



Reports of Cases

OPINION OF ADVOCATE GENERAL
SZPUNAR
delivered on 4 June 2019¹

Case C-18/18

Eva Glawischnig-Piesczek
v
Facebook Ireland Limited

(Request for a preliminary ruling from the Oberster Gerichtshof (Supreme Court, Austria))

(Reference for a preliminary ruling — Freedom to provide services — Directive 2000/31/EC — Information society services — Liability of intermediary service providers — Obligation of an internet site hosting services provider (Facebook) to delete illegal information — Scope)

I. Introduction

1. *The internet's not written in pencil, it's written in ink*, says a character in an American film released in 2010. I am referring here, and it is no coincidence, to the film *The Social Network*.
2. In fact, the key issue in the present case is whether a host which operates an online social network platform may be required to delete, with the help of a metaphorical ink eraser, certain content placed online by users of that platform.
3. More specifically, by its questions for a preliminary ruling, the referring court asks the Court to specify the personal scope and the material scope of the obligations that may be imposed on a host provider without a general monitoring obligation, which is prohibited under Article 15(1) of Directive 2000/31/EC,² being thus imposed on that host provider. The referring court also asks the Court to rule on whether, in the context of an injunction issued by a court of a Member State, a host provider may be ordered to remove certain content not only for internet users in that Member State but also worldwide.

II. Legal framework

A. EU law

4. Articles 14 and 15 of Directive 2000/31 are in Section 4, entitled 'Liability of intermediary service providers', of Chapter II of that directive.

¹ Original language: French.

² Directive of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ 2000 L 178, p. 1).

5. Article 14(1) and (3) of Directive 2000/31, entitled ‘Hosting’, provides:

‘1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

- (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

...

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.’

6. Article 15(1) of Directive 2000/31, entitled ‘No general obligation to monitor’, provides:

‘Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.’

B. Austrian law

7. According to Paragraph 18(1) of the E-Commerce-Gesetz (Law on electronic commerce), whereby the Austrian legislature transposed Directive 2000/31, providers of hosting services are under no general obligation to monitor the information which they store, transmit or make accessible, or to seek themselves facts or circumstances indicating illegal activity.

8. In accordance with Paragraph 1330(1) of the Allgemeines Bürgerliches Gesetzbuch (General Civil Code, ‘the ABGB’), anyone who has sustained actual harm or loss of profit owing to an injury to his honour is to be entitled to claim compensation. Under subparagraph 2 of that paragraph, the same is to apply when a person reports facts prejudicial to the reputation, material situation and future prospects of a third party which he knew or ought to have known to be inaccurate. In that case, a denial and publication thereof may be required.

9. Pursuant to Paragraph 78(1) of the Urheberrechtsgesetz (Law on copyright, ‘the UrhG’), images representing a person must not be displayed publicly or disseminated in another way that makes them accessible to the public if such publication or dissemination harms the legitimate interests of the person concerned or, if that person has died without having authorised or ordered such publication, the legitimate interests of a close relative.

III. The facts of the main proceedings

10. Ms Eva Glawischnig-Piesczek was a member of the Nationalrat (National Council, Austria), chair of the parliamentary party *die Grünen* (‘the Greens’) and the federal spokesperson of that party.

11. Facebook Ireland Limited, a company registered in Ireland having its headquarters in Dublin, is a subsidiary of the United States corporation Facebook Inc. Facebook Ireland operates, for users outside the United States and Canada, an online social network platform accessible at the address www.facebook.com. That platform enables users to create profile pages and to publish comments.

12. On 3 April 2016 a user of that platform shared on their personal page an article from the Austrian online news magazine *oe24.at* entitled ‘Greens: Minimum income for refugees should stay’. That publication had the effect of generating on the platform a ‘thumbnail’ of the original site, containing the title and a brief summary of the article, and a photograph of the applicant. That user also published, in connection with that article, an accompanying disparaging comment about the applicant accusing her of being a ‘lousy traitor of the people’, a ‘corrupt oaf’ and a member of a ‘fascist party’. The content placed online by that user could be consulted by any user of the platform in question.

13. By letter of 7 July 2016, the applicant, *inter alia*, asked Facebook Ireland to delete that comment.

14. As Facebook Ireland did not remove the comment in question, the applicant brought an action before the Handelsgericht Wien (Commercial Court, Vienna, Austria) and requested that court to issue an injunction ordering Facebook Ireland to cease publication and/or dissemination of the photographs of the applicant if the accompanying message disseminated the same allegations and/or ‘equivalent content’, namely that the applicant was a ‘lousy traitor of the people’ and/or a ‘corrupt oaf’ and/or a member of a ‘fascist party’.

15. On 7 December 2016 the Handelsgericht Wien (Commercial Court, Vienna) made the interlocutory order applied for.

16. Facebook Ireland subsequently disabled access in Austria to the content initially published.

17. On appeal, the Oberlandesgericht Wien (Higher Regional Court, Vienna, Austria) upheld the order made at first instance as regards the identical allegations. In doing so, it did not grant Facebook Ireland’s request that the interlocutory order be limited to the Republic of Austria. On the other hand, it held that the obligation to cease the dissemination of allegations of equivalent content related only to those brought to the knowledge of Facebook Ireland by the applicant in the main proceedings, by third parties or otherwise.

18. The courts of first and second instance based their decisions on Paragraph 78 of the UrhG and Paragraph 1330 of the ABGB, and took the view, in particular, that the public comment contained statements which were excessively harmful to the applicant’s reputation and gave the impression that she was involved in unlawful conduct, without providing the slightest evidence in that regard. Nor, according to those courts, was it permissible to rely on the right to freedom of expression for statements relating to a politician if there was no connection with a political debate or a debate that was in the public interest.

19. The two parties to the main proceedings brought actions before the Oberster Gerichtshof (Supreme Court, Austria), which considered that the statements at issue were intended to damage the applicant’s reputation, to insult her and to defame her.

20. The referring court is required to adjudicate on the question whether the cease and desist order made against a host provider which operates a social network with a large number of users may also be extended, worldwide, to statements with identical wording and/or having equivalent content of which it is not aware.

21. In that regard, the Oberster Gerichtshof (Supreme Court) states that, according to its own case-law, such an obligation must be considered to be proportionate where the service provider was already aware that the interests of the person concerned had been harmed on at least one occasion as a result of the contribution of a recipient of the service and where the risk that other infringements would be committed is thus demonstrated.

IV. The questions for a preliminary ruling and the procedure before the Court

22. It was in those circumstances that the Oberster Gerichtshof (Supreme Court), by decision of 25 October 2017, received at the Court on 10 January 2018, decided to stay proceedings and to refer the following questions to the Court:

- ‘(1) Does Article 15(1) of Directive [2000/31] generally preclude any of the obligations listed below of a host provider which has not expeditiously removed illegal information, specifically not just this illegal information within the meaning of Article 14(1)(a) of [that] directive, but also other identically worded items of information:
- (a) worldwide?
 - (b) in the relevant Member State?
 - (c) of the relevant user worldwide?
 - (d) of the relevant user in the relevant Member State?
- (2) In so far as Question 1 is answered in the negative: Does this also apply in each case for information with an equivalent meaning?
- (3) Does this also apply for information with an equivalent meaning as soon as the operator has become aware of this circumstance?’

23. Written observations were lodged by the applicant, Facebook Ireland, the Austrian, Latvian, Portuguese and Finnish Governments and also by the European Commission. Those parties, with the exception of the Portuguese Government, were represented at the hearing on 13 February 2019.

V. Analysis

A. The first and second questions

24. By its first and second questions, which should be examined together, the referring court asks the Court to determine the material scope and the personal scope of a monitoring obligation which may be imposed, in the context of an injunction, on the provider of an information society service consisting in storing information provided by a recipient of that service (a host provider), without a general monitoring obligation, which is prohibited by Article 15(1) of Directive 2000/31, thus being imposed.

25. Admittedly, these first two questions are concerned with the removal of information disseminated via an online social network platform rather than with the monitoring or filtering of that information. It should be observed, however, that social network platforms are media the content of which is generated principally not by their founding and managing companies but by their users. In addition, that content, which in the meantime is reproduced and altered, is constantly being exchanged between users.

26. In order to be able to delete information disseminated via such a platform or to disable access to it, irrespective of the author of the information and whatever its content, a host provider must first be able to identify that particular information among all the information stored on its servers. In order to do so, it must, in one way or another, monitor or filter that information. However, according to Article 15(1) of Directive 2000/31, to which the questions for a preliminary ruling refer, a Member State may not impose a general monitoring obligation on a host provider. All of that means that, by its first two questions, the referring court is seeking, in essence, to ascertain the personal scope and the material scope of such an obligation, which are consistent with the requirements laid down in Directive 2000/31.

27. By its first question, the referring court also asks the Court to clarify whether a host provider may be ordered to remove, worldwide, information disseminated via a social network platform.

28. In order to answer those two questions, I shall examine, in the first place, the scheme of Directive 2000/31 applicable to Facebook Ireland in its capacity as a host provider and then the implications of its being characterised as a host provider as regards the injunctions addressed to that service provider. In the second place, I shall then analyse the requirements laid down by EU law as regards the material scope and the personal scope of a monitoring obligation that may be imposed on a host provider in the context of an injunction, without a general monitoring obligation in that respect being thus imposed. Last, in the third place, I shall address the question of the territorial scope of a removal obligation.

1. The injunctions addressed to host providers in the light of Directive 2000/31

29. It should be borne in mind that, in order for the storage effected by the provider of an information society service to come within Article 14 of Directive 2000/31, that service provider's conduct must be limited to that of an 'intermediary service provider' within the meaning intended by the legislature in the context of Section 4 of that directive. In addition, according to recital 42 of that directive, such a service provider's conduct is purely technical, automatic and passive, which implies that it has neither knowledge of nor control over the data which it stores and that the role which it plays must therefore be neutral.³

30. The Court has already had occasion to make clear that the owner of a social network platform which stores on its services information provided by the users of that platform, relating to their profile, is a hosting service provider within the meaning of Article 14 of Directive 2000/31.⁴ Irrespective of the doubts that one might have in that regard, it is apparent from the request for a preliminary ruling that in the referring court's view it is common ground that Facebook Ireland is a host provider whose conduct is limited to that of an intermediary service provider.

31. Under Directive 2000/31, a host provider whose conduct is limited to that of an intermediary service provider enjoys relative immunity from liability for the information which it stores. In fact, that immunity is granted only if such a host provider was not aware of the illegal nature of the information stored or of the activity carried out by means of that information and on condition that, once made aware of that illegality, it acts expeditiously to remove the information or to disable access to it. Conversely, if that host provider does not fulfil those conditions, that is to say, if it was aware of the illegality of the information stored but did not take action in order to remove it or to disable access to it, Directive 2000/31 does not preclude its being held indirectly liable for that information.⁵

³ See, in particular, judgment of 23 March 2010, *Google France and Google* (C-236/08 to C-238/08, EU:C:2010:159, paragraphs 112 and 113).

⁴ See judgment of 16 February 2012, *SABAM* (C-360/10, EU:C:2012:85, paragraph 27).

⁵ See Article 14 of Directive 2000/31. See also my Opinion in *Stichting Brein* (C-610/15, EU:C:2017:99, points 67 and 68).

32. Furthermore, it is apparent from Article 14(3) of Directive 2000/31 that the immunity granted to an intermediary service provider does not prevent a court or administrative authority, in accordance with Member States' legal systems, from requiring that service provider to terminate or prevent an infringement. It follows from that provision that an intermediary service provider may be the addressee of injunctions, even though, according to the conditions set out in Article 14(1) of that directive, that service provider is not itself liable for the information stored on its servers.⁶

33. The conditions and detailed procedures applicable to such injunctions are matters for national law.⁷ However, the rules laid down by the Member States must comply with the requirements laid down in EU law, in particular in Directive 2000/31.

34. All of that reflects the EU legislature's intention to strike a balance, by means of that directive, between the different interests of host providers whose conduct is limited to that of an intermediary service provider, of users of their services and of persons harmed by any infringement committed in the use of those services. Consequently, it is for the Member States, when they implement the measures to transpose Directive 2000/31, not only to comply with the requirements laid down in that directive, but also to ensure that they do not rely on an interpretation that would be inconsistent with the fundamental rights involved or with the other general principles of EU law, such as the principle of proportionality.⁸

2. The requirements laid down with regard to the personal scope and the material scope of a monitoring obligation

(a) The prohibition of a general monitoring obligation

35. It should be observed that Article 15(1) of Directive 2000/31 prohibits Member States from imposing a general obligation on, among others, providers of services whose activity consists in storing information to monitor the information which they store or a general obligation actively to seek facts or circumstances indicating illegal activity. Furthermore, it is apparent from the case-law that that provision precludes, in particular, a host provider whose conduct is limited to that of an intermediary service provider from being ordered to monitor all⁹ or virtually all¹⁰ of the data of all users of its service in order to prevent any future infringement.

36. If, contrary to that provision, a Member State were able, in the context of an injunction, to impose a general monitoring obligation on a host provider, it cannot be precluded that the latter might well lose the status of intermediary service provider and the immunity that goes with it. In fact, the role of a host provider carrying out general monitoring would no longer be neutral. The activity of that host provider would not retain its technical, automatic and passive nature, which would imply that that host provider would be aware of the information stored and would monitor it.

37. Furthermore, even if such a risk did not exist, a host provider carrying out general monitoring could, as a matter of principle, be held liable for any illegal activity or information even if the conditions laid down in Article 14(1)(a) and (b) of that directive were not actually fulfilled.

⁶ See judgment of 7 August 2018, *SNB-REACT* (C-521/17, EU:C:2018:639, paragraph 51). See, also, to that effect, 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, No 2, p. 5.

⁷ See my Opinion in *Mc Fadden* (C-484/14, EU:C:2016:170). See also Husovec, M., *Injunctions Against Intermediaries in the European Union. Accountable But Not Liable?*, Cambridge University Press, Cambridge, 2017, pp. 57 and 58.

⁸ See to that effect, concerning respect for fundamental rights and for the principle of proportionality, judgment of 29 January 2008, *Promusicae* (C-275/06, EU:C:2008:54, paragraph 68).

⁹ See judgments of 12 July 2011, *L'Oréal and Others* (C-324/09, EU:C:2011:474, paragraphs 139 and 144), and of 24 November 2011, *Scarlet Extended* (C-70/10, EU:C:2011:771, paragraphs 36 and 40).

¹⁰ See judgment of 16 February 2012, *SABAM* (C-360/10, EU:C:2012:85, paragraphs 37 and 38).

38. Admittedly, Article 14(1)(a) of Directive 2000/31 makes the liability of an intermediary service provider subject to actual knowledge of the illegal activity or information. However, having regard to a general monitoring obligation, the illegal nature of any activity or information might be considered to be automatically brought to the knowledge of that intermediary service provider and the latter would have to remove the information or disable access to it without having been aware of its illegal content.¹¹ Consequently, the logic or relative immunity from liability for the information stored by an intermediary service provider would be systematically overturned, which would undermine the practical effect of Article 14(1) of Directive 2000/31.

39. In short, the role of a host provider carrying out such general monitoring would no longer be neutral, since the activity of that host provider would no longer retain its technical, automatic and passive nature, which would imply that the host provider would be aware of the information stored and would monitor that information. Consequently, the implementation of a general monitoring obligation, imposed on a host provider in the context of an injunction authorised, *prima facie*, under Article 14(3) of Directive 2000/31, could render Article 14 of that directive inapplicable to that host provider.

40. I thus infer from a reading of Article 14(3) in conjunction with Article 15(1) of Directive 2000/31 that an obligation imposed on an intermediary service provider in the context of an injunction cannot have the consequence that, by reference to all or virtually all of the information stored, the role of that intermediary service provider is no longer neutral in the sense described in the preceding point.

(b) The monitoring obligation applicable in a specific case

41. As stated in recital 47 of Directive 2000/31, the prohibition on imposing general obligations, laid down in Article 15(1) of that directive, does not concern monitoring obligations *in a specific case*. In fact, it follows from the wording of Article 14(3) of Directive 2000/31 that a host provider may be ordered to *prevent* an infringement, which, as the Commission claims, logically implies a certain form of monitoring in the future, without that monitoring being transformed into a general monitoring obligation.¹² Under Article 18 of that directive, moreover, Member States are required to ensure that court actions available under their national law concerning information society services' activities allow for the rapid adoption of measures designed, *inter alia*, to *prevent any further impairment* of the interests involved.

42. Furthermore, it follows from the judgment in *L'Oréal and Others*¹³ that a host provider may be ordered to take measures to prevent the occurrence of any *further infringements* of the same nature by the same recipient.

43. In that judgment, the Court did not interpret solely the provisions of Directive 2000/31, but also the provisions of Directive 2004/48/EC.¹⁴ In doing so, the Court defined a monitoring obligation consistent with the requirements imposed by those directives as opposed to the obligation prohibited under Article 15(1) of Directive 2000/31 to *actively monitor all or virtually all* of the data in order to prevent any further infringement.¹⁵ Independently of the specific context of the judgment in *L'Oréal and Others*¹⁶ and of the references to Directive 2004/48, the reasoning in that judgment in relation to the obligations of host providers consistent with EU law, depending on their general or specific nature, is of a cross-cutting nature and is therefore in my view capable of being transposed to the present case.

¹¹ See to that effect Opinion of Advocate General Jääskinen in *L'Oréal and Others* (C-324/09, EU:C:2010:757, point 143).

¹² See, also, to that effect, Rosati, E., *Copyright and the Court of Justice of the European Union*, Oxford University Press, Oxford, 2019, p. 158.

¹³ Judgment of 12 July 2011 (C-324/09, EU:C:2011:474, paragraph 144).

¹⁴ Directive of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45).

¹⁵ Judgment of 12 July 2011, *L'Oréal and Others* (C-324/09, EU:C:2011:474, paragraphs 139 and 144).

¹⁶ Judgment of 12 July 2011 (C-324/09, EU:C:2011:474).

44. Consequently, in order to prevent any further infringement, a host provider may be ordered, in the context of an injunction, to remove illegal information which has not yet been disseminated at the time when that injunction is adopted, without the dissemination of that information being brought, again and separately from the original removal request, to its knowledge.

45. However, in order not to result in the imposition of a general obligation, a monitoring obligation must, as seems to follow from the judgment in *L'Oréal and Others*,¹⁷ satisfy additional requirements, namely it must concern infringements of the *same nature* by the *same recipient of the same rights*, in that particular case trade mark rights.

46. Thus, I infer from that judgment that active monitoring is not irreconcilable with Directive 2000/31, unlike active monitoring the subject of which is not targeted at the specific case of an infringement.

47. Along the same lines, I pointed out in my Opinion in *Mc Fadden*,¹⁸ which concerned a provider of access to a communication network within the meaning of Article 12 of Directive 2000/31, taking inspiration from the preparatory work for Directive 2000/31, that in order for an obligation to be able to be considered to be applicable *to a specific case* it must, in particular, be limited in terms of *the subject* and *the duration* of the monitoring.

48. Those general requirements, formulated in the abstract, seem to me to be capable of being transposed to circumstances such as those of the main proceedings, in spite of the fact that, when the reasoning concerning the monitoring obligation relating to providers of access to a communications network such as the internet is applied, by analogy to host providers such as Facebook Ireland, the roles carried out by those intermediary service providers are different. To take, for example, a host provider such as Facebook Ireland, the contents of its platform seem to constitute all of the data stored, while for an internet access provider those contents represent only a tiny proportion of the data transmitted. Conversely, the nature and the intensity of the involvement of such a host provider in the processing of the digital content differ significantly from those of an internet access provider. As the Commission observes, a host provider is better placed than an access provider to take measures to seek and remove illegal information.

49. Furthermore, the requirement that a monitoring obligation be limited in time reflects a number of judgments of the Court.¹⁹ Although it is apparent from the case-law that the limitation in time of an obligation imposed in the context of an injunction relates more to the problem of the general principles of EU law,²⁰ I consider that a permanent monitoring obligation would be difficult to reconcile with the concept of an obligation applicable in a specific case, within the meaning of recital 47 of Directive 2000/31.

50. Accordingly, the targeted nature of a monitoring obligation should be envisaged by taking into consideration the duration of that monitoring and the information relating to the nature of the infringements in question, their author and their subject. Those elements are all interdependent and linked with each other. A global assessment is therefore required in order to answer the question whether an injunction does or does not comply with the prohibition laid down in Article 15(1) of Directive 2000/31.

¹⁷ Judgment of 12 July 2011, *L'Oréal and Others* (C-324/09, EU:C:2011:474, paragraphs 141 and 144).

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

¹⁹ More specifically, the Court stated, in the judgment of 12 July 2011, *L'Oréal and Others* (C-324/09, EU:C:2011:474, paragraph 140), that an injunction designed to prevent possible infringements of trade marks in the context of an information society service, namely an online market place, cannot have as its object or effect a general and *permanent* prohibition on the selling of goods bearing those trade marks. Likewise, the Court stated, in the judgment of 16 February 2012, *SABAM* (C-360/10, EU:C:2012:85, paragraph 45), that EU law precludes a monitoring obligation, imposed in the context of an injunction addressed to a service provider, having *no limitation in time*.

²⁰ This was the approach taken by Advocate General Jääskinen in his Opinion in *L'Oréal and Others* (C-324/09, EU:C:2010:757, point 181), which in my view strongly influenced the wording of the passages in question of the judgment delivered by the Court in that case.

(c) *Intermediate conclusions*

51. To recapitulate this part of my analysis, in the first place, it is apparent from a reading of Article 14(3) in conjunction with Article 15(1) of Directive 2000/31 that an obligation imposed on an intermediary service provider in the context of an injunction cannot lead to a situation in which, by reference to all or virtually all of the information stored, the role of that intermediary service provider would no longer be technical, automatic and passive, which would imply that the host provider concerned would be aware of that information and would monitor it.²¹

52. In the second place, active monitoring is not irreconcilable with Directive 2000/31, unlike active monitoring the subject of which is not targeted at the specific case of an infringement.²²

53. In the third place, the targeted nature of a monitoring obligation should be envisaged by taking into consideration the duration of that monitoring and the information relating to the nature of the infringements in question, their author and their subject.²³

54. It is in the light of those considerations that it is appropriate to address the personal scope and the material scope of a monitoring obligation of a service provider operating a social network platform, which amounts, in the present case, to seeking and identifying, among the information stored, information identical to that characterised as illegal by the court seised and also to seeking information equivalent to that information.

(d) *Application in the present case*

(1) *Information identical to the information characterised as illegal*

55. With the exception of Facebook Ireland, all the interested parties maintain that it must be possible to order a host provider to remove or block access to statements identical to the statement characterised as illegal that are published by the same user. The applicant, the Austrian and Latvian Governments and the Commission are, in essence, of the view that the same applies to statements published by other users.

56. It is apparent from the order for reference that the court at second instance considered that the reference to ‘identically worded items of information’ was to publications of photographs of the applicant *with the same accompanying text*. Likewise, the referring court explains that its doubts relate in particular to whether the injunction issued against Facebook Ireland may be extended to *statements (accompanying texts) that are word for word the same* and to those with equivalent content. I thus take that reference to ‘identically worded items of information’ to mean that the referring court has in mind precise manual reproductions of the information which it has characterised as illegal and, as the Austrian Government submits, automated reproductions, made through the ‘share’ function.

57. In that regard, I am of the view that a host provider that operates a social network platform may, for the purpose of enforcing an injunction issued by a court of a Member State, be ordered to seek and identify all the information identical to the information that has been characterised as illegal by that court.

²¹ See point 39 of this Opinion.

²² See point 46 of this Opinion.

²³ See point 50 of this Opinion.

58. In fact, as is clear from my analysis, a host provider may be ordered to prevent any further infringement of the same type and by the same recipient of an information society service.²⁴ Such a situation does indeed represent a specific case of an infringement that has actually been identified, so that the obligation to identify, among the information originating from a single user, the information identical to that characterised as illegal does not constitute a general monitoring obligation.

59. To my mind, the same applies with regard to information identical to the information characterised as illegal which is disseminated by other users. I am aware of the fact that this reasoning has the effect that the personal scope of a monitoring obligation encompasses every user and, accordingly, all the information disseminated via a platform.

60. Nonetheless, an obligation to seek and identify information identical to the information that has been characterised as illegal by the court seised is always targeted at the specific case of an infringement. In addition, the present case relates to an obligation imposed in the context of an interlocutory order, which is effective until the proceedings are definitively closed. Thus, such an obligation imposed on a host provider is, by the nature of things, limited in time.

61. Furthermore, the reproduction of the same content by any user of a social network platform seems to me, as a general rule, to be capable of being detected with the help of software tools, without the host provider being obliged to employ active non-automatic filtering of all the information disseminated via its platform.

62. In addition, imposing the obligation to seek and identify all the information identical to the information that was characterised as illegal makes it possible to ensure a fair balance between the fundamental rights involved.

63. First of all, seeking and identifying information identical to that which has been characterised as illegal by a court seised does not require sophisticated techniques that might represent an extraordinary burden. Such an obligation therefore does not appear to entail an excessive breach of the right to freedom to conduct a business which a host provider operating a social network platform such as Facebook Ireland enjoys under Article 16 of the Charter of Fundamental Rights of the European Union ('the Charter').

64. Next, in view of the ease with which information can be reproduced in the internet environment, the seeking and identification of information identical to that which has been characterised as illegal is necessary in order to ensure the effective protection of private life and personality rights.

65. Last, such an obligation respects internet users' fundamental right to freedom of expression and information, guaranteed in Article 11 of the Charter, in so far as the protection of that freedom need not necessarily be ensured absolutely, but must be weighed against the protection of other fundamental rights. As regards the information identical to the information that was characterised as illegal, it consists, *prima facie* and as a general rule, in repetitions of an infringement actually characterised as illegal. Those repetitions should be characterised in the same way, although such characterisation may be nuanced by reference, in particular, to the context of what is alleged to be an illegal statement. Incidentally, it should be noted that third parties who may be indirectly affected by injunctions are

²⁴ See points 42 and 45 of this Opinion.

not parties to the proceedings in which those injunctions are issued. It is for that reason, in particular, that it is necessary to ensure that those third parties are able to challenge, before a court, the implementing measures adopted by a host provider on the basis of an injunction,²⁵ and that possibility must not be conditional on being characterised as a party to main proceedings.²⁶

(2) *Equivalent information*

66. As regards the material scope of a monitoring obligation, the applicant maintains that a host provider may be subject to the obligation to remove statements that have equivalent content to that characterised as illegal and are published by the same user. The Austrian Government and the Commission, on the other hand, submit that the possibility of imposing such an obligation depends on the outcome of the weighing of the interests involved. Only the applicant contends that it is possible to order a host provider to remove statements that have content equivalent to the statement that was characterised as illegal and are published by other users.

67. The reference to ‘equivalent information’ or to information ‘having equivalent content’ gives rise to difficulties of interpretation, since the referring court does not state the meaning of those expressions. It may however be inferred from the reference for a preliminary ruling that the reference to information ‘having equivalent content’ is to information that *scarcely diverges* from the original information or to situations in which *the message remains essentially unaltered*. I take those indications to mean that a reproduction of the information that was characterised as illegal containing a typographical error and a reproduction having slightly altered syntax or punctuation constitutes ‘equivalent information’. It is not clear, however, that the equivalence referred to in the second question does not go further than such cases.

68. Admittedly, it is apparent from the judgment in *L’Oréal and Others*²⁷ that an information society service provider may be ordered to take measures that help to prevent *new infringements* of the *same kind* of the same rights.

69. However, it is important not to lose sight of the factual context in which the relevant case-law was developed, namely the context of infringements of intellectual property law. Generally, such infringements consist in the dissemination of the same content as that protected or, at least, a content resembling the protected content, any changes in that content, which are sometimes difficult to make, requiring specific intervention.

70. On the other hand, it is unusual for a defamatory act to use the precise terms of an act of the same type. That is, in part, the result of the personalised nature of the way in which ideas are expressed. In addition, unlike infringements of intellectual property law, defamatory acts subsequent to the original defamatory act reproduce rather the fact of uttering words that harm a person’s reputation than the form of the original act. For that reason, in connection with defamation, a mere reference to acts of the same nature could not play the same role as in connection with infringements of intellectual property law.

²⁵ See, by analogy, judgment of 27 March 2014, *UPC Telekabel Wien* (C-314/12, EU:C:2014:192, paragraph 57).

²⁶ See, by analogy, judgments of 25 May 2016, *Meroni* (C-559/14, EU:C:2016:349, paragraphs 49 and 50), and of 21 December 2016, *Biuro podróży ‘Partner’* (C-119/15, EU:C:2016:987, paragraph 40). On the problem area of the principle of effective judicial protection vis-à-vis third parties, see, also, Kaléda, 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 and 223.

²⁷ Judgment of 12 July 2011 (C-324/09, EU:C:2011:474).

71. In any event, the interpretation given to the reference to ‘equivalent information’ is liable to affect the scope of a monitoring obligation and the exercise of the fundamental rights involved. A court adjudicating, in the context of an injunction, on the removal of ‘equivalent information’ must thus respect the principle of legal certainty and ensure that the effects of that injunction are clear, precise and foreseeable. In doing so, that court must weigh up the fundamental rights involved and take account of the principle of proportionality.

72. Without prejudice to those considerations, and again taking inspiration from the judgment in *L’Oréal and Others*,²⁸ I am of the view that, for even more compelling reasons, a host provider may be ordered to identify information equivalent to that characterised as illegal and originating from the same user. Incidentally, in that case also, that user should be guaranteed the possibility of challenging before a court the implementing measures adopted by a host provider in order to comply with an injunction.

73. Conversely, the identification of information equivalent to that characterised as illegal originating from other users would require the monitoring of all the information disseminated via a social network platform. Unlike information identical to that characterised as illegal, information equivalent to that information cannot be identified unless a host provider employs sophisticated solutions. Consequently, not only would the role of a service provider carrying out general monitoring no longer be neutral, in the sense that it would not be merely technical, automatic and passive, but that service provider, by exercising a form of censorship, would become an active contributor to that platform.

74. Furthermore, an obligation to identify information equivalent to that characterised as illegal originating from any user would not ensure a fair balance between the protection of private life and personality rights, the protection of freedom to conduct a business and the protection of freedom of expression and information. On the one hand, seeking and identifying such information would require costly solutions, which would have to be developed and introduced by a host provider. On the other hand, the implementation of those solutions would lead to censorship, so that freedom of expression and information might well be systematically restricted.

75. In the light of the foregoing considerations, I propose that the answer to the first and second questions, in so far as they relate to the personal scope and the material scope of a monitoring obligation, should be that Article 15(1) of Directive 2000/31 must be interpreted as meaning that it does not preclude a host provider operating a social network platform from being ordered, in the context of an injunction, to seek and identify, among all the information disseminated by users of that platform, the information identical to the information that was characterised as illegal by a court that has issued that injunction. In the context of such an injunction, a host provider may be ordered to seek and identify the information equivalent to that characterised as illegal only among the information disseminated by the user who disseminated that illegal information. A court adjudicating on the removal of such equivalent information must ensure that the effects of its injunction are clear, precise and foreseeable. In doing so, it must weigh up the fundamental rights involved and take account of the principle of proportionality.

²⁸ Judgment of 12 July 2011 (C-324/09, EU:C:2011:474).

3. Removal worldwide

(a) Preliminary observations

76. I shall now address the referring court's doubts in respect of the territorial scope of a removal obligation. Those doubts relate, in essence, to whether a host provider may be ordered to remove content which has been characterised as illegal under the national law of a Member State not only in that Member State but also worldwide.

77. As a preliminary point, it is true that Facebook Ireland, as a subsidiary of Facebook, operates an electronic platform solely for users outside the United States and Canada. However, that circumstance does not seem to be such as to preclude the removal worldwide of the information disseminated via that platform. In fact, Facebook Ireland does not deny that it is in a position to ensure such removal worldwide.

78. It should be observed, however, that the EU legislature has not harmonised the material rules on harm to private life and personality rights, including defamation.²⁹ Nor, in the absence of consensus at EU level,³⁰ has the EU legislature harmonised the conflict-of-law rules in that field.³¹ Thus, when hearing actions in defamation, each court in the European Union applies the law designated as applicable under the national conflict rules.

79. The situation at issue in the main proceedings is, *prima facie*, different from that which constituted the starting point of my analysis concerning the territorial scope of a de-referencing of the results of a search engine in *Google (Territorial scope of de-referencing)*,³² cited by Facebook Ireland and the Latvian Government. That case concerns Directive 95/46/EC,³³ which harmonises, at Union level, certain material rules on data protection. It was, notably, the fact that the applicable material rules are harmonised that led me to conclude that a service provider had to be required to delete the results displayed following a search carried out not only from a single Member State but from a place within the European Union.³⁴ However, in my Opinion in that case I did not exclude the possibility that there might be situations in which the interest of the Union requires the application of the provisions of that directive beyond the territory of the European Union.³⁵

80. Consequently, as regards defamatory infringements, the imposition in one Member State of an obligation consisting in removing certain information worldwide, for all users of an electronic platform, because of the illegality of that information established under an applicable law, would have the consequence that the finding of its illegality would have effects in other States. In other words, the finding of the illegal nature of the information in question would extend to the territories of those other States. However, it is not precluded that, according to the laws designated as applicable under those States' national conflict rules, that information might be considered legal.

81. As the discussion between the interested parties illustrates, the reluctance to afford such extraterritorial effects to injunctions reflects the position of Facebook Ireland and that of the Latvian, Portuguese and Finnish Governments. With the exception of the Portuguese Government, moreover, those parties also seem to entertain doubts as to the territorial extent of the jurisdiction of the courts

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

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

31 See Article 1(2) of Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) (OJ 2007 L 199, p. 40).

32 I am referring here to my Opinion in *Google (Territorial scope of de-referencing)* (C-507/17, EU:C:2019:15).

33 Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

34 See my Opinion in *Google (Territorial scope of de-referencing)* (C-507/17, EU:C:2019:15, points 47, 55, 76 and 77).

35 See my Opinion in *Google (Territorial scope of de-referencing)* (C-507/17, EU:C:2019:15, point 62).

of a Member State. In essence, those parties seem to consider that the court of a Member State may not adjudicate, in the context of an injunction addressed to a host provider, on the removal of content outside the territory of that Member State. It is therefore appropriate to analyse those two questions, namely the territorial scope of a removal obligation and the extent of the jurisdiction of the courts of a Member State, addressing first of all the question of jurisdiction, which, as a general rule, precedes the question of substance.

(b) *The territorial scope of the jurisdiction*

82. Directive 2000/31 does not regulate jurisdiction to adjudicate on injunctions. On the other hand, as is clear from the judgment in *eDate Advertising and Others*,³⁶ in the event of an alleged infringement of personality rights through content placed online on an internet site, a person who considers that he has been harmed has the option to bring the matter before the competent courts of the Member States under Regulation (EU) No 1215/2012.³⁷ In fact, while the conflict rules relating to defamation are not harmonised at EU level, the position is different for the rules on jurisdiction.

83. In that regard, it is appropriate to add that the jurisdiction rules in Regulation No 1215/2012 also apply to disputes concerning the removal of defamatory content placed online.³⁸ It is immaterial in the present case, moreover, that such a request is directed not against a publisher but against the host provider of the content placed online. That being the case, I shall not propose that the Court reformulate the questions referred to it, since only the interested parties entertain doubts as to the territorial extent of jurisdiction. Nonetheless, I should like to make a few observations on the subject.

84. According to the judgment in *eDate Advertising and Others*,³⁹ a person who considers that he has been harmed may bring proceedings before, in particular, the courts of the Member State in which his centre of interests is located. Those courts have jurisdiction to adjudicate on all the damage caused. It seems that, in the present case, the court before which the applicant brought proceedings is the court of the place of her centre of interests.⁴⁰

85. It is true that, in the judgment in *eDate Advertising and Others*,⁴¹ the Court indicated that a person who considers that he has been harmed may bring an action in one forum in respect of all the damage caused, depending on the place in which the damage caused in the European Union occurred. Admittedly, that may give the impression that the territorial extent of the jurisdiction of that forum does not encompass the facts relating to the territories of third States. However, that consideration reflects rather the fact that, in order to have jurisdiction under Regulation No 1215/2012, on the basis

³⁶ Judgment of 25 October 2011 (C-509/09 and C-161/10, EU:C:2011:685, paragraphs 43 and 44).

³⁷ Regulation of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ 2012 L 351, p. 1).

³⁸ Judgment of 17 October 2017, *Bolagsupplysningen and Ilsjan* (C-194/16, EU:C:2017:766, paragraph 44).

³⁹ Judgment of 25 October 2011 (C-509/09 and C-161/10, EU:C:2011:685, paragraph 48).

⁴⁰ Consequently, in spite of the fact that the referring court is called upon to adjudicate on an interlocutory order, there is no need to consider the implications of Article 35 of Regulation No 1215/2012 on the territorial extent of jurisdiction and on the territorial scope of a removal obligation imposed in the context of an injunction.

⁴¹ Judgment of 25 October 2011 (C-509/09 and C-161/10, EU:C:2011:685, paragraph 48).

of the place in which the damage occurred, that forum must be a court of a Member State. Furthermore, with the exception of that consideration, the Court stated on numerous occasions in that judgment that that forum had jurisdiction to adjudicate on all the damage resulting from the defamation.⁴²

86. I infer that, contrary to Facebook Ireland's contention, and that of the Latvian and Finnish Governments, the court of a Member State may, as a general rule, adjudicate on the removal of content outside the territory of that Member State, as the territorial extent of its jurisdiction is universal.⁴³ A court of a Member State may be prevented from adjudicating on a removal worldwide not because of a question of jurisdiction but, possibly, because of a question of substance.

87. It is now appropriate to analyse the question of the extraterritorial effects of injunctions addressed to host providers, which, as I observed in point 81 of this Opinion, amounts to the question of the territorial scope of a removal obligation.

(c) The territorial scope of a removal obligation

88. First of all, it should be observed that, as the Finnish Government acknowledges, Article 15(1) of Directive 2000/31 does not regulate the territorial effects of injunctions addressed to information society service providers. In addition, provided that they satisfy the requirements laid down in Directive 2000/31, removal obligations imposed on those service providers in the context of injunctions are a matter for national law.

89. Next, it is difficult, in the absence of regulation by the Union with respect to harm to private life and personality rights, to justify the territorial effects of an injunction by relying on the protection of fundamental rights guaranteed in Articles 1, 7 and 8 of the Charter. In fact, the scope of the Charter follows the scope of EU law and not vice versa,⁴⁴ and, in the present case, as regards its substance, the applicant's action is not based on EU law.

90. In that regard, it should be observed that the applicant does not appear to be relying on rights relating to the protection of personal data and that she does not take issue with Facebook Ireland for having 'carried out' an illegal processing of her data, as her claim is based on the general provisions of civil law. Nor does the referring court rely on the legal instruments of EU law relevant to data protection. It relies only on Directive 2000/31. However, it follows from Article 1(5)(b) thereof that that directive is not to apply to questions relating to information society services covered by the directives concerning the protection of personal data.

⁴² Judgment of 25 October 2011, *eDate Advertising and Others* (C-509/09 and C 161/10, EU:C:2011:685, paragraphs 48, 51 and 52). See also judgment of 17 October 2017, *Bolagsupplysningen and Ilsjan* (C-194/16, EU:C:2017:766, paragraphs 38 and 47). Furthermore, according to the interpretations put on that judgment in the literature, the forum of the centre of interests may adjudicate throughout the world on the damage caused. See Mankowski, P., in Magnus, U., and Mankowski, P. (Eds), *Brussels I bis Regulation – Commentary*, Otto Schmidt, Cologne, 2016, Art. 7, paragraph 364. The same applies to the territorial extent of the general jurisdiction of the forum of the defendant. In the judgment of 1 March 2005, *Owusu* (C-281/02, EU:C:2005:120, paragraph 26), the Court considered that the Brussels [Convention of 27 September 1968 on jurisdiction and the enforcement of judgments in civil and commercial matters (OJ 1978 L 304, p. 36)] may apply when the claimant and the defendant are domiciled in one Member State while the facts at issue occurred in a third country. I infer that in such a case the forum of the debtor has jurisdiction to adjudicate on such disputed facts. See also Van Calster, G., Luks, C., *Extraterritoriality and private international law, Recht in beweging – 19de VRG Alumnidag 2012*, MAKLU, Antwerp, