Recueil de la jurisprudence

CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. MACIEJ SZPUNAR
présentées le 4 juin 2019 [1]

Affaire C-18/18

Eva Glawischnig-Piesczek
contre
Facebook Ireland Limited

[demande de décision préjudicielle formée par l'Oberster Gerichtshof (Cour suprême, Autriche)]

« Renvoi préjudiciel – Libre prestation de services – Directive 2000/31/CE – Services de la société de l'information – Responsabilité des prestataires intermédiaires – Obligation d'un prestataire de services d'hébergement de sites Internet (Facebook) d'effacer des informations illicites – Portée »

I. Introduction

1. *Sur Internet on n'écrit pas au crayon mais à l'encre*, constate un personnage d'un film américain sorti en 2010. Je me réfère ici, et ce n'est pas hasard, au film *The Social Network*.

2. En effet, au cœur de la présente affaire se pose la question de savoir si un hébergeur qui exploite une plateforme de réseau social en ligne peut être tenu de faire disparaître, à l'aide d'un efface-encre métaphorique, certains contenus mis en ligne par des utilisateurs de cette plateforme.

3. Plus précisément, par ses questions préjudicielles, la juridiction de renvoi invite la Cour à préciser les portées personnelle et matérielle des obligations qui peuvent être imposées à un hébergeur, sans que cela conduise à imposer une obligation générale en matière de surveillance, interdite en vertu de l'article 15, paragraphe 1, de la directive 2000/31/CE [2]. La juridiction de renvoi demande également à la Cour de juger si, dans le cadre d'une injonction rendue par la juridiction d'un État membre, un hébergeur peut être contraint de retirer certains contenus non seulement pour les internautes de cet État membre, mais également au niveau mondial.

II. Le cadre juridique

A. Le droit de l'Union

4. Les articles 14 et 15 de la directive 2000/31 figurent dans la section 4, intitulée « Responsabilité des prestataires intermédiaires », du chapitre II de cette directive.

1 Langue originale : le français.

2 Directive du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique ») (JO 2000, L 178, p. 1).

5. L'article 14, paragraphes 1 et 3, de la directive 2000/31, intitulé « Hébergement », dispose :

« 1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que :

a) le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente

ou

b) le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

[...]

3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation et n'affecte pas non plus la possibilité, pour les États membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible. »

6. L'article 15, paragraphe 1, de la directive 2000/31, intitulé « Absence d'obligation générale en matière de surveillance », dispose :

« Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites. »

B. Le droit autrichien

7. Aux termes de l'article 18, paragraphe 1, du E-Commerce-Gesetz (loi sur le commerce électronique), par laquelle le législateur autrichien a transposé la directive 2000/31, les prestataires de services d'hébergement n'ont pas d'obligation générale de surveiller les informations qu'ils stockent, transmettent ou rendent accessibles, ni de rechercher d'eux-mêmes des faits ou des circonstances révélant des activités illicites.

8. Conformément à l'article 1330, paragraphe 1, de l'Allgemeines Bürgerliches Gesetzbuch (code civil général, ci-après l'« ABGB »), quiconque ayant subi un préjudice réel ou un manque à gagner en raison d'une atteinte portée à son honneur est fondé à en demander réparation. En vertu du paragraphe 2 de cet article, il en va de même lorsqu'une personne rapporte des faits portant atteinte à la réputation, à la situation matérielle et aux perspectives d'avenir de tiers et dont elle connaissait ou aurait dû connaître l'inexactitude. Dans ce cas, le démenti et la publication de celui-ci peuvent être exigés.

9. En application de l'article 78, paragraphe 1, de l'Urheberrechtsgesetz (loi sur le droit d'auteur, ci-après l'« UrhG »), les images représentant une personne ne doivent pas être exposées publiquement ni diffusées d'une autre manière qui les rendraient accessibles au public, si cela porte atteinte aux intérêts légitimes de la personne concernée ou, si celle-ci est morte sans en avoir autorisé ou ordonné la publication, à ceux d'un parent proche.

III. Les faits du litige au principal

10. Mme Eva Glawischnig-Piesczek était députée au Nationalrat (Conseil national, Autriche), présidente du groupe parlementaire *die Grünen* (« les Verts ») et porte-parole fédérale de ce parti.

11. Facebook Ireland Limited, société immatriculée en Irlande ayant son siège à Dublin, est une filiale de la société américaine Facebook Inc. Facebook Ireland exploite, pour les utilisateurs situés hors des États-Unis et du Canada, une plateforme de réseau social en ligne, accessible à l'adresse www.facebook.com. Cette plateforme permet aux utilisateurs de créer des pages de profil et de publier des commentaires.

12. Le 3 avril 2016, un utilisateur de ladite plateforme a partagé, sur sa page personnelle, un article du magazine d'information autrichien en ligne *oe24.at* intitulé « Les Verts : en faveur du maintien d'un revenu minimal pour les réfugiés ». Cette publication a eu pour effet de générer sur cette plateforme un « aperçu vignette » du site d'origine, comportant le titre et un bref résumé de cet article, ainsi qu'une photographie de la requérante. Cet utilisateur a en outre publié, à propos de cet article, un commentaire d'accompagnement dégradant à l'égard de la requérante en lui reprochant d'être une « sale traîtresse du peuple », une « idiote corrompue » et un membre d'un « parti de fascistes ». Les contenus mis en ligne par cet utilisateur pouvaient être consultés par chaque utilisateur de la plateforme en cause.

13. Par lettre du 7 juillet 2016, la requérante a, notamment, demandé à Facebook Ireland d'effacer ce commentaire.

14. Facebook Ireland n'ayant pas retiré le commentaire en cause, la requérante a introduit un recours devant le Handelsgericht Wien (tribunal de commerce de Vienne, Autriche) et a demandé à ce tribunal de rendre une ordonnance de référé ordonnant à Facebook Ireland de cesser de publier et/ou de diffuser des photos de la requérante dès lors que le message d'accompagnement diffuse des allégations identiques et/ou de « contenu équivalent », à savoir que la requérante serait une « sale traîtresse du peuple » et/ou une « idiote corrompue » et/ou membre d'un « parti de fascistes ».

15. Le 7 décembre 2016, le Handelsgericht Wien (tribunal de commerce de Vienne) a rendu l'ordonnance de référé demandée.

16. Par la suite, Facebook Ireland a rendu l'accès au contenu initialement publié impossible en Autriche.

17. Saisi en appel, l'Oberlandesgericht Wien (tribunal régional supérieur de Vienne, Autriche) a confirmé l'ordonnance rendue en première instance s'agissant des allégations identiques. Cela faisant, ce tribunal n'a pas fait droit à la demande de Facebook Ireland visant à limiter l'ordonnance de référé à la République d'Autriche. En revanche, ledit tribunal a jugé que l'obligation de cesser la diffusion d'allégations de contenu équivalent visait uniquement celles portées à la connaissance de Facebook Ireland par la requérante au principal, par des tiers ou d'une autre manière.

18. Les tribunaux de première et deuxième instances ont fondé leurs décisions sur l'article 78 de l'UrhG et l'article 1330 de l'ABGB, en considérant, notamment, que le commentaire publié contenait des déclarations portant une atteinte excessive à l'honneur de la requérante et laissait entendre que celle-ci aurait eu un comportement délictueux, sans fournir la moindre preuve à cet égard. En outre, selon ces tribunaux, en matière de déclarations formulées à l'encontre d'une personnalité politique, sans rapport avec un débat politique ou d'intérêt général, toute référence au droit à la liberté d'expression serait également inadmissible.

19. Les deux parties au principal ont formé des recours devant l'Oberster Gerichtshof (Cour suprême, Autriche), qui a considéré que les déclarations en cause visaient à porter atteinte à l'honneur de la requérante, à l'injurier et à la diffamer.

20. La juridiction de renvoi est appelée à statuer sur la question de savoir si l'injonction de cessation, délivrée à l'encontre d'un hébergeur qui exploite un réseau social comptant de nombreux utilisateurs, peut aussi être étendue, au niveau mondial, aux déclarations textuellement identiques et/ou de contenu équivalent dont il n'a pas connaissance.

21. À cet égard, l'Oberster Gerichtshof (Cour suprême) indique que, selon sa propre jurisprudence, une telle obligation doit être considérée comme étant proportionnée lorsque le prestataire a déjà pris connaissance d'au moins une atteinte aux intérêts de la personne concernée causée par la contribution d'un destinataire du service et que le risque que soient commises d'autres violations est ainsi avéré.

IV. Les questions préjudicielles et la procédure devant la Cour

22. C'est dans ces circonstances que l'Oberster Gerichtshof (Cour suprême), par décision du 25 octobre 2017, parvenue à la Cour le 10 janvier 2018, a décidé de surseoir à statuer et de soumettre les questions suivantes à l'appréciation de la Cour :

« 1) L'article 15, paragraphe 1, de la directive [2000/31] s'oppose-t-il, d'une manière générale, à ce que l'une des obligations énumérées ci-après soit imposée à un hébergeur qui n'a pas promptement retiré certaines informations illicites, à savoir non seulement ces informations illicites elles-mêmes au sens de l'article 14, paragraphe 1, sous a), de [cette] directive, mais également d'autres informations identiques :

   a) au niveau mondial ?

   b) dans l'État membre concerné ?

   c) du destinataire concerné du service au niveau mondial ?

   d) du destinataire concerné du service dans l'État membre concerné ?

2) En cas de réponse négative à la première question : en va-t-il de même concernant les informations de contenu équivalent ?

3) En va-t-il de même concernant les informations de contenu équivalent dès le moment où l'exploitant a connaissance de cette circonstance ? »

23. Des observations écrites ont été déposées par la requérante, Facebook Ireland, les gouvernements autrichien, letton, portugais et finlandais ainsi que par la Commission européenne. Les mêmes intéressés, à l'exception du gouvernement portugais, ont été représentés lors de l'audience qui s'est tenue le 13 février 2019.

V. Analyse

A. Sur les première et deuxième questions préjudicielles

24. Par ses première et deuxième questions, qui doivent être examinées conjointement, la juridiction de renvoi demande à la Cour de déterminer les portées matérielle et personnelle d'une obligation de surveillance qui peut être imposée, dans le cadre d'une injonction, au prestataire d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire de ce service (un hébergeur), sans que cela conduise à imposer une obligation générale en matière de surveillance, interdite par l'article 15, paragraphe 1, de la directive 2000/31.

25. Certes, ces deux premières questions visent le retrait des informations diffusées au moyen d'une plateforme de réseau social en ligne plutôt que la surveillance ou le filtrage de celles-ci. Il convient toutefois d'observer que les plateformes de réseau social constituent des médias dont le contenu est généré principalement non pas par leurs sociétés fondatrices et gérantes mais par leurs utilisateurs. Au surplus, ce contenu, reproduit et modifié entretemps, fait l'objet d'échanges constants entre les utilisateurs.

26. Un hébergeur, pour pouvoir supprimer une information diffusée au moyen d'une telle plateforme ou rendre son accès impossible, quel que soit l'auteur de cette information et quel que soit son contenu, doit au préalable identifier cette information parmi celles stockées sur ses serveurs. Pour ce faire, il doit, d'une manière ou d'une autre, surveiller ou filtrer ces informations. Or, selon l'article 15, paragraphe 1, de la directive 2000/31, visé dans les questions préjudicielles, un État membre ne peut pas imposer à un hébergeur une obligation générale en matière de surveillance. Tout cela implique que, par ses deux premières questions, la juridiction de renvoi s'interroge, en substance, sur les portées personnelle et matérielle d'une telle obligation, qui sont conformes aux exigences posées par la directive 2000/31.

27. Par sa première question, la juridiction de renvoi demande également à la Cour de préciser si un hébergeur peut être contraint de retirer, au niveau mondial, des informations diffusées au moyen d'une plateforme de réseau social.

28. Afin de répondre à ces deux questions, j'examinerai en premier lieu, d'une part, le régime de la directive 2000/31 applicable à Facebook Ireland en tant qu'hébergeur et, d'autre part, les implications de sa qualification d'hébergeur en ce qui concerne les injonctions adressées à ce prestataire. En deuxième lieu, je procéderai à l'analyse des exigences posées par le droit de l'Union quant aux portées matérielle et personnelle d'une obligation en matière de surveillance pouvant être imposée à un hébergeur dans le cadre d'une injonction, sans que cela conduise à l'imposition d'une obligation générale en cette matière. Enfin, en troisième lieu, j'aborderai la question de la portée territoriale d'une obligation de retrait.

1. Les injonctions adressées aux hébergeurs au regard de la directive 2000/31

29. Il convient de rappeler que, pour que le stockage effectué par le prestataire d'un service de la société de l'information relève de l'article 14 de la directive 2000/31, le comportement de ce prestataire doit se limiter à celui d'un « prestataire intermédiaire » au sens voulu par le législateur dans le cadre de la section 4 de cette directive. En outre, selon le considérant 42 de ladite directive, son comportement est purement technique, automatique et passif, ce qui implique l'absence de connaissance ou de contrôle des données qu'il stocke et que le rôle qu'il exerce doit donc être neutre [3].

3 Voir, notamment, arrêt du 23 mars 2010, Google France et Google (C-236/08 à C-238/08, EU:C:2010:159, points 112 et 113).

30. La Cour a déjà eu l'occasion de clarifier qu'un exploitant d'une plateforme de réseau social qui stocke sur ses serveurs des informations fournies par les utilisateurs de cette plateforme, relatives à leur profil, est un prestataire de services d'hébergement au sens de l'article 14 de la directive 2000/31 [4]. Indépendamment des doutes que l'on pourrait avoir à cet égard, il ressort de la demande de renvoi préjudiciel que, pour la juridiction de renvoi, il est constant que Facebook Ireland est un hébergeur dont le comportement se limite à celui d'un prestataire intermédiaire.

31. Sous l'empire de la directive 2000/31, un hébergeur dont le comportement se limite à celui d'un prestataire intermédiaire bénéfice d'une immunité relative en matière de responsabilité pour les informations qu'il stocke. En effet, cette immunité est accordée uniquement si un tel hébergeur n'avait pas connaissance du caractère illégal des informations stockées ou de l'activité menée au moyen de ces informations et à condition que, une fois averti de cette illégalité, il agisse promptement pour retirer les informations en cause ou rendre l'accès à celles-ci impossible. En revanche, si cet hébergeur ne remplit pas ces conditions, c'est-à-dire s'il avait connaissance de l'illégalité des informations stockées mais n'a pas agi afin de les retirer ou d'en rendre l'accès impossible, la directive 2000/31 ne s'oppose pas à ce qu'il puisse être tenu indirectement responsable de ces informations [5].

32. Par ailleurs, il ressort de l'article 14, paragraphe 3, de la directive 2000/31 que l'immunité accordée à un prestataire intermédiaire ne fait pas obstacle à ce qu'une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, exige de ce prestataire qu'il mette un terme à une violation ou prévienne une violation. Il découle de cette disposition qu'un prestataire intermédiaire peut être le destinataire d'injonctions, même si, selon les conditions énoncées à l'article 14, paragraphe 1, de cette directive, ce prestataire n'est pas lui-même responsable des informations stockées sur ses serveurs [6].

33. Les conditions et les modalités de telles injonctions visant des prestataires intermédiaires relèvent du droit national [7]. Les règles instaurées par les États membres doivent toutefois respecter les exigences posées par le droit de l'Union, notamment par la directive 2000/31.

34. Tout cela reflète la volonté du législateur de l'Union de mettre en balance, à travers cette directive, les différents intérêts des hébergeurs dont le comportement se limite à celui d'un prestataire intermédiaire, des utilisateurs de leurs services ainsi que des personnes lésées par toute violation commise au cours de l'utilisation de ces services. En conséquence, il incombe aux États membres, lors de la mise en œuvre des mesures de transposition de la directive 2000/31, non seulement de respecter les exigences posées par cette directive, mais également de veiller à ne pas se fonder sur une interprétation qui entrerait en conflit avec les droits fondamentaux en présence ou avec les autres principes généraux du droit de l'Union, tels que le principe de proportionnalité [8].

4 Voir arrêt du 16 février 2012, SABAM (C-360/10, EU:C:2012:85, point 27).

5 Voir article 14 de la directive 2000/31. Voir, également, mes conclusions dans l'affaire Stichting Brein (C 610/15, EU:C:2017:99, points 67 et 68).

6 Voir arrêt du 7 août 2018, SNB-REACT (C-521/17, EU:C:2018:639, point 51). Voir, également, en ce sens, 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° 2, p. 5.

7 Voir mes conclusions dans l'affaire Mc Fadden (C-484/14, EU:C:2016:170). Voir, également, Husovec, M., *Injunctions Against Intermediaires in the European Union. Accountable But Not Liable ?*, Cambridge University Press, Cambridge, 2017, p. 57 et 58.

8 Voir, en ce sens, en ce qui concerne le respect des droits fondamentaux et du principe de proportionnalité, arrêt du 29 janvier 2008, Promusicae (C-275/06, EU:C:2008:54, point 68).

2. Les exigences posées quant aux portées personnelle et matérielle d'une obligation en matière de surveillance

a) L'interdiction d'une obligation générale en matière de surveillance

35. Il convient d'observer que l'article 15, paragraphe 1, de la directive 2000/31 interdit aux États membres d'imposer, notamment aux prestataires de services dont l'activité consiste à stocker des informations, une obligation générale de surveiller les informations qu'ils stockent ou une obligation générale de rechercher activement les faits ou les circonstances révélant des activités illicites. Par ailleurs, il ressort de la jurisprudence que cette disposition s'oppose, notamment, à ce qu'un hébergeur dont le comportement se limite à celui d'un prestataire intermédiaire soit contraint de procéder à une surveillance de la totalité [9] ou de la quasi-totalité [10] des données de tous les utilisateurs de son service afin de prévenir toute atteinte future.

36. Si, contrairement à ce que prévoit cette disposition, un État membre pouvait imposer, dans le cadre d'une injonction, une obligation générale en matière de surveillance à un hébergeur, il n'est pas exclu que celui-ci risquerait de perdre la qualité de prestataire intermédiaire ainsi que l'immunité qui l'accompagne. En effet, le rôle d'un hébergeur exerçant une surveillance générale ne serait plus neutre. L'activité de cet hébergeur ne conserverait pas son caractère technique, automatique et passif, ce qui impliquerait que ledit hébergeur aurait connaissance des informations stockées et exercerait un contrôle sur celles-ci.

37. En outre, même si un tel risque n'existait pas, un hébergeur exerçant une surveillance générale pourrait, par principe, être tenu pour responsable de toute activité ou information illicite, sans que les conditions énoncées à l'article 14, paragraphe 1, sous a) et b), de cette directive soient effectivement remplies.

38. Certes, l'article 14, paragraphe 1, sous a), de la directive 2000/31 subordonne la responsabilité d'un prestataire intermédiaire à la prise effective de connaissance de l'activité ou de l'information illicite. Toutefois, compte tenu d'une obligation générale en matière de surveillance, le caractère illicite de toute activité ou information pourrait être considéré comme étant d'office porté à la connaissance de ce prestataire intermédiaire et celui-ci devrait procéder au retrait de ces informations ou en rendre l'accès impossible, sans qu'il ait saisi le contenu illicite [11]. En conséquence, la logique de l'immunité relative en matière de responsabilité pour les informations stockées par un prestataire intermédiaire serait systématiquement renversée, ce qui porterait atteinte à l'effet utile de l'article 14, paragraphe 1, de la directive 2000/31.

39. Pour résumer, le rôle d'un hébergeur exerçant une telle surveillance générale ne serait plus neutre, dans la mesure où l'activité de cet hébergeur ne conserverait pas son caractère technique, automatique et passif, ce qui impliquerait que ledit hébergeur aurait connaissance des informations stockées et exercerait un contrôle sur celles-ci. En conséquence, la mise en œuvre d'une obligation générale en matière de surveillance, imposée à un hébergeur dans le cadre d'une injonction autorisée, a priori, en vertu de l'article 14, paragraphe 3, de la directive 2000/31, pourrait rendre l'article 14 de cette directive inapplicable à l'égard de cet hébergeur.

9 Voir arrêts du 12 juillet 2011, L'Oréal e.a. (C-324/09, EU:C:2011:474, points 139 et 144), ainsi que du 24 novembre 2011, Scarlet Extended (C-70/10, EU:C:2011:771, points 36 et 40).

10 Voir arrêt du 16 février 2012, SABAM (C-360/10, EU:C:2012:85, points 37 et 38).

11 Voir, en ce sens, conclusions de l'avocat général Jääskinen dans l'affaire L'Oréal e.a. (C-324/09, EU:C:2010:757, point 143).

40. Je déduis ainsi de la lecture combinée de l'article 14, paragraphe 3, et de l'article 15, paragraphe 1, de la directive 2000/31 qu'une obligation imposée à un prestataire intermédiaire dans le cadre d'une injonction ne saurait conduire à ce que, par rapport à la totalité ou à la quasi-totalité des informations stockées, le rôle de ce prestataire intermédiaire ne soit plus neutre dans le sens décrit au point précédent.

b) L'obligation de surveillance applicable à un cas spécifique

41. Ainsi que l'énonce le considérant 47 de la directive 2000/31, l'interdiction d'imposer des obligations générales, prévue à l'article 15, paragraphe 1, de cette directive, ne concerne pas les obligations de surveillance applicables *à un cas spécifique*. En effet, il ressort du libellé de l'article 14, paragraphe 3, de la directive 2000/31 qu'un hébergeur peut être contraint *de prévenir* une violation, ce qui implique logiquement, ainsi que le fait valoir la Commission, une certaine forme de surveillance dans le futur, sans que cette surveillance se transforme en obligation de surveillance générale [12]. L'article 18 de cette directive exige en outre des États membres qu'ils veillent à ce que les recours juridictionnels disponibles dans leur droit national portant sur les activités des services de la société de l'information permettent l'adoption rapide de mesures visant, notamment, *à prévenir toute nouvelle atteinte* aux intérêts concernés.

42. Par ailleurs, il ressort de l'arrêt L'Oréal e.a. [13] qu'un hébergeur peut être contraint de prendre des mesures qui contribuent à éviter que de *nouvelles atteintes* de même nature par le même destinataire aient lieu.

43. Dans cet arrêt, la Cour a interprété non pas exclusivement les dispositions de la directive 2000/31, mais également celles de la directive 2004/48/CE [14]. Or, ce faisant, la Cour a défini une obligation en matière de surveillance conforme aux exigences posées par ces directives par opposition à l'obligation interdite à l'article 15, paragraphe 1, de la directive 2000/31, à savoir celle *de surveillance active de la totalité – quasi-totalité* des données afin de prévenir toute atteinte future [15]. Indépendamment du contexte spécifique de l'arrêt L'Oréal e.a. [16] et des références à la directive 2004/48, les considérations de cet arrêt relatives aux obligations des hébergeurs conformes au droit de l'Union, en fonction de leur caractère général ou non, sont de nature transversale et, partant, sont, selon moi, transposables au cas d'espèce.

44. Par conséquent, afin de prévenir toute atteinte future, un hébergeur peut être contraint, dans le cadre d'une injonction, de retirer des informations illicites n'ayant pas encore été diffusées au moment de l'adoption de cette injonction, sans que la diffusion de ces informations soit portée, de nouveau et de manière séparée par rapport à la demande initiale de retrait, à sa connaissance.

45. Toutefois, afin de ne pas aboutir à l'imposition d'une obligation générale, une obligation de surveillance doit, ainsi qu'il semble découler de l'arrêt L'Oréal e.a. [17], répondre à des exigences additionnelles, à savoir porter sur des atteintes de *même nature* du *même destinataire aux mêmes droits*, en l'espèce, celui des marques.

46. Ainsi, j'en déduis que la surveillance active n'est pas inconciliable avec la directive 2000/31, contrairement à la surveillance active dont l'objet n'est pas ciblé sur le cas spécifique d'une atteinte.

12 Voir, également, en ce sens, Rosati, E., *Copyright and the Court of Justice of the European Union*, Oxford University Press, Oxford, 2019, p. 158.

13 Arrêt du 12 juillet 2011 (C-324/09, EU:C:2011:474, point 144).

14 Directive du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle (JO 2004, L 157, p. 45).

15 Arrêt du 12 juillet 2011, L'Oréal e.a. (C-324/09, EU:C:2011:474, points 139 et 144).

16 Arrêt du 12 juillet 2011 (C-324/09, EU:C:2011:474).

17 Arrêt du 12 juillet 2011, L'Oréal e.a. (C-324/09, EU:C:2011:474, points 141 et 144).

47. Dans cet ordre d'idées, j'ai indiqué dans mes conclusions dans l'affaire Mc Fadden [18], relative à un fournisseur d'accès à un réseau de communication au sens de l'article 12 de la directive 2000/31, m'inspirant des travaux préparatoires de la directive 2000/31, que pour qu'une obligation puisse être considérée comme applicable *à un cas spécifique* il convient notamment qu'elle soit limitée au regard de *l'objet* et de *la durée* de surveillance.

48. Ces exigences générales formulées de manière abstraite me semblent transposables à des circonstances telles que celles de l'affaire au principal, malgré le fait que, lors de l'application, par analogie aux hébergeurs tels que Facebook Ireland, des considérations en matière d'obligation de surveillance relatives aux fournisseurs d'accès à un réseau de communication tel qu'Internet, les rôles exercés par ces prestataires intermédiaires sont différents. Par exemple, si l'on considère un hébergeur tel que Facebook Ireland, les contenus de sa plateforme semblent constituer la totalité des données stockées, tandis que, pour un fournisseur d'accès à Internet, ces contenus ne représentent qu'une infime partie seulement des données transmises. En contrepartie, le caractère et l'intensité de l'implication d'un tel hébergeur dans le traitement des contenus numériques diffèrent sensiblement de ceux d'un fournisseur d'accès à Internet. Ainsi que l'observe la Commission, un hébergeur est mieux placé pour prendre des mesures afin de rechercher et d'éliminer des informations illicites qu'un fournisseur d'accès.

49. Par ailleurs, l'exigence relative à la limitation temporelle d'une obligation en matière de surveillance fait écho à plusieurs arrêts de la Cour [19]. Même s'il ressort de la jurisprudence que la limitation temporelle d'une obligation posée dans le cadre d'une injonction se rapporte plutôt à la problématique des principes généraux du droit de l'Union [20], j'estime qu'une obligation de surveillance permanente serait difficilement conciliable avec le concept d'une obligation applicable à un cas spécifique au sens du considérant 47 de la directive 2000/31.

50. Dès lors, le caractère ciblé d'une obligation en matière de surveillance devrait être envisagé en prenant en considération la durée de cette surveillance ainsi que les précisions relatives à la nature des atteintes visées, à leur auteur et à leur objet. Tous ces éléments sont interdépendants et liés les uns aux autres. Il convient ainsi de les évaluer de manière globale afin de répondre à la question de savoir si une injonction respecte ou non l'interdiction prévue à l'article 15, paragraphe 1, de la directive 2000/31.

c) Conclusions intermédiaires

51. Pour récapituler cette partie de mon analyse, en premier lieu, il ressort de la lecture combinée de l'article 14, paragraphe 3, et de l'article 15, paragraphe 1, de la directive 2000/31 qu'une obligation imposée à un prestataire intermédiaire dans le cadre d'une injonction ne saurait conduire à la situation où, par rapport à la totalité ou à la quasi-totalité des informations stockées, le rôle de ce prestataire intermédiaire ne serait pas plus technique, automatique et passif, ce qui impliquerait que l'hébergeur concerné aurait connaissance de ces informations et exercerait un contrôle sur celles-ci [21].

18 C-484/14, EU:C:2016:170, point 132.

19 Plus précisément, la Cour a indiqué, dans l'arrêt du 12 juillet 2011, L'Oréal e.a. (C-324/09, EU:C:2011:474, point 140), que l'injonction visant à prévenir d'éventuelles atteintes portées à des marques dans le cadre du service de la société de l'information, à savoir une place de marché en ligne, ne saurait avoir pour objet ou pour effet d'instaurer une interdiction générale et *permanente* de mise en vente de produits de ces marques. Dans la même veine, la Cour a constaté, dans l'arrêt du 16 février 2012, SABAM (C-360/10, EU:C:2012:85, point 45), que le droit de l'Union s'oppose notamment à ce qu'une obligation de surveillance, posée dans le cadre d'une injonction adressée à un prestataire, soit *illimitée dans le temps*.

20 Cette approche a été celle retenue par l'avocat général Jääskinen dans ses conclusions dans l'affaire L'Oréal e.a. (C-324/09, EU:C:2010:757, point 181), celles-ci ayant, à mon sens, fortement inspiré la formulation des passages en cause de l'arrêt rendu par la Cour dans cette affaire.

21 Voir point 39 des présentes conclusions.

52. En second lieu, la surveillance active n'est pas inconciliable avec la directive 2000/31, contrairement à la surveillance active dont l'objet n'est pas ciblé sur le cas spécifique d'une atteinte [22].

53. En troisième lieu, le caractère ciblé d'une obligation en matière de surveillance devrait être envisagé en prenant en considération la durée de cette surveillance ainsi que les précisions relatives à la nature des atteintes visées, à leur auteur et à leur objet [23].

54. C'est à la lumière de ces considérations qu'il convient d'aborder les portées personnelle et matérielle d'une obligation en matière de surveillance d'un prestataire exploitant une plateforme de réseau social. Celles-ci se résument, en l'espèce, à la recherche et à l'identification, parmi des contenus stockés, d'informations identiques à celle ayant été qualifiée d'illicite par la juridiction saisie ainsi qu'à la recherche d'informations équivalant à celle-ci.

d) Application en l'espèce

1) Les informations identiques à celle ayant été qualifiée d'illicite

55. Exception faite de Facebook Ireland, tous les intéressés soutiennent qu'il doit être possible d'ordonner à un hébergeur de supprimer ou de bloquer l'accès aux déclarations identiques à celle ayant été qualifiée d'illicite publiées par le même utilisateur. La requérante, les gouvernements autrichien et letton, ainsi que la Commission sont, en substance, d'avis qu'il en va de même en ce qui concerne celles publiées par d'autres utilisateurs.

56. Il ressort du renvoi préjudiciel que le tribunal de deuxième instance a considéré que la référence aux « informations identiques » visait les publications de photos de la requérante *accompagnées du même texte*. Dans cet ordre d'idées, la juridiction de renvoi explique que ses doutes portent notamment sur le point de savoir si l'injonction délivrée à l'encontre de Facebook Ireland peut être étendue aux *déclarations (messages d'accompagnement) textuellement identiques* et à celles de contenu équivalent. Je comprends ainsi cette référence aux « informations identiques » en ce sens que la juridiction de renvoi vise les reproductions manuelles et exactes de l'information qu'elle a qualifiée d'illicite et, ainsi que l'indique le gouvernement autrichien, les reproductions automatisées, effectuées grâce à la fonction de « partage ».

57. À cet égard, je suis d'avis qu'un hébergeur qui exploite une plateforme de réseau social peut être contraint, pour mettre en œuvre une injonction rendue par une juridiction d'un État membre, de rechercher et d'identifier toutes les informations identiques à celle ayant été qualifiée d'illicite par cette juridiction.

58. En effet, ainsi qu'il ressort de mon analyse, un hébergeur peut être contraint de prévenir toute nouvelle atteinte du même type et du même destinataire d'un service de la société de l'information [24]. Dans un tel cas, il s'agit bien d'un cas spécifique d'une atteinte concrètement identifiée, de sorte que l'obligation d'identifier, parmi celles provenant d'un seul utilisateur, les informations identiques à celle qualifiée d'illicite ne constitue pas une obligation générale en matière de surveillance.

59. À mon avis, il en va de même en ce qui concerne les informations identiques à celle ayant été qualifiée d'illicite diffusées par d'autres utilisateurs. Je suis conscient du fait que ce raisonnement conduit à ce que la portée personnelle d'une obligation en matière de surveillance englobe tout utilisateur et, partant, l'intégralité des informations diffusées au moyen d'une plateforme.

22 Voir point 46 des présentes conclusions.

23 Voir point 50 des présentes conclusions.

24 Voir points 42 et 45 des présentes conclusions.

60. Néanmoins, une obligation de rechercher et d'identifier des informations identiques à celle ayant été qualifiée d'illicite par la juridiction saisie est toujours ciblée sur le cas spécifique d'une atteinte. En outre, il s'agit en l'espèce d'une obligation imposée dans le cadre d'une ordonnance de référé, qui produit ses effets jusqu'à la clôture définitive de la procédure. Ainsi, une telle obligation imposée à un hébergeur est, par la nature des choses, limitée dans le temps.

61. Par ailleurs, la reproduction du même contenu par tout utilisateur d'une plateforme de réseau social me semble, en règle générale, détectable à l'aide d'outils informatiques, et ce sans que l'hébergeur soit obligé d'avoir recours à un filtrage actif et non automatique de l'intégralité des informations diffusées au moyen de sa plateforme.

62. En outre, imposer l'obligation de rechercher et d'identifier toutes les informations identiques à celle ayant été qualifiée d'illicite permet d'assurer un juste équilibre entre les droits fondamentaux en présence.

63. Tout d'abord, la recherche et l'identification des informations identiques à celle ayant été qualifiée d'illicite par une juridiction saisie ne requièrent pas des moyens techniques sophistiqués, susceptibles de représenter une charge extraordinaire. Dès lors, une telle obligation n'apparaît pas comme portant une atteinte excessive au droit à la liberté d'entreprise dont bénéfice un hébergeur qui exploite une plateforme de réseau social tel que Facebook Ireland en vertu de l'article 16 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

64. Ensuite, compte tenu de la facilité de reproduction des informations dans l'environnement d'Internet, la recherche et l'identification des informations identiques à celle ayant été qualifiée d'illicite s'avère nécessaire pour assurer la protection efficace de la vie privée et des droits de la personnalité.

65. Enfin, une telle obligation respecte le droit fondamental des utilisateurs d'Internet à la liberté d'expression et d'information, garanti à l'article 11 de la Charte, dans la mesure où la protection de cette liberté doit non pas nécessairement être assurée de manière absolue mais être mise en balance avec la protection d'autres droits fondamentaux. S'agissant des informations identiques à celle ayant été qualifiée d'illicite, elles constituent, a priori et en règle générale, des répétitions d'une atteinte concrètement qualifiée d'illicite. Ces répétitions devraient faire l'objet d'une qualification identique, celle-ci étant toutefois susceptible d'être nuancée en fonction, notamment, du contexte d'une déclaration prétendument illicite. Au passage, il convient de relever que les tiers pouvant être indirectement affectés par des injonctions ne font pas partie des procédures dans le cadre desquelles ces injonctions sont rendues. C'est notamment pour cette raison qu'il convient d'assurer la possibilité pour ces tiers de contester, devant un juge, les mesures d'exécution adoptées par un hébergeur sur la base d'une injonction [25], cette possibilité ne devant pas être conditionnée par le fait d'être qualifié de partie à une procédure principale [26].

25 Voir, par analogie, arrêt du 27 mars 2014, UPC Telekabel Wien (C-314/12, EU:C:2014:192, point 57).

26 Voir, par analogie, arrêts du 25 mai 2016, Meroni (C-559/14, EU:C:2016:349, points 49 et 50), et du 21 décembre 2016, Biuro podróży « Partner » (C-119/15, EU:C:2016:987, point 40). Sur la problématique du principe de protection juridictionnelle effective à l'égard des tiers, voir, également, 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, p. 222 et 223.

2) Les informations équivalentes

66. S'agissant de la portée matérielle d'une obligation en matière de surveillance, la requérante soutient qu'un hébergeur peut être soumis à l'obligation de retirer les déclarations de contenu équivalant à celle qualifiée d'illicite publiées par le même utilisateur. En revanche, le gouvernement autrichien et la Commission considèrent que la possibilité d'imposer une telle obligation dépend du résultat de la mise en balance des intérêts en cause. Seule la requérante estime qu'il est possible d'enjoindre à un hébergeur de retirer des déclarations de contenu équivalant à celle ayant été qualifiée d'illicite publiées par d'autres utilisateurs.

67. La référence aux « informations équivalentes » ou à celles « dont le contenu est équivalent » donne lieu à des difficultés d'interprétation dans la mesure où la juridiction de renvoi ne précise pas le sens de ces expressions. On peut cependant déduire du renvoi préjudiciel que la référence aux informations « dont le contenu est équivalent » vise les informations qui *divergent à peine* de l'information initiale ou les situations dans lesquelles *le message reste, en substance, inchangé*. Je comprends ces indications en ce sens qu'une reproduction de l'information ayant été qualifiée d'illicite comportant une erreur de frappe ainsi que celle ayant une syntaxe ou ponctuation nuancée, constitue une « information équivalente ». Il n'est toutefois pas évident que l'équivalence visée par la deuxième question n'aille pas au-delà de tels cas.

68. Certes, il ressort de l'arrêt L'Oréal e.a.[27] que le prestataire d'un service de la société de l'information peut être contraint de prendre des mesures qui contribuent à prévenir de *nouvelles atteintes* de *même nature* aux mêmes droits.

69. Il convient toutefois de ne pas perdre de vue le contexte factuel dans lequel la jurisprudence pertinente a été développée, à savoir celui des violations du droit de propriété intellectuelle. En règle générale, de telles violations consistent en la diffusion du même contenu que celui protégé ou, à tout le moins, d'un contenu ressemblant à celui protégé, les éventuelles modifications de celui-ci, parfois difficiles à apporter, nécessitent une intervention spécifique.

70. En revanche, il est inhabituel qu'un acte diffamatoire reprenne les termes exacts d'un acte de même nature. Cela découle, en partie, du caractère personnalisé de la façon d'exprimer des idées. En outre, contrairement aux violations du droit de propriété intellectuelle, les actes diffamatoires ultérieurs à l'acte diffamatoire initial reproduisent plutôt le fait de tenir des propos portant atteinte à l'honneur d'une personne que la forme de l'acte initial. Pour cette raison, en matière de diffamation, la simple référence à des actes de même nature ne pourrait pas jouer le même rôle qu'en matière de violations du droit de propriété intellectuelle.

71. En tout état de cause, l'interprétation donnée à la référence aux « informations équivalentes » est susceptible d'affecter la portée d'une obligation en matière de surveillance et l'exercice des droits fondamentaux en présence. Une juridiction statuant, dans le cadre d'une injonction, sur le retrait des « informations équivalentes » doit ainsi respecter le principe de sécurité juridique et garantir que les effets de cette injonction sont clairs, précis et prévisibles. Ce faisant, cette juridiction doit mettre en balance les droits fondamentaux en présence et tenir compte du principe de proportionnalité.

72. Sans préjudice de ces considérations, m'inspirant à nouveau de l'arrêt L'Oréal e.a.[28], je suis d'avis que, a fortiori, un hébergeur peut être contraint d'identifier des informations équivalant à celle qualifiée d'illicite provenant du même utilisateur. En passant, dans ce cas également, il conviendrait d'assurer à cet utilisateur la possibilité de contester, devant un juge, les mesures d'exécution adoptées par un hébergeur au cours de la mise en œuvre d'une injonction.

27 Arrêt du 12 juillet 2011 (C-324/09, EU:C:2011:474).

28 Arrêt du 12 juillet 2011 (C-324/09, EU:C:2011:474).

73. En revanche, l'identification d'informations équivalant à celle qualifiée d'illicite provenant d'autres utilisateurs nécessiterait la surveillance de la totalité des informations diffusées au moyen d'une plateforme de réseau social. Or, à la différence des informations identiques à celle ayant été qualifiée d'illicite, les informations équivalant à celle-ci ne peuvent pas être identifiées sans qu'un hébergeur recoure à des solutions sophistiquées. En conséquence, non seulement le rôle d'un prestataire exerçant une surveillance générale ne serait plus neutre, en ce sens qu'il ne serait pas seulement technique, automatique et passif mais ce prestataire, en exerçant une forme de censure, deviendrait un contributeur actif de cette plateforme.

74. Par ailleurs, une obligation d'identification d'informations équivalant à celle qualifiée d'illicite provenant de tout utilisateur n'assurerait pas un juste équilibre entre la protection de la vie privée et des droits de la personnalité, celle de la liberté d'entreprise, ainsi que celle de la liberté d'expression et d'information. D'une part, la recherche et l'identification de telles informations nécessiteraient des solutions coûteuses, qui devraient être développées et introduites par un hébergeur. D'autre part, la mise en œuvre de ces solutions conduirait à une censure, de sorte que la liberté d'expression et d'information serait susceptible d'être systématiquement restreinte.

75. À la lumière des considérations qui précèdent, je propose de répondre aux première et deuxième questions, dans la mesure où elles portent sur les portées personnelle et matérielle d'une obligation de surveillance, que l'article 15, paragraphe 1, de la directive 2000/31 doit être interprété en ce sens qu'il ne s'oppose pas à ce qu'un hébergeur qui exploite une plateforme de réseau social soit contraint, dans le cadre d'une injonction, de rechercher et d'identifier, parmi toutes les informations diffusées par les utilisateurs de cette plateforme, les informations identiques à celle ayant été qualifiée d'illicite par une juridiction ayant rendu cette injonction. Dans le cadre d'une telle injonction, un hébergeur peut être contraint de rechercher et d'identifier les informations équivalant à celle qualifiée d'illicite uniquement parmi des informations diffusées par l'utilisateur ayant diffusé cette information. Une juridiction statuant sur le retrait de telles informations équivalentes doit garantir que les effets de son injonction sont clairs, précis et prévisibles. Ce faisant, elle doit mettre en balance les droits fondamentaux en présence et tenir compte du principe de proportionnalité.

3. Sur le retrait au niveau mondial

a) Observations liminaires

76. Je vais à présent me pencher sur les doutes de la juridiction de renvoi quant à la portée territoriale d'une obligation de retrait. Ceux-ci concernent, en substance, la question de savoir si un hébergeur peut être contraint de retirer des contenus qui ont été qualifiés d'illicites en vertu du droit national d'un État membre, non seulement au niveau de cet État membre, mais également au niveau mondial.

77. À titre liminaire, il est vrai que Facebook Ireland exploite, en tant que filiale de Facebook, une plateforme électronique uniquement pour les utilisateurs situés hors des États-Unis et du Canada. Toutefois, cette circonstance ne semble pas être de nature à exclure le retrait au niveau mondial des informations diffusées au moyen de cette plateforme. En effet, Facebook Ireland ne conteste pas le fait d'être en mesure d'assurer un tel retrait au niveau mondial.

78. Il convient toutefois d'observer que le législateur de l'Union n'a pas harmonisé les règles matérielles en matière d'atteinte à la vie privée et aux droits de la personnalité, y compris la diffamation [29]. En outre, en l'absence de consensus au niveau de l'Union [30], le législateur de l'Union n'a pas non plus harmonisé les règles de conflit en la matière [31]. Ainsi, pour connaître des actions en diffamation, chaque juridiction de l'Union a recours à la loi désignée comme applicable en vertu des règles nationales de conflit.

79. La situation en cause au principal est, a priori, différente de celle qui constituait le point de départ de mon analyse relative à la portée territoriale d'un déréférencement des résultats d'un moteur de recherche dans l'affaire Google (Portée territoriale du déréférencement) [32], évoquée par Facebook Ireland et le gouvernement letton. Cette affaire concerne la directive 95/46/CE [33], qui harmonise, au niveau de l'Union, certaines règles matérielles relatives à la protection des données. C'est notamment le fait que les règles en cette matière sont harmonisées qui m'a conduit à conclure qu'un prestataire devait être tenu de supprimer les résultats affichés à la suite d'une recherche effectuée non pas uniquement à partir d'un seul État membre mais à partir d'un lieu situé dans l'Union [34]. Toutefois, dans mes conclusions présentées dans cette affaire, je n'excluais pas qu'il puisse y avoir des situations dans lesquelles l'intérêt de l'Union exige une application des dispositions de cette directive au-delà du territoire de l'Union [35].

80. En conséquence, en ce qui concerne les atteintes diffamatoires, l'imposition dans un État membre d'une obligation consistant à retirer certaines informations au niveau mondial, pour tous les utilisateurs d'une plateforme électronique, en raison de l'illicéité de ces informations établie au titre d'une loi applicable, conduirait à ce que la constatation de leur caractère illicite produise des effets dans d'autres États. En d'autres termes, la constatation du caractère illicite des informations en cause s'étendrait aux territoires de ces autres États. Toutefois, il n'est pas exclu que, selon les lois désignées comme applicables en vertu des règles nationales de conflit de ces États, cette information pourrait être considérée comme licite.

81. Ainsi que l'illustre le débat entre les intéressés, d'une part, la réticence à accorder de tels effets extraterritoriaux à des injonctions fait écho à la position de Facebook Ireland ainsi qu'à celle des gouvernements letton, portugais et finlandais. D'autre part, à l'exception du gouvernement portugais, ces intéressés semblent également nourrir des doutes sur l'étendue territoriale de la compétence des juridictions d'un État membre. En substance, lesdits intéressés semblent considérer que la juridiction d'un État membre ne peut pas statuer, dans le cadre d'une injonction adressée à un hébergeur, sur le retrait de contenus en dehors du territoire de cet État membre. Il convient dès lors d'analyser ces deux questions, à savoir la portée territoriale d'une obligation de retrait et l'étendue de la compétence des juridictions d'un État membre, en abordant tout d'abord celle de la compétence, qui est, en règle générale, préalable à celle du fond.

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

30 Voir Van Calster, G., *European Private International Law*, Hart Publishing, Oxford, Portland, 2016, p. 248 à 251.

31 Voir article 1er, paragraphe 2, du règlement (CE) nº 864/2007 du Parlement européen et du Conseil, du 11 juillet 2007, sur la loi applicable aux obligations non contractuelles (« Rome II ») (JO 2007, L 199, p. 40).

32 Je me réfère ici à mes conclusions dans l'affaire Google (Portée territoriale du déréférencement) (C-507/17, EU:C:2019:15).

33 Directive du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31).

34 Voir mes conclusions dans l'affaire Google (Portée territoriale du déréférencement) (C-507/17, EU:C:2019:15, points 47, 55, 76 et 77).

35 Voir mes conclusions dans l'affaire Google (Portée territoriale du déréférencement) (C-507/17, EU:C:2019:15, point 62).

b) Sur l'étendue territoriale de la compétence

82. La directive 2000/31 ne réglemente pas la compétence pour statuer sur des injonctions. En revanche, ainsi qu'il ressort de l'arrêt eDate Advertising e.a.[36], en cas d'atteinte alléguée aux droits de la personnalité au moyen de contenus mis en ligne sur un site Internet, une personne qui s'estime lésée a la faculté de saisir les juridictions des États membres compétentes en vertu du règlement (UE) nº 1215/2012[37]. En effet, tandis que les règles de conflit en matière de diffamation ne sont pas harmonisées au niveau de l'Union, il en est autrement en ce qui concerne les règles de compétence.

83. À cet égard, il convient d'ajouter que les règles de compétence du règlement nº 1215/2012 s'appliquent également aux litiges en matière de suppression des contenus diffamatoires mis en ligne[38]. En outre, il importe peu que, en l'espèce, une telle demande soit dirigée non pas contre un émetteur mais contre un hébergeur des contenus mis en ligne. Cela étant posé, je ne proposerai pas à la Cour de reformuler les questions préjudicielles, dans la mesure où seuls les intéressés nourrissent des doutes sur l'étendue territoriale de la compétence. Je souhaiterais néanmoins formuler quelques remarques à ce sujet.

84. Selon l'arrêt eDate Advertising e.a.[39], une personne qui s'estime lésée peut saisir, notamment, les juridictions de l'État membre dans lequel se trouve le centre de ses intérêts. Ces juridictions sont compétentes pour statuer sur l'intégralité du dommage causé. Il semble que, en l'espèce, la juridiction saisie par la requérante soit celle du lieu du centre de ses intérêts[40].

85. Il est vrai que, dans l'arrêt eDate Advertising e.a.[41], la Cour a indiqué qu'une personne s'estimant lésée pouvait saisir, en fonction du lieu de la matérialisation du dommage causé dans l'Union, un for au titre de l'intégralité de ce dommage. Certes, cela peut faire penser que l'étendue territoriale de la compétence de ce for n'engloberait pas les faits se rapportant aux territoires des États tiers. Toutefois, cette considération fait plutôt écho au fait qu'un for, pour être compétent en vertu du règlement nº 1215/2012, au titre du lieu de la matérialisation du dommage, doit être une juridiction d'un État membre. Par ailleurs, exception faite de cette considération, la Cour a indiqué à maintes reprises dans cet arrêt que ce for était compétent pour statuer sur l'intégralité des dommages résultant de la diffamation[42].

36 Arrêt du 25 octobre 2011 (C-509/09 et C-161/10, EU:C:2011:685, points 43 et 44).

37 Règlement du Parlement et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (JO 2012, L 35, p. 1).

38 Arrêt du 17 octobre 2017, Bolagsupplysningen et Ilsjan (C-194/16, EU:C:2017:766, point 44).

39 Arrêt du 25 octobre 2011 (C-509/09 et C-161/10, EU:C:2011:685, point 48).

40 En conséquence, malgré le fait que la juridiction de renvoi est appelée à statuer sur une ordonnance de référé, il n'y a pas lieu de s'interroger sur les implications de l'article 35 du règlement nº 1215/2012 sur l'étendue territoriale de la compétence et sur la portée territoriale d'une obligation de retrait imposée dans le cadre d'une injonction.

41 Arrêt du 25 octobre 2011 (C-509/09 et C-161/10, EU:C:2011:685, point 48).

42 Arrêt du 25 octobre 2011, eDate Advertising e.a. (C-509/09 et C-161/10, EU:C:2011:685, points 48, 51 et 52). Voir, également, arrêt du 17 octobre 2017, Bolagsupplysningen et Ilsjan (C-194/16, EU:C:2017:766, points 38 et 47). Par ailleurs, selon les interprétations doctrinales de cet arrêt, le for du lieu du centre des intérêts peut statuer dans le monde entier sur des dommages causés. Voir Mankowski, P., dans Magnus, U., et Mankowski, P. (sous la dir. de), Brussels I bis Regulation – Commentary, Otto Schmidt, Cologne, 2016, Art. 7, point 364. Il en va de même en ce qui concerne l'étendue territoriale de la compétence générale du for du défendeur. Dans l'arrêt du 1er mars 2005, Owusu (C-281/02, EU:C:2005:120, point 26), la Cour a considéré que la convention de Bruxelles [convention du 27 septembre 1968 concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale (JO 1972, L 299, p. 32)] peut s'appliquer lorsque le demandeur et le défendeur sont domiciliés dans un État membre, tandis que les faits litigieux sont localisés dans un État tiers. J'en déduis que, dans un tel cas, le for du débiteur est compétent pour statuer sur de tels fait litigieux. Voir, également, Van Calster, G., Luks, C., Extraterritoriality and private international law, Recht in beweging – 19de VRG Alumnidag 2012, MAKLU, Anvers, Apeldoorn, 2012, p. 132.

86. J'en déduis que, contrairement à ce que soutiennent Facebook Ireland ainsi que les gouvernements letton et finlandais, la juridiction d'un État membre peut, en principe, statuer sur le retrait de contenus en dehors du territoire de cet État membre, l'étendue territoriale de sa compétence ayant un caractère universel [43]. Une juridiction d'un État membre peut être empêchée de statuer sur un retrait au niveau mondial en raison non pas d'une question de compétence mais, éventuellement, d'une question de fond.

87. Il convient maintenant d'analyser la question des effets extraterritoriaux des injonctions adressées aux hébergeurs qui, en l'espèce, ainsi que je l'ai indiqué au point 81 des présentes conclusions, se résume à la question de la portée territoriale d'une obligation de retrait.

c) Sur la portée territoriale d'une obligation de retrait

88. Tout d'abord, il convient d'observer que, ainsi que l'admet le gouvernement finlandais, l'article 15, paragraphe 1, de la directive 2000/31 ne réglemente pas les effets territoriaux des injonctions adressées aux prestataires des services de la société de l'information. En outre, sous réserve de satisfaire aux exigences prescrites par la directive 2000/31, les obligations de retrait imposées à ces prestataires dans le cadre des injonctions relèvent du droit national.

89. Ensuite, il est difficile, en l'absence d'une réglementation de l'Union en matière d'atteinte à la vie privée et aux droits de la personnalité, de justifier les effets territoriaux d'une injonction en invoquant la protection des droits fondamentaux garantis aux articles 1er, 7 et 8 de la Charte. En effet, le champ d'application de la Charte suit le champ d'application du droit de l'Union et non l'inverse [44] et, en l'espèce, quant à son fond, le recours de la requérante n'est pas basé sur le droit de l'Union.

90. À cet égard, il convient d'observer que la requérante ne semble pas se prévaloir des droits en matière de protection des données personnelles et qu'elle ne reproche pas à Facebook Ireland d'avoir « procédé » à un traitement illicite de ses données, sa demande étant fondée sur les dispositions générales du droit civil. Par ailleurs, la juridiction de renvoi n'invoque pas des instruments juridiques du droit de l'Union pertinents en cette matière. Elle invoque uniquement la directive 2000/31. Or, il ressort de l'article 1er, paragraphe 5, sous b), de cette directive que celle-ci ne s'applique pas aux questions relatives aux services de la société de l'information, qui sont couvertes par les directives relatives à la protection des données personnelles.

91. Enfin, si l'on peut tirer du règlement nº 1215/2012 des enseignements en ce qui concerne les effets produits par des injonctions dans les États membres, tel n'est pas le cas en ce qui concerne ceux produits en dehors de l'Union. En effet, ce règlement n'exige pas qu'une injonction rendue par la juridiction d'un État membre produise des effets également dans des États tiers. De plus, le fait qu'une juridiction soit compétente pour statuer sur le fond en vertu d'une règle de compétence du droit de l'Union n'implique pas que, ce faisant, elle applique uniquement des règles matérielles qui entrent dans le champ d'application du droit de l'Union et, partant, de la Charte.

43 Il s'agit donc ici d'une compétence dite « globale » ou « générale ». Voir Larsen, T. B., « The extent of jurisdiction under the forum delicti rule in European trademark litigation », *Journal of Private International Law*, 2018, vol. 14, nº 3, p. 550 et 551.

44 Voir arrêt du 26 février 2013, Åkerberg Fransson (C-617/10, EU:C:2013:105, point 19). Voir, également, mes conclusions dans l'affaire Google (Portée territoriale du déréférencement) (C-507/17, EU:C:2019:15, point 55).

92. Pour ces raisons, tant la question des effets extraterritoriaux d'une injonction imposant une obligation de retrait que celle de la portée territoriale d'une telle obligation devraient faire l'objet d'une analyse effectuée à l'aune non pas du droit de l'Union mais, notamment, du droit international public et privé non harmonisé au niveau de l'Union [45]. En effet, rien n'indique que la situation faisant l'objet de l'affaire au principal puisse relever du champ d'application du droit de l'Union et, partant, des règles de droit international ayant une incidence sur l'interprétation du droit de l'Union [46].

93. Par conséquent, s'agissant de la portée territoriale d'une obligation de retrait imposée à un hébergeur dans le cadre d'une injonction, il y a lieu de considérer que celle-ci n'est réglementée ni par l'article 15, paragraphe 1, de la directive 2000/31 ni par aucune autre disposition de cette directive et, partant, que cette disposition ne s'oppose pas à ce qu'un hébergeur soit contraint de retirer des informations diffusées au moyen d'une plateforme de réseau social au niveau mondial. Par ailleurs, ladite portée territoriale n'est pas non plus réglementée par le droit de l'Union dans la mesure où, en l'espèce, le recours de la requérante n'est pas fondé sur celui-ci.

94. Cela étant, tant par souci d'exhaustivité que dans l'hypothèse où la Cour ne suivrait pas ma proposition, je formulerai quelques remarques supplémentaires en ce qui concerne le retrait des informations diffusées au moyen d'une plateforme de réseau social au niveau mondial.

95. En vertu du droit international, il n'est pas exclu qu'une injonction puisse produire des effets dits « extraterritoriaux» [47]. Or, ainsi que je l'ai indiqué au point 80 des présentes conclusions, une telle approche conduirait à ce que la constatation du caractère illicite des informations concernées s'étende aux territoires d'autres États membres, indépendamment du caractère licite ou non de ces informations en vertu de la loi désignée comme applicable selon les règles de conflit de ces États membres.

96. Partant, on pourrait arguer que la Cour a déjà implicitement admis une telle approche dans l'arrêt Bolagsupplysningen et Ilsjan [48]. Il est vrai que, dans cet arrêt, la Cour n'a nullement statué sur la loi applicable à une demande de suppression des contenus mis en ligne. Toutefois, la Cour a jugé que, eu égard à *la nature ubiquitaire des contenus mis en ligne sur un site Internet* et au fait que *la portée de leur diffusion est en principe universelle*, une demande visant notamment à la suppression de tels contenus doit être portée devant une juridiction compétente pour connaître de l'intégralité d'une demande en réparation du dommage. Ce faisant, selon moi, cette juridiction appliquerait la loi ou les lois désignées comme applicables en vertu de ses règles de conflit [49]. Il n'est pas à exclure qu'une juridiction d'un État membre appliquerait, dans ce contexte, une seule loi désignée comme applicable.

97. Toutefois, si une telle juridiction ne pouvait pas statuer sur la suppression des contenus mis en ligne au niveau mondial, se poserait alors la question de savoir quelle juridiction serait mieux placée pour se prononcer sur une telle suppression. En fait, chaque juridiction serait confrontée aux désagréments décrits au point précédent. En outre, devrait-on exiger d'un demandeur, malgré ces difficultés pratiques, qu'il prouve que l'information qualifiée d'illicite selon la loi désignée comme applicable en vertu des règles de conflit de l'État membre saisi est illicite selon toutes les lois potentiellement applicables ?

45 S'agissant des effets extraterritoriaux des décisions judiciaires, il est parfois difficile de tracer une limite entre le droit international public et privé. Voir Maier, H. G., « Extraterritorial Jurisdiction at a Crossroads : An Intersection between Public and Private International Law », *The American Journal of International Law*, vol. 76, nº 2, p. 280, et Svantesson, D. J. B., *Solving the Internet Jurisdiction Puzzle*, Oxford University Press, Oxford, 2017, p. 40.

46 Voir, en ce sens, ordonnance du 12 juillet 2012, Currà e.a. (C-466/11, EU:C:2012:465, point 19).

47 Voir 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 Arrêt du 17 octobre 2017 (C-194/16, EU:C:2017:766, point 44).

49 Voir, également, en ce qui concerne les implications de cet arrêt, 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, nº 9, p. 1030, et 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, nº 2, p. 122, point 59.

98. Même si l'on admettait que les considérations relatives au caractère territorial de la protection découlant des règles matérielles en matière d'atteinte à la vie privée et aux droits de la personnalité ne font pas obstacle à une telle exigence, il conviendrait encore de tenir compte des droits fondamentaux reconnus à l'échelle mondiale.

99. En effet, ainsi que je l'ai indiqué dans un contexte différent, l'intérêt légitime du public à accéder à une information va forcément varier selon sa localisation géographique, d'un État tiers à l'autre [50]. De ce fait, s'agissant d'un retrait au niveau mondial, il existerait un danger que sa mise en œuvre empêche des personnes établies dans des États autres que celui de la juridiction saisie d'accéder à l'information.

100. Pour conclure, il ressort des considérations qui précèdent que la juridiction d'un État membre peut, en théorie, statuer sur le retrait d'informations diffusées au moyen d'Internet au niveau mondial. Toutefois, en raison des différences existant entre, d'une part, les lois nationales et, d'autre part, la protection de la vie privée et des droits de la personnalité prévue par celles-ci, et afin de respecter les droits fondamentaux largement répandus, une telle juridiction doit plutôt adopter une attitude d'autolimitation. Dès lors, dans le respect de la courtoisie internationale [51], évoquée par le gouvernement portugais, cette juridiction devrait, dans la mesure du possible, limiter les effets extraterritoriaux de ses injonctions en matière d'atteinte à la vie privée et aux droits de la personnalité [52]. La mise en œuvre d'une obligation de retrait ne devrait pas aller au-delà de ce qui est nécessaire pour atteindre la protection de la personne lésée. Ainsi, au lieu de supprimer le contenu, ladite juridiction pourrait, le cas échéant, ordonner de rendre impossible l'accès à ces informations à l'aide du géoblocage.

101. Ces considérations ne sauraient être remises en cause par l'argument de la requérante selon lequel le géoblocage des informations illicites serait facilement contournable par un serveur proxy ou par d'autres moyens.

102. Pour reprendre une réflexion formulée dans le contexte de situations relevant du droit de l'Union : la protection de la vie privée et des droits de la personnalité ne doit pas nécessairement être assurée de manière absolue mais doit être mise en balance avec la protection d'autres droits fondamentaux [53]. Il convient ainsi d'éviter des mesures exorbitantes qui ignoreraient le soin d'assurer un juste équilibre entre les différents droits fondamentaux [54].

103. Sans préjudice des remarques supplémentaires qui précèdent, s'agissant de la portée territoriale d'une obligation de retrait, je maintiens la position que j'ai avancée au point 93 des présentes conclusions.

B. Sur la troisième question préjudicielle

104. Par sa troisième question, la juridiction de renvoi cherche à savoir si l'article 15 de la directive 2000/31 s'oppose à ce que soit adressée à un hébergeur une injonction lui imposant l'obligation de retirer de sa plateforme des informations équivalant à celle ayant été jugée illicite dans le cadre d'une procédure en justice après qu'il a pris connaissance de ces informations.

50 Voir mes conclusions dans l'affaire Google (Portée territoriale du déréférencement) (C-507/17, EU:C:2019:15, point 60).

51 Voir, notamment, sur les implications pratiques de cette courtoisie internationale, Maier, H. G., op. cit., p. 283.

52 Voir doctrine citée à la note en bas de page 47. Voir, également, dans des contextes bien différents de celui de la présente affaire, Scott, J., « The New EU "Extraterritoriality" », *Common Market Law Review*, 2014, vol. 51, n° 5, p. 1378.

53 Voir, par analogie, en ce qui concerne la mise en balance du droit de propriété intellectuelle et du droit au respect de la vie privée et familiale, garanti à l'article 7 de la Charte, arrêt du 18 octobre 2018, Bastei Lübbe (C-149/17, EU:C:2018:841, points 44 à 47). Voir, également, mes conclusions dans l'affaire Bastei Lübbe (C-149/17, EU:C:2018:400, points 37 à 39).

54 Voir, en ce sens, en ce qui concerne la protection de la propriété intellectuelle, arrêt du 27 mars 2014, UPC Telekabel Wien (C-314/12, EU:C:2014:192, 58 à 63). Voir, également, conclusions de l'avocat général Cruz Villalón dans l'affaire UPC Telekabel Wien (C-314/12, EU:C:2013:781, points 99 à 101), ainsi que mes conclusions dans l'affaire Stichting Brein (C-610/15, EU:C:2017:99, points 69 à 72).

105. La requérante ainsi que les gouvernements autrichien, letton, portugais et finlandais considèrent, en substance, que l'article 15, paragraphe 1, de la directive 2000/31 ne fait pas obstacle à ce qu'il soit enjoint à un hébergeur de retirer des informations de contenu équivalant à celui ayant été jugé illicite, lorsqu'il en a eu connaissance. Compte tenu de son analyse de la première question, Facebook Ireland considère qu'il n'y a pas lieu de répondre à la troisième question.

106. Je me rallie au point de vue partagé, en substance, par la requérante et l'ensemble des gouvernements.

107. En effet, dès lors qu'une obligation de retrait n'implique pas de surveillance générale des informations stockées par un hébergeur, mais découle d'une prise de connaissance résultant de la notification effectuée par la personne concernée ou par les tiers, il n'y a pas de violation de l'interdiction prévue à l'article 15, paragraphe 1, de la directive 2000/31.

108. Par conséquent, je propose de répondre à la troisième question préjudicielle que l'article 15, paragraphe 1, de la directive 2000/31 doit être interprété en ce sens qu'il ne s'oppose pas à ce qu'un hébergeur soit contraint de retirer des informations équivalant à celle ayant été qualifiée d'illicite, dès lors qu'une obligation de retrait n'implique pas une surveillance générale des informations stockées, et découle d'une prise de connaissance résultant de la notification effectuée par la personne concernée, les tiers ou une autre source.

VI. Conclusion

109. Au vu de l'ensemble des considérations qui précèdent, je propose à la Cour d'apporter la réponse suivante aux questions préjudicielles déférées par le l'Oberster Gerichtshof (Cour suprême, Autriche) :

1) L'article 15, paragraphe 1, de la directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique ») doit être interprété en ce sens qu'il ne s'oppose pas à ce qu'un hébergeur qui exploite une plateforme de réseau social soit contraint, dans le cadre d'une injonction, de rechercher et d'identifier, parmi toutes les informations diffusées par les utilisateurs de cette plateforme, les informations identiques à celle ayant été qualifiée d'illicite par une juridiction ayant rendu cette injonction. Dans le cadre d'une telle injonction, un hébergeur peut être contraint de rechercher et d'identifier les informations équivalant à celle qualifiée d'illicite uniquement parmi des informations diffusées par l'utilisateur ayant diffusé cette information. Une juridiction statuant sur le retrait de telles informations équivalentes doit garantir que les effets de son injonction sont clairs, précis et prévisibles. Ce faisant, elle doit mettre en balance les droits fondamentaux en présence et tenir compte du principe de proportionnalité.

2) S'agissant de la portée territoriale d'une obligation de retrait imposée à un hébergeur dans le cadre d'une injonction, il y a lieu de considérer que celle-ci n'est réglementée ni par l'article 15, paragraphe 1, de la directive 2000/31 ni par aucune autre disposition de cette directive et, partant, que cette disposition ne s'oppose pas à ce qu'un hébergeur soit contraint de retirer des informations diffusées au moyen d'une plateforme de réseau social au niveau mondial. Par ailleurs, ladite portée territoriale n'est pas non plus réglementée par le droit de l'Union dans la mesure où, en l'espèce, le recours de la requérante n'est pas fondé sur celui-ci.

3) L'article 15, paragraphe 1, de la directive 2000/31 doit être interprété en ce sens qu'il ne s'oppose pas à ce qu'un hébergeur soit contraint de retirer des informations équivalant à celle ayant été qualifiée d'illicite, dès lors qu'une obligation de retrait n'implique pas une surveillance générale des informations stockées, et découle d'une prise de connaissance résultant de la notification effectuée par la personne concernée, les tiers ou une autre source.