ao alcance pessoal e material de uma obrigação em matéria de vigilância

a) Proibição de uma obrigação geral de vigilância

35. Cumpre observar que o artigo 15.º, n.º 1, da Diretiva 2000/31 proíbe os Estados-Membros de imporem, nomeadamente aos prestadores de serviços cuja atividade consista na armazenagem de informações, uma obrigação geral de vigilância das informações que armazenem ou uma obrigação geral de procurar ativamente factos ou circunstâncias que indiciem atividades ilícitas. Por outro lado, resulta da jurisprudência que essa disposição se opõe, designadamente, a que um fornecedor de armazenamento cujo comportamento se limite ao de um prestador intermediário seja obrigado a proceder a uma vigilância da totalidade [9] ou da quase totalidade [10] dos dados de todos os utilizadores do seu serviço a fim de prevenir qualquer violação futura.

36. Se, contrariamente ao que prevê essa disposição, um Estado-Membro pudesse impor, no quadro de uma medida inibitória, uma obrigação geral de vigilância a um fornecedor de armazenamento, não é de excluir que este se arriscasse a perder a qualidade de prestador intermediário e a imunidade que a acompanha. Com efeito, o papel de um fornecedor de armazenamento que exercesse uma vigilância geral já não seria neutro. A atividade desse fornecedor de armazenamento não iria manter o seu caráter técnico, automático e passivo, o que implicaria que o referido fornecedor teria conhecimento das informações armazenadas e exerceria um controlo sobre as mesmas.

37. Além disso, mesmo que esse risco não existisse, um fornecedor de armazenamento que exercesse uma vigilância geral poderia, em princípio, ser considerado responsável por qualquer atividade ou informação ilegal, sem que os requisitos enunciados no artigo 14.º, n.º 1, alíneas a) e b), dessa diretiva estivessem efetivamente preenchidos.

38. É certo que o artigo 14.º, n.º 1, alínea a), da Diretiva 2000/31 sujeita a responsabilidade de um prestador intermediário à tomada efetiva de conhecimento da atividade ou da informação ilegal. Todavia, perante uma obrigação geral de vigilância, o caráter ilícito de qualquer atividade ou informação poderia ser considerado como tendo sido levado automaticamente ao conhecimento desse prestador intermediário, que teria de proceder à remoção dessas informações ou impossibilitar o acesso às mesmas, sem que tivesse apreendido o seu conteúdo ilícito [11]. Consequentemente, a lógica da imunidade relativa em matéria de responsabilidade pelas informações armazenadas por um prestador intermediário seria sistematicamente invertida, o que prejudicaria o efeito útil do artigo 14.º, n.º 1, da Diretiva 2000/31.

39. Resumindo, o papel de um fornecedor de armazenamento que exercesse essa vigilância geral já não seria neutro, na medida em que a sua atividade não iria conservar o seu caráter técnico, automático e passivo, o que implicaria que o referido fornecedor de armazenamento teria conhecimento das informações armazenadas e exerceria um controlo sobre as mesmas. Por conseguinte, a aplicação da obrigação geral de vigilância, imposta a um fornecedor de armazenamento no quadro de uma medida inibitória autorizada, *a priori*, ao abrigo do artigo 14.º, n.º 3, da Diretiva 2000/31, poderia tornar o artigo 14.º dessa diretiva inaplicável a esse fornecedor de armazenamento.

40. Assim, deduzo da leitura conjugada do artigo 14.º, n.º 3, e do artigo 15.º, n.º 1, da Diretiva 2000/31 que uma obrigação imposta a um prestador intermediário no quadro de uma medida inibitória não pode conduzir a que, relativamente à totalidade ou à quase totalidade das informações armazenadas, o papel desse prestador intermediário deixe de ser neutro no sentido descrito no número anterior.

9 V. Acórdãos de 12 de julho de 2011, L'Oréal e o. (C-324/09, EU:C:2011:474, n.os 139 e 144), e de 24 de novembro de 2011, Scarlet Extended (C-70/10, EU:C:2011:771, n.os 36 e 40).

10 V. Acórdão de 16 de fevereiro de 2012, SABAM (C-360/10, EU:C:2012:85, n.os 37 e 38).

11 V., neste sentido, Conclusões do advogado-geral N. Jääskinen no processo L'Oréal e o. (C-324/09, EU:C:2010:757, n.º 143).

b) Obrigação de vigilância em casos específicos

41. Conforme enuncia o considerando 47 da Diretiva 2000/31, a proibição de impor obrigações gerais, prevista no artigo 15.º, n.º 1, dessa diretiva, não diz respeito a obrigações de vigilância *em casos específicos*. Com efeito, resulta da redação do artigo 14.º, n.º 3, da Diretiva 2000/31 que um fornecedor de armazenamento pode ser obrigado a *prevenir* uma infração, o que implica logicamente, como alega a Comissão, uma certa forma de vigilância no futuro, sem que essa vigilância se transforme em obrigação de vigilância geral [12]. O artigo 18.º dessa diretiva exige, além disso, que os Estados-Membros assegurem que as ações judiciais disponíveis em direito nacional em relação às atividades de serviços da sociedade da informação permitam a rápida adoção de medidas destinadas, designadamente, *a evitar quaisquer outros novos prejuízos* às partes interessadas.

42. Por outro lado, resulta do Acórdão L'Oréal e o. [13] que um fornecedor de armazenamento pode ser obrigado a tomar medidas que contribuam para evitar que ocorram *outros prejuízos* de mesma natureza pelo mesmo destinatário.

43. Nesse acórdão, o Tribunal de Justiça interpretou não só as disposições da Diretiva 2000/31, mas também as disposições da Diretiva 2004/48/CE [14]. Ora, ao fazê-lo, o Tribunal de Justiça definiu a obrigação de vigilância de acordo com as exigências estabelecidas por essas diretivas, por oposição à obrigação proibida pelo artigo 15.º, n.º 1, da Diretiva 2000/31, a saber, a obrigação *de vigilância ativa da totalidade — quase totalidade* dos dados a fim de prevenir qualquer violação futura [15]. Independentemente do contexto específico do Acórdão L'Oréal e o. [16] e das referências à Diretiva 2004/48, as considerações desse acórdão relativas às obrigações dos fornecedores de armazenamento conformes ao direito da União, em função do seu caráter geral ou não, são de natureza transversal e, por conseguinte, são, a meu ver, aplicáveis ao caso em apreço.

44. Assim, a fim de prevenir qualquer violação futura, um fornecedor de armazenamento pode ser obrigado, no quadro de uma medida inibitória, a retirar informações ilegais ainda não divulgadas no momento da imposição dessa medida inibitória, sem que a divulgação dessas informações tenha sido levada, de novo e de forma separada em relação ao pedido inicial de remoção, ao seu conhecimento.

45. Todavia, para não conduzir à imposição de uma obrigação geral, uma obrigação de vigilância deve, conforme parece decorrer do Acórdão L'Oréal e o. [17], responder a exigências adicionais, a saber, incidir sobre violações de *mesma natureza*, por parte do *mesmo destinatário*, *aos mesmos direitos*, nesse caso, o das marcas.

46. Assim, deduzo daqui que a vigilância ativa não é inconciliável com a Diretiva 2000/31, contrariamente à vigilância ativa cujo objeto não seja direcionado para casos específicos de violação.

47. Nesta ordem de ideias, referi nas minhas Conclusões no processo Mc Fadden [18], relativo a um fornecedor de acesso a uma rede de comunicações na aceção do artigo 12.º da Diretiva 2000/31, inspirando-me nos trabalhos preparatórios da Diretiva 2000/31, que para que uma obrigação possa ser considerada uma obrigação *em casos específicos*, deve, nomeadamente, ser limitada relativamente ao *objeto* e à *duração* da vigilância.

12 V., igualmente, neste sentido, Rosati, E., *Copyright and the Court of Justice of the European Union*, Oxford University Press, Oxford, 2019, p. 158.

13 Acórdão de 12 de julho de 2011 (C-324/09, EU:C:2011:474, n.º 144).

14 Diretiva do Parlamento Europeu e do Conselho, de 29 de abril de 2004, relativa ao respeito dos direitos de propriedade Intelectual (JO 2004, L 157, p. 45).

15 Acórdão de 12 de julho de 2011, L'Oréal e o. (C-324/09, EU:C:2011:474, n.ºs 139 e 144).

16 Acórdão de 12 de julho de 2011 (C-324/09, EU:C:2011:474).

17 Acórdão de 12 de julho de 2011, L'Oréal e o. (C-324/09, EU:C:2011:474, n.ºs 141 e 144).

18 C-484/14, EU:C:2016:170, n.º 132.

48. Essas exigências gerais formuladas de forma abstrata parecem-me transponíveis para circunstâncias como as do processo principal, apesar de, na aplicação por analogia aos fornecedores de armazenamento, como a Facebook Ireland, das considerações em matéria de obrigação de vigilância aplicáveis aos fornecedores de acesso a uma rede de comunicação, como a Internet, os papéis exercidos por esses prestadores intermediários serem diferentes. Por exemplo, se considerarmos um fornecedor de armazenamento como a Facebook Ireland, os conteúdos da sua plataforma parecem constituir a totalidade dos dados armazenados, ao passo que, para um fornecedor de acesso à Internet, esses conteúdos representam apenas uma ínfima parte dos dados transmitidos. Em contrapartida, a natureza e a intensidade da implicação desse fornecedor de armazenamento no tratamento dos conteúdos digitais diferem sensivelmente das de um fornecedor de acesso à Internet. Conforme observa a Comissão, um fornecedor de armazenamento está melhor colocado para tomar medidas a fim de procurar e eliminar informações ilegais que um fornecedor de acesso.

49. Por outro lado, a exigência relativa à limitação temporal de uma obrigação de vigilância reflete vários acórdãos do Tribunal de Justiça [19]. Embora resulte da jurisprudência que a limitação temporal de uma obrigação imposta no quadro de uma medida inibitória se refere mais à problemática dos princípios gerais do direito da União [20], considero que uma obrigação de vigilância permanente seria dificilmente conciliável com o conceito de obrigação num caso específico, na aceção do considerando 47 da Diretiva 2000/31.

50. Assim, o caráter direcionado de uma obrigação de vigilância deve ser previsto tendo em consideração a duração dessa vigilância e as precisões relativas à natureza das violações visadas, ao seu autor e ao seu objeto. Todos esses elementos são interdependentes e ligados uns aos outros. Assim, há que os avaliar de forma global para responder à questão de saber se uma medida inibitória respeita ou não a proibição prevista no artigo 15.º, n.º 1, da Diretiva 2000/31.

c) Conclusões intercalares

51. Para recapitular esta parte da minha análise, em primeiro lugar, resulta da leitura conjugada do artigo 14.º, n.º 3, e do artigo 15.º, n.º 1, da Diretiva 2000/31 que uma obrigação imposta a um prestador intermediário no quadro de uma medida inibitória não pode conduzir à situação em que, relativamente à totalidade ou à quase totalidade das informações armazenadas, o papel desse prestador intermediário deixe de ser técnico, automático e passivo, o que implicaria que o fornecedor de armazenamento em causa teria conhecimento dessas informações e exerceria um controlo sobre as mesmas [21].

52. Em segundo lugar, a vigilância ativa não é inconciliável com a Diretiva 2000/31, contrariamente à vigilância ativa cujo objeto não seja direcionado para casos específicos de violação [22].

53. Em terceiro lugar, o caráter direcionado de uma obrigação de vigilância deve ser previsto tendo em consideração a duração dessa vigilância e as precisões relativas à natureza das violações visadas, ao seu autor e ao seu objeto [23].

19 Mais especificamente, o Tribunal de Justiça referiu, no Acórdão de 12 de julho de 2011, L'Oréal e o. (C-324/09, EU:C:2011:474, n.º 140), que a medida inibitória que visa prevenir eventuais violações de marcas no quadro do serviço da sociedade da informação, a saber, um sítio de comércio eletrónico, não pode ter por objeto ou por efeito instituir uma proibição geral e permanente de colocação no mercado de produtos dessas marcas. No mesmo espírito, o Tribunal de Justiça referiu, no Acórdão de 16 de fevereiro de 2012, SABAM (C-360/10, EU:C:2012:85, n.º 45), que o direito da União se opõe, nomeadamente, a que uma obrigação de vigilância, estabelecida no quadro de uma medida inibitória imposta a um prestador, seja *ilimitada no tempo*.

20 Essa abordagem foi a retida pelo advogado-geral N. Jääskinen nas suas Conclusões no processo L'Oréal e o. (C-324/09, EU:C:2010:757, n.º 181), que, a meu ver, inspiraram fortemente a formulação dos trechos em causa do Acórdão proferido pelo Tribunal de Justiça nesse processo.

21 V. n.º 39 das presentes conclusões.

22 V. n.º 46 das presentes conclusões.

23 V. n.º 50 das presentes conclusões.

54. É à luz destas considerações que há que abordar o alcance pessoal e material de uma obrigação de vigilância de um prestador que explora uma plataforma de rede social. Esse alcance resume-se, no caso em apreço, à procura e à identificação, de entre conteúdos armazenados, de informações idênticas à que foi qualificada de ilegal pelo órgão jurisdicional que foi chamado a decidir e à procura de informações semelhantes à mesma.

d) Aplicação ao caso em apreço

1) Informações idênticas à informação que foi qualificada de ilegal

55. Com exceção da Facebook Ireland, todos os interessados sustentam que deve ser possível ordenar a um fornecedor de armazenamento suprimir ou bloquear o acesso às declarações idênticas à que tenha sido qualificada de ilegal, publicadas pelo mesmo utilizador. A recorrente, os Governos austríaco e letão, bem como a Comissão, são, em substância, de opinião que o mesmo se aplica às declarações publicadas por outros utilizadores.

56. Resulta do reenvio prejudicial que o tribunal de segunda instância considerou que a referência às «informações idênticas» visava as publicações de fotografias da recorrente *acompanhadas do mesmo texto*. Nesta ordem de ideias, o órgão jurisdicional de reenvio explica que as suas dúvidas incidem, nomeadamente, sobre a questão de saber se a medida inibitória imposta à Facebook Ireland pode ser alargada às *declarações (mensagens de acompanhamento) literalmente idênticas* e às declarações de conteúdo semelhante. Entendo assim essa referência às «informações idênticas» no sentido de que o órgão jurisdicional de reenvio se refere às reproduções manuais e exatas da informação que qualificou de ilegal e, como indica o Governo austríaco, às reproduções automatizadas, efetuadas através da função de «partilha».

57. A este respeito, sou de opinião que um fornecedor de armazenamento que explora uma plataforma de rede social pode ser obrigado, para cumprir uma medida inibitória imposta por um órgão jurisdicional de um Estado-Membro, a procurar e identificar todas as informações idênticas à que foi qualificada de ilegal por esse órgão jurisdicional.

58. Com efeito, conforme resulta da minha análise, um fornecedor de armazenamento pode ser obrigado a prevenir qualquer nova violação do mesmo tipo e do mesmo utilizador de um serviço da sociedade de informação [24]. Nesse caso, trata-se efetivamente de um caso específico de uma violação concretamente identificada, de modo que a obrigação de identificar, de entre as informações provenientes de um único utilizador, as informações idênticas à qualificada de ilegal não constitui uma obrigação geral de vigilância.

59. A meu ver, o mesmo acontece no que diz respeito às informações idênticas à que foi qualificada de ilegal, divulgadas por outros utilizadores. Estou consciente de que este raciocínio leva a que o alcance pessoal de uma obrigação de vigilância abranja qualquer utilizador e, portanto, a totalidade das informações divulgadas através de uma plataforma.

60. No entanto, uma obrigação de procurar e identificar informações idênticas à que foi qualificada de ilegal pelo órgão jurisdicional que foi chamado a decidir é sempre direcionada para o caso específico de uma violação. Além disso, trata-se, no caso em apreço, de uma obrigação imposta por um despacho de medidas provisórias, que produz os seus efeitos até que o processo seja definitivamente findo. Assim, tal obrigação imposta a um fornecedor de armazenamento é, pela própria natureza das coisas, limitada no tempo.

24 V. n.os 42 e 45 das presentes conclusões.

61. Por outro lado, a reprodução do mesmo conteúdo por qualquer utilizador de uma plataforma de rede social parece-me, regra geral, detetável com ajuda de ferramentas informáticas, e isto sem que o fornecedor de armazenamento seja obrigado a recorrer a uma filtragem ativa e não automática da totalidade das informações divulgadas através da sua plataforma.

62. Além disso, impor a obrigação de procurar e identificar todas as informações idênticas à que foi qualificada de ilegal permite assegurar um justo equilíbrio entre os direitos fundamentais em causa.

63. Em primeiro lugar, a procura e a identificação de informações idênticas à que foi qualificada de ilegal por um órgão jurisdicional que foi chamado a decidir não requerem meios técnicos sofisticados, passíveis de representar um encargo extraordinário. Por conseguinte, tal obrigação não se afigura consubstanciar um ataque excessivo ao direito à liberdade de empresa de que beneficia um fornecedor de armazenamento que explora uma plataforma de rede social, como a Facebook Ireland, ao abrigo do artigo 16.º da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»).

64. Mais, tendo em conta a facilidade de reprodução de informações no ambiente da Internet, a procura e a identificação de informações idênticas à que foi qualificada de ilegal mostram-se necessárias para assegurar uma proteção eficaz da vida privada e dos direitos de personalidade.

65. Por último, essa obrigação respeita o direito fundamental dos utilizadores da Internet à liberdade de expressão e de informação, garantido pelo artigo 11.º da Carta, na medida em que a proteção dessa liberdade não deve necessariamente ser assegurada de modo absoluto, mas deve ser contrabalançada com a proteção de outros direitos fundamentais. No que respeita às informações idênticas à que foi qualificada de ilegal, estas constituem, *a priori*, e, regra geral, repetições de uma violação concretamente qualificada de ilegal. Essas repetições deveriam ser objeto de uma qualificação idêntica, que pode, todavia, ser mitigada em função, nomeadamente, do contexto de uma declaração pretensamente ilegal. A este propósito, importa salientar que os terceiros que podem ser indiretamente afetados por medidas inibitórias não participam nos processos no âmbito dos quais são impostas essas medidas inibitórias. É nomeadamente por essa razão que deve ser assegurada a possibilidade de esses terceiros contestarem, perante um juiz, as medidas de execução adotadas por um fornecedor de armazenamento com base numa medida inibitória [25], não devendo essa possibilidade depender do facto de esse terceiro ser qualificado de parte num processo principal [26].

2) Informações semelhantes

66. No que respeita ao alcance material de uma obrigação de vigilância, a recorrente sustenta que um fornecedor de armazenamento pode ser sujeito à obrigação de retirar as declarações de conteúdo semelhante ao da declaração qualificada de ilegal, publicadas pelo mesmo utilizador. Em contrapartida, o Governo austríaco e a Comissão consideram que a possibilidade de impor tal obrigação depende do resultado da ponderação dos interesses em causa. Apenas a recorrente considera que é possível ordenar a um fornecedor de armazenamento que retire declarações de conteúdo semelhante ao da declaração que foi qualificada de ilegal, publicadas por outros utilizadores.

67. A referência às «informações semelhantes» ou às informações «de conteúdo semelhante» cria dificuldades de interpretação na medida em que o órgão jurisdicional de reenvio não especifica o sentido dessas expressões. No entanto, pode deduzir-se do reenvio prejudicial que a referência às informações «de conteúdo semelhante» visa as informações que *pouco divergem* da informação inicial ou as situações em que *a mensagem se mantém, em substância, inalterada*. Entendo essas indicações

25 V., por analogia, Acórdão de 27 de março de 2014, UPC Telekabel Wien (C-314/12, EU:C:2014:192, n.º 57).

26 V., por analogia, Acórdãos de 25 de maio de 2016, Meroni (C-559/14, EU:C:2016:349, n.ºs 49 e 50), e de 21 de dezembro de 2016, Biuro podróży «Partner» (C-119/15, EU:C:2016:987, n.º 40). Quanto à problemática do princípio da tutela jurisdicional efetiva em relação a terceiros, v., igualmente, Kalėda, S. L., «The Role of the Principle of Effective Judicial Protection in Relation to Website Blocking Injunctions», *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2017, pp. 222 e 223.

no sentido de que uma reprodução de informação que tenha sido qualificada de ilegal que contém um erro datilográfico ou algumas *nuances* na sintaxe ou pontuação, constitui uma «informação semelhante». Todavia, não é evidente que a semelhança referida na segunda questão não vá além desses casos.

68. É certo que resulta do Acórdão L'Oréal e o.[27] que o prestador de um serviço da sociedade de informação pode ser obrigado a tomar medidas que contribuam para prevenir *novas violações* da *mesma natureza* aos mesmos direitos.

69. Todavia, não se deve perder de vista o contexto factual em que foi desenvolvida a jurisprudência pertinente, a saber, o das violações do direito de propriedade intelectual. Regra geral, tais violações consistem na divulgação do mesmo conteúdo que o protegido ou, pelo menos, de um conteúdo parecido com o protegido, sendo que as eventuais alterações do mesmo, por vezes difíceis de introduzir, necessitam de uma intervenção específica.

70. Em contrapartida, não é habitual que um ato difamatório retome os termos exatos de um ato da mesma natureza. Tal decorre, em parte, do caráter personalizado do modo de exprimir ideias. Além disso, contrariamente às violações do direito de propriedade intelectual, os atos difamatórios ulteriores ao ato difamatório inicial reproduzem antes o facto de tecer considerações ofensivas da honra de uma pessoa do que a forma do ato inicial. Por esta razão, em matéria de difamação, a simples referência a atos da mesma natureza não pode desempenhar o mesmo papel que em matéria de violação do direito de propriedade intelectual.

71. Em todo o caso, a interpretação dada à referência às «informações semelhantes» é suscetível de afetar o alcance de uma obrigação de vigilância e o exercício dos direitos fundamentais em causa. Um órgão jurisdicional que, no quadro de uma medida inibitória, se pronuncie a respeito da remoção das «informações semelhantes» deve, assim, respeitar o princípio da segurança jurídica e garantir que os efeitos dessa medida inibitória sejam claros, precisos e previsíveis. Ao fazê-lo, esse órgão jurisdicional deve ponderar os direitos fundamentais em causa e ter em conta o princípio da proporcionalidade.

72. Sem prejuízo destas considerações, inspirando-me novamente no Acórdão L'Oréal e o.[28], sou de opinião que, *a fortiori*, um fornecedor de armazenamento pode ser obrigado a identificar informações semelhantes à informação qualificada de ilegal, provenientes do mesmo utilizador. De resto, também neste último caso, haveria que garantir a esse utilizador a possibilidade de contestar, perante um juiz, as medidas de execução adotadas por um fornecedor de armazenamento no cumprimento de uma medida inibitória.

73. Em contrapartida, a identificação de informações semelhantes à qualificada de ilegal, provenientes de outros utilizadores, exigiria a vigilância da totalidade das informações divulgadas através de uma plataforma de rede social. Ora, ao contrário das informações idênticas à que foi qualificada de ilegal, as informações semelhantes a esta não podem ser identificadas sem que um fornecedor de armazenamento recorra a soluções sofisticadas. Consequentemente, não só o papel de um prestador que exercesse uma vigilância geral deixaria de ser neutro, no sentido de não ser apenas técnico, automático e passivo, como também esse prestador, exercendo uma forma de censura, se tornaria um contribuinte ativo para essa plataforma.

27 Acórdão de 12 de julho de 2011 (C-324/09, EU:C:2011:474).

28 Acórdão de 12 de julho de 2011 (C-324/09, EU:C:2011:474).

74. Aliás, uma obrigação de identificação de informações semelhantes à qualificada de ilícita, provenientes de qualquer utilizador, não asseguraria um justo equilíbrio entre a proteção da vida privada e dos direitos de personalidade, a proteção da liberdade de empresa e a proteção da liberdade de expressão e de informação. Por um lado, a procura e a identificação de tais informações exigiriam soluções dispendiosas, que deveriam ser desenvolvidas e introduzidas pelo fornecedor de armazenamento. Por outro, a implementação dessas soluções conduziria a uma censura, podendo a liberdade de expressão e de informação ser sistematicamente restringida.

75. À luz das considerações que precedem, proponho responder à primeira e segunda questões, na medida em que as mesmas incidem sobre o alcance pessoal e material de uma obrigação de vigilância, que o artigo 15.º, n.º 1, da Diretiva 2000/31 deve ser interpretado no sentido de que não se opõe a que um fornecedor de armazenamento que explora uma plataforma de rede social seja obrigado, no quadro de uma medida inibitória, a procurar e identificar, de entre todas as informações divulgadas pelos utilizadores dessa plataforma, as informações idênticas à que foi qualificada de ilegal pelo órgão jurisdicional que impôs essa medida inibitória. No âmbito de tal medida, um fornecedor de armazenamento pode ser obrigado a procurar e identificar as informações semelhantes à qualificada de ilegal apenas de entre as informações divulgadas pelo utilizador que divulgou essa informação. Um órgão jurisdicional que imponha a remoção dessas informações semelhantes deve garantir que os efeitos da sua medida inibitória são claros, precisos e previsíveis. Ao fazê-lo, deve ponderar os direitos fundamentais em causa e ter em conta o princípio da proporcionalidade.

3. Quanto à remoção a nível mundial

a) Observações preliminares

76. Vou agora debruçar-me sobre as dúvidas do órgão jurisdicional de reenvio quanto ao alcance territorial de uma obrigação de remoção. Essas dúvidas dizem respeito, em substância, à questão de saber se um fornecedor de armazenamento pode ser obrigado a remover conteúdos que foram qualificados de ilegais ao abrigo do direito nacional de um Estado-Membro, não só nesse Estado-Membro, mas também a nível mundial.

77. A título preliminar, é verdade que a Facebook Ireland explora, enquanto filial da Facebook, uma plataforma eletrónica apenas para os utilizadores situados fora dos Estados Unidos e do Canadá. Todavia, essa circunstância não parece ser de natureza a excluir a remoção a nível mundial das informações divulgadas através dessa plataforma. Com efeito, a Facebook Ireland não contesta o facto de ser capaz de assegurar essa remoção a nível mundial.

78. Todavia, deve observar-se que o legislador da União não harmonizou as regras substantivas em matéria de violação da vida privada e dos direitos de personalidade, incluindo a difamação [29]. Além disso, na falta de consenso na União [30], o legislador da União também não harmonizou as regras de conflito nessa matéria [31]. Assim, para conhecer das ações intentadas por difamação, cada órgão jurisdicional da União recorre à lei designada como aplicável nos termos das regras nacionais de conflito.

29 V. Savin, A., *EU Internet law*, Elgar European Law, Cheltenham — Northampton, 2017, p. 130.

30 V. Van Calster, G., *European Private International Law*, Hart Publishing, Oxford, Portland, 2016, pp. 248 a 251.

31 V. artigo 1.º, n.º 2, do Regulamento (CE) n.º 864/2007 do Parlamento Europeu e do Conselho, de 11 de julho de 2007, relativo à lei aplicável às obrigações extracontratuais («Roma II») (JO 2007, L 199, p. 40).

79. A situação em causa no processo principal é, *a priori*, diferente da que constituía o ponto de partida da minha análise relativa ao alcance territorial de uma supressão de uma hiperligação nos resultados de um motor de busca no processo Google (Alcance territorial da supressão de uma hiperligação) [32], evocado pela Facebook Ireland e pelo Governo letão. Esse processo diz respeito à Diretiva 95/46/CE [33], que harmoniza, na União, determinadas regras materiais relativas à proteção de dados. É, nomeadamente, o facto de as regras nessa matéria serem harmonizadas que me leva a concluir que um prestador deveria ser obrigado a suprimir os resultados apresentados na sequência de uma pesquisa efetuada não apenas a partir de um único Estado-Membro ou, igualmente, a partir de um Estado terceiro, mas a partir de um local situado na União [34]. Todavia, nas minhas conclusões apresentadas nesse processo, não excluí que pudessem existir situações em que o interesse da União exigisse uma aplicação das disposições dessa diretiva além do território da União [35].

80. Por conseguinte, no que respeita às ofensas difamatórias, a imposição num Estado-Membro de uma obrigação que consiste em remover determinadas informações a nível mundial, para todos os utilizadores de uma plataforma eletrónica, em razão da ilicitude dessas informações, determinada ao abrigo de uma lei aplicável, levaria a que a declaração do seu caráter ilegal produzisse efeitos noutros Estados. Por outras palavras, a declaração do caráter ilegal das informações em causa estender-se-ia aos territórios desses outros Estados. Todavia, não está excluído que, de acordo com as leis designadas como aplicáveis ao abrigo das regras nacionais de conflito desses Estados, essa informação possa ser considerada lícita.

81. Conforme ilustra o debate entre os interessados, por um lado, a reticência em conceder tais efeitos extraterritoriais a medidas inibitórias reflete a posição da Facebook Ireland, bem como a dos Governos letão, português e finlandês. Por outro lado, com exceção do Governo português, esses interessados parecem igualmente ter dúvidas sobre o âmbito territorial da competência dos órgãos jurisdicionais de um Estado-Membro. Em substância, os referidos interessados parecem considerar que o órgão jurisdicional de um Estado-Membro não pode decidir, no quadro de uma medida inibitória imposta a um fornecedor de armazenamento, a remoção de conteúdos fora do território desse Estado-Membro. Assim, há que analisar estas duas questões, a saber, o alcance territorial de uma obrigação de remoção e o âmbito da competência dos órgãos jurisdicionais de um Estado-Membro, examinando, em primeiro lugar, a questão da competência, que, regra geral, precede a apreciação do mérito.

b) Quanto ao âmbito territorial da competência

82. A Diretiva 2000/31 não regula a competência para decidir sobre a imposição de medidas inibitórias. Em contrapartida, conforme resulta do Acórdão eDate Advertising e o. [36], em caso de alegada violação dos direitos de personalidade através de conteúdos colocados em linha num sítio na Internet, uma pessoa que se considerar lesada tem a faculdade de recorrer aos órgãos jurisdicionais dos Estados-Membros competentes ao abrigo do Regulamento (UE) n.º 1215/2012 [37]. Com efeito, se as regras de conflito em matéria de difamação não são harmonizadas na União, o mesmo já não acontece no que respeita às regras de competência.

32 Refiro-me aqui às minhas Conclusões no processo Google (Alcance territorial da supressão de uma hiperligação) (C-507/17, EU:C:2019:15).

33 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).

34 V. as minhas Conclusões no processo Google (Alcance territorial da supressão de uma hiperligação) (C-507/17, EU:C:2019:15, n.os 47, 55, 76 e 77).

35 V. as minhas Conclusões no processo Google (Alcance territorial da supressão de uma hiperligação) (C-507/17, EU:C:2019:15, n.º 62).

36 Acórdão de 25 de outubro de 2011 (C-509/09 e C-161/10, EU:C:2011:685, n.os 43 e 44).

37 Regulamento do Parlamento e do Conselho de 12 de dezembro de 2012, relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial (JO 2012, L 35, p. 1).

83. A este respeito, cabe acrescentar que as regras de competência do Regulamento n.º 1215/2012 se aplicam igualmente aos litígios em matéria de supressão dos conteúdos difamatórios colocados em linha [38]. Além disso, pouco importa que, no caso em apreço, tal pedido seja apresentado, não contra um emitente, mas contra um fornecedor de armazenamento dos conteúdos colocados em linha. Posto isto, não proporei que o Tribunal de Justiça reformule as questões prejudiciais, na medida em que apenas os interessados têm dúvidas sobre o âmbito territorial da competência. No entanto, gostaria de formular algumas observações a este respeito.

84. Segundo o Acórdão eDate Advertising e o. [39], quem se considerar lesado pode recorrer, nomeadamente, aos órgãos jurisdicionais do Estado-Membro onde se encontra o centro dos seus interesses. Esses órgãos jurisdicionais são competentes para decidir sobre a totalidade do dano causado. Parece que, no caso em apreço, o órgão jurisdicional chamado a conhecer do litígio pela recorrente é o do lugar do centro dos interesses desta [40].

85. É verdade que, no Acórdão eDate Advertising e o. [41], o Tribunal de Justiça indicou que uma pessoa que se considere lesada pode, em função do lugar da materialização do dano causado na União, intentar uma ação num determinado foro pela integralidade desse dano. É verdade que isto pode levar a pensar que o âmbito territorial da competência desse foro não englobaria os factos relativos aos territórios dos Estados terceiros. Todavia, esta consideração reflete mais o facto de um foro, para ser competente nos termos do Regulamento n.º 1215/2012 ao abrigo do critério do lugar da materialização do dano, dever ser um órgão jurisdicional de um Estado-Membro. Por outro lado, exceção feita a esta consideração, o Tribunal de Justiça referiu reiteradamente nesse acórdão que esse foro era competente para decidir sobre a totalidade dos danos resultantes da difamação [42].

86. Daqui deduzo que, contrariamente ao que sustentam a Facebook Ireland e os Governos letão e finlandês, o órgão jurisdicional de um Estado-Membro pode, em princípio, decidir sobre a remoção de conteúdos fora do território desse Estado-Membro, tendo o âmbito territorial da sua competência caráter universal [43]. Um órgão jurisdicional de um Estado-Membro pode ser impedido de decidir sobre uma remoção a nível mundial, não devido a uma questão de competência, mas, eventualmente, a uma questão de mérito.

87. Importa agora analisar a questão dos efeitos extraterritoriais das medidas inibitórias impostas aos fornecedores de armazenamento que, no caso em apreço, conforme indiquei no n.º 81 das presentes conclusões, se resume à questão do alcance territorial de uma obrigação de remoção.

38 Acórdão de 17 de outubro de 2017, Bolagsupplysningen e Ilsjan (C-194/16, EU:C:2017:766, n.º 44).

39 Acórdão de 25 de outubro de 2011 (C-509/09 e C-161/10, EU:C:2011:685, n.º 48).

40 Consequentemente, apesar de o órgão jurisdicional de reenvio ser chamado a pronunciar-se sobre um despacho de medidas provisórias, não se impõe questionar as implicações do artigo 35.º do Regulamento n.º 1215/2012 sobre o âmbito territorial da competência e sobre o alcance territorial de uma obrigação de remoção imposta no quadro de uma medida inibitória.

41 Acórdão de 25 de outubro de 2011 (C-509/09 e C-161/10, EU:C:2011:685, n.º 48).

42 Acórdão de 25 de outubro de 2011, eDate Advertising e o. (C-509/09 e C-161/10, EU:C:2011:685, n.ºs 48, 51 e 52). V., igualmente, Acórdão de 17 de outubro de 2017, Bolagsupplysningen e Ilsjan (C-194/16, EU:C:2017:766, n.ºs 38 e 47). Por outro lado, segundo as interpretações doutrinais desse acórdão, o foro do local do centro de interesses é competente para decidir no mundo inteiro sobre os danos causados. V. Mankowski, P., *in* Magnus, U., e Mankowski, P. (sob a direção de), Brussels I bis Regulation — Commentary, Otto Schmidt, Colónia, 2016, artigo 7.º, n.º 364. O mesmo acontece no que respeita ao âmbito territorial da competência geral do foro do demandado. No Acórdão de 1 de março de 2005, Owusu (C-281/02, EU:C:2005:120, n.º 26), o Tribunal de Justiça considerou que a Convenção de Bruxelas [Convenção de 27 de setembro de 1968 relativa à Competência Jurisdicional e à Execução de Decisões em Matéria Civil e Comercial (JO 1972, L 299, p. 32)] pode aplicar-se quando o demandante e o demandado têm domicílio num Estado-Membro, enquanto os factos controvertidos estão localizados num Estado terceiro. Daqui deduzo que, nesse caso, é o foro do devedor o competente para decidir tais factos controvertidos. V, igualmente, Van Calster, G., Luks, C., Extraterritoriality and private international law, Recht in beweging - 19de VRG Alumnidag 2012, MAKLU, Anvers — Apeldoorn, 2012, p. 132.

43 Por conseguinte, trata-se aqui de uma competência dita «global» ou «geral». V. Larsen, T.B., «The extent of jurisdiction under the forum delicti rule in European trademark litigation», *Journal of Private International Law*, 2018, vol. 14, n.º 3, pp. 550 e 551.

c) Quanto ao alcance territorial de uma obrigação de remoção

88. Em primeiro lugar, deve observar-se que, conforme admite o Governo finlandês, o artigo 15.º, n.º 1, da Diretiva 2000/31 não regula os efeitos territoriais das medidas inibitórias impostas aos prestadores de serviços da sociedade de informação. Além disso, sob reserva de satisfazer as exigências prescritas pela Diretiva 2000/31, as obrigações de remoção impostas a esses prestadores no quadro de medidas inibitórias relevam do direito nacional.

89. Em seguida, na falta de regulamentação da União em matéria de violação da vida privada e dos direitos de personalidade, é difícil justificar os efeitos territoriais de uma medida inibitória invocando a proteção dos direitos fundamentais garantidos pelos artigos 1.º, 7.º e 8.º da Carta. Com efeito, o âmbito de aplicação da Carta acompanha o âmbito de aplicação do direito da União e não o contrário [44] e, no caso vertente, quanto ao mérito, o recurso da recorrente não se baseia no direito da União.

90. A este respeito, deve observar-se que a recorrente não parece invocar os direitos em matéria de proteção de dados pessoais e que não acusa a Facebook Ireland de ter «procedido» a um tratamento ilícito dos seus dados, baseando-se o seu pedido nas disposições gerais do direito civil. Além disso, o órgão jurisdicional de reenvio não invoca instrumentos jurídicos do direito da União pertinentes nesta matéria. Invoca apenas a Diretiva 2000/31. Ora, resulta do artigo 1.º, n.º 5, alínea b), dessa diretiva que a mesma não se aplica às questões respeitantes aos serviços da sociedade da informação, as quais são abrangidas pelas diretivas relativas à proteção dos dados pessoais.

91. Por último, se se pode tirar ensinamentos do Regulamento n.º 1215/2012 no que respeita aos efeitos produzidos pelas medidas inibitórias nos Estados-Membros, tal não acontece no que se refere aos efeitos produzidos fora da União. Com efeito, esse regulamento não exige que uma medida inibitória imposta pelo órgão jurisdicional de um Estado-Membro produza efeitos igualmente em Estados terceiros. Mais, o facto de um órgão jurisdicional ser competente para decidir do mérito ao abrigo de uma regra de competência do direito da União não implica que, ao fazê-lo, aplique unicamente regras materiais abrangidas pelo âmbito de aplicação do direito da União e, portanto, da Carta.

92. Por estas razões, tanto a questão dos efeitos extraterritoriais de uma medida inibitória que imponha uma obrigação de remoção como a questão do alcance territorial dessa obrigação deveriam ser objeto de uma análise à luz, não do direito da União, mas, nomeadamente, do direito internacional público e privado não harmonizado na União [45]. Com efeito, nada indica que a situação que é objeto do processo principal possa estar abrangida pelo âmbito de aplicação do direito da União e, portanto, das regras de direito internacional que têm incidência na interpretação do direito da União [46].

93. Por conseguinte, quanto ao alcance territorial de uma obrigação de remoção imposta a um fornecedor de armazenamento no âmbito de uma medida inibitória, importa considerar que a mesma não é regulada nem pelo artigo 15.º, n.º 1, da Diretiva 2000/31 nem por nenhuma outra disposição dessa diretiva e, por conseguinte, que essa disposição não se opõe a que um fornecedor de armazenamento seja obrigado a remover informações divulgadas através de uma plataforma de rede social a nível mundial. Por outro lado, o referido alcance territorial também não é regulado pelo direito da União, na medida em que, no caso em apreço, o recurso da recorrente não é baseado nesse direito.

44 V. Acórdão de 26 de fevereiro de 2013, Åkerberg Fransson (C-617/10, EU:C:2013:105, n.º 19). V., igualmente, as minhas Conclusões no processo Google (Alcance territorial da supressão de uma hiperligação) (C-507/17, EU:C:2019:15, n.º 55).

45 Quanto aos efeitos extraterritoriais das decisões judiciais, é por vezes difícil traçar um limite entre o direito internacional público e privado. V. Maier, H.G, «Extraterritorial Jurisdiction at a Crossroads: An Intersection between Public and Private International Law», *The American Journal of International Law*, vol. 76, n.º 2, p. 280, e Svantesson, D.J.B., *Solving the Internet Jurisdiction Puzzle*, Oxford University Press, Oxford, 2017, p. 40.

46 V., neste sentido, Despacho de 12 de julho de 2012, Currà e o. (C-466/11, EU:C:2012:465, n.º 19).

94. Assim sendo, tanto por razões de exaustividade como na hipótese de o Tribunal de Justiça não seguir a minha proposta, formularei algumas observações adicionais no que respeita à remoção das informações divulgadas através de uma plataforma de rede social a nível mundial.

95. Nos termos do direito internacional, não é de excluir que uma medida inibitória possa produzir efeitos ditos «extraterritoriais» [47]. Ora, conforme indiquei no n.º 80 das presentes conclusões, tal abordagem levaria a que a declaração do caráter ilícito das informações em causa se estendesse aos territórios de outros Estados-Membros, independentemente do caráter lícito ou não dessas informações ao abrigo da lei designada como aplicável nos termos das regras de conflito desses Estados-Membros.

96. Assim, poder-se-ia argumentar que o Tribunal de Justiça já admitiu implicitamente essa abordagem no Acórdão Bolagsupplysningen e Ilsjan [48]. É verdade que, nesse acórdão, o Tribunal de Justiça não se pronunciou de forma alguma sobre a lei aplicável a um pedido de supressão dos conteúdos colocados em linha. Todavia, o Tribunal de Justiça declarou que, tendo em conta *a natureza ubiquitária dos conteúdos colocados em linha num sítio Internet* e o facto de *o alcance da sua divulgação ser em princípio universal*, um pedido que visa, designadamente, a supressão desses conteúdos deve ser apresentado num órgão jurisdicional competente para conhecer da totalidade do pedido de reparação do dano. Ao fazê-lo, em minha opinião, esse órgão jurisdicional aplicaria a lei ou as leis designadas como aplicáveis ao abrigo das suas regras de conflito [49]. Não é de excluir que um órgão jurisdicional de um Estado-Membro aplique, nesse contexto, uma única lei designada como aplicável.

97. No entanto, se esse órgão jurisdicional não pudesse decidir sobre a supressão dos conteúdos colocados em linha a nível mundial, colocar-se-ia então a questão de saber que órgão jurisdicional estaria mais bem colocado para se pronunciar sobre essa supressão. De facto, cada órgão jurisdicional seria confrontado com as contrariedades descritas no número anterior. Além disso, deve exigir-se que um demandante, apesar dessas dificuldades práticas, demonstre que a informação qualificada de ilegal, nos termos da lei designada como aplicável ao abrigo das normas de conflito do Estado-Membro em causa, é ilícita de acordo com todas as leis potencialmente aplicáveis?

98. Mesmo que se admitisse que as considerações relativas ao caráter territorial da proteção decorrente das normas materiais em matéria de violação da vida privada e dos direitos de personalidade não obstam a tal exigência, haveria ainda que ter em conta os direitos fundamentais reconhecidos à escala mundial.

99. Com efeito, conforme referi num contexto diferente, o interesse legítimo do público em aceder a uma informação vai necessariamente variar consoante a sua localização geográfica, de um Estado terceiro para outro [50]. Por isso, tratando-se de uma remoção a nível mundial, existiria o perigo de que tal remoção, uma vez posta em prática, impedisse que pessoas que se encontrassem em Estados diferentes do Estado do órgão jurisdicional chamado a conhecer do litígio acedessem à informação.

100. Para concluir, resulta das considerações precedentes que o órgão jurisdicional de um Estado-Membro pode, em teoria, decidir sobre a remoção de informações divulgadas através da Internet a nível mundial. Todavia, devido às diferenças existentes entre, por um lado, as leis nacionais e, por outro, a proteção da vida privada e dos direitos de personalidade nelas prevista, e a fim de

47 Douglas, M., «*Extraterritorial injunctions affecting the internet*», *Journal of Equity*, 2018, vol. 12, p. 48; Riordan, J., *The Liability of Internet Intermediaries*, Oxford University Press, Oxford, 2011, p. 418.

48 Acórdão de 17 de outubro de 2017 (C-194/16, EU:C:2017:766, n.º 44).

49 V., igualmente, no que diz respeito às implicações deste acórdão, Lundstedt, L., «Putting Right Holders in the Centre: Bolagsupplysningen and Ilsjan (C-194/16): What Does It Mean for International Jurisdiction over Transborder Intellectual Property Infringement Disputes?», *International Review of Intellectual Property and Competition Law*, 2018, vol. 49, n.º 9, p. 1030, e Svantesson, D. J. B., «European Union Claims of Jurisdiction over the Internet — an Analysis of Three Recent Key Developments», *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2018, vol. 9, n.º 2, p. 122, n.º 59.

50 V. as minhas Conclusões no processo Google (Alcance territorial da supressão de uma hiperligação) (C-507/17, EU:C:2019:15, n.º 60).

respeitar os direitos fundamentais amplamente difundidos, esse órgão jurisdicional deve antes adotar uma atitude de autolimitação. Deste modo, no respeito da cortesia internacional [51], evocada pelo Governo português, esse órgão jurisdicional deveria, na medida do possível, limitar os efeitos extraterritoriais das suas medidas inibitórias em matéria de violação da vida privada e dos direitos de personalidade [52]. A imposição de uma obrigação de remoção não deve ir além do necessário para alcançar a proteção da pessoa lesada. Assim, em vez de suprimir o conteúdo, o referido órgão jurisdicional poderia eventualmente ordenar que o acesso a essas informações se tornasse impossível com o auxílio do geobloqueio.

101. Estas considerações não são postas em causa pelo argumento da recorrente segundo o qual o geobloqueio das informações ilegais é facilmente contornável por um servidor *proxy* ou por outros meios.

102. Para retomar uma reflexão formulada no contexto de situações que relevam do direito da União: a proteção da vida privada e dos direitos de personalidade não deve necessariamente ser assegurada de modo absoluto, mas deve ser contrabalançada com a proteção de outros direitos fundamentais [53]. Assim, há que evitar medidas exorbitantes que ignorem o cuidado de assegurar um justo equilíbrio entre os diferentes direitos fundamentais [54].

103. Sem prejuízo das precedentes observações adicionais, no que respeita ao alcance territorial de uma obrigação de remoção, mantenho a posição já avançada no n.º 93 das presentes conclusões.

B. Quanto à terceira questão prejudicial

104. Com a sua terceira questão, o órgão jurisdicional de reenvio pretende saber se o artigo 15.º da Diretiva 2000/31 se opõe a que uma medida inibitória imponha ao fornecedor de armazenamento a obrigação de remover da sua plataforma informações semelhantes à que foi julgada ilegal no âmbito de um processo judicial após ter tomado conhecimento dessas informações.

105. A recorrente e os Governos austríaco, letão, português e finlandês consideram, em substância, que o artigo 15.º, n.º 1, da Diretiva 2000/31 não obsta a que seja ordenado a um fornecedor de armazenamento que remova informações de conteúdo semelhante ao que foi julgado ilícito, quando tenha tomado conhecimento do mesmo. Tendo em conta a sua análise da primeira questão, a Facebook Ireland considera que não há que responder à terceira questão.

106. Adiro ao ponto de vista partilhado, em substância, pela recorrente e pelo conjunto dos governos.

107. Com efeito, se uma obrigação de remoção não implicar uma vigilância geral das informações armazenadas por um fornecedor de armazenamento, mas decorrer de uma tomada de conhecimento resultante da notificação efetuada pela pessoa em causa ou por terceiros, não há violação da proibição prevista no artigo 15.º, n.º 1, da Diretiva 2000/31.

51 V., nomeadamente, sobre as implicações práticas dessa cortesia internacional, Maier, H. G, *op. cit.*, p. 283.

52 V. doutrina citada na nota 47. V., igualmente, em contextos bem diferentes dos do presente processo, Scott, J., «The New EU "Extraterritoriality"», *Common Market Law Review*, 2014, vol. 51, n.º 5, p. 1378.

53 V., por analogia, no que respeita à ponderação do direito de propriedade intelectual e do direito ao respeito da vida privada e familiar, garantido pelo artigo 7.º da Carta, Acórdão de 18 de outubro de 2018, Bastei Lübbe (C-149/17, EU:C:2018:841, n.ºs 44 a 47). V., igualmente, as minhas Conclusões no processo Bastei Lübbe (C-149/17, EU:C:2018:400, n.ºs 37 a 39).

54 V., neste sentido, no que respeita à proteção da propriedade intelectual, Acórdão de 27 de março de 2014, UPC Telekabel Wien (C-314/12, EU:C:2014:192, 58 a 63). V., igualmente, Conclusões do advogado-geral P. Cruz Villalón no processo UPC Telekabel Wien (C-314/12, EU:C:2013:781, n.ºs 99 a 101), e as minhas Conclusões no processo Stichting Brein (C-610/15, EU:C:2017:99, n.ºs 69 a 72).

108. Por conseguinte, proponho responder à terceira questão prejudicial que o artigo 15.º, n.º 1, da Diretiva 2000/31 deve ser interpretado no sentido de que não se opõe a que um fornecedor de armazenamento seja obrigado a remover informações semelhantes à que foi qualificada de ilegal, se a obrigação de remoção não implicar uma vigilância geral das informações armazenadas e decorrer de uma tomada de conhecimento resultante da notificação efetuada pela pessoa em causa, por terceiros ou por outra fonte.

VI. Conclusão

109. À luz do conjunto das considerações precedentes, proponho que o Tribunal de Justiça responda da seguinte forma às questões prejudiciais submetidas pelo Oberster Gerichtshof (Supremo Tribunal, Áustria):

1) O artigo 15.º, n.º 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»), deve ser interpretado no sentido de que não se opõe a que um fornecedor de armazenamento que explora uma plataforma de rede social seja obrigado, no quadro de uma medida inibitória, a procurar e identificar, de entre todas as informações divulgadas pelos utilizadores dessa plataforma, as informações idênticas à que foi qualificada de ilegal pelo órgão jurisdicional que impôs essa medida inibitória. No âmbito dessa medida inibitória, um fornecedor de armazenamento pode ser obrigado a procurar e identificar as informações semelhantes à qualificada de ilegal apenas de entre as informações divulgadas pelo utilizador que divulgou essa informação. Um órgão jurisdicional que imponha a remoção dessas informações semelhantes deve garantir que os efeitos da sua medida inibitória são claros, precisos e previsíveis. Ao fazê-lo, deve ponderar os direitos fundamentais em causa e ter em conta o princípio da proporcionalidade.

2) Quanto ao alcance territorial de uma obrigação de remoção imposta a um fornecedor de armazenamento no âmbito de uma medida inibitória, há que considerar que a mesma não é regulada nem pelo artigo 15.º, n.º 1, da Diretiva 2000/31 nem por nenhuma outra disposição dessa diretiva e, por conseguinte, que essa disposição não se opõe a que um fornecedor de armazenamento seja obrigado a remover informações divulgadas através de uma plataforma de rede social a nível mundial. Por outro lado, o referido alcance territorial também não é regulado pelo direito da União, na medida em que, no caso em apreço, o recurso da recorrente não é baseado nesse direito.

3) O artigo 15.º, n.º 1, da Diretiva 2000/31 deve ser interpretado no sentido de que não se opõe a que um fornecedor de armazenamento seja obrigado a remover informações semelhantes à que foi qualificada de ilegal, se a obrigação de remoção não implicar uma vigilância geral das informações armazenadas e decorrer de uma tomada de conhecimento resultante da notificação efetuada pela pessoa em causa, por terceiros ou por outra fonte.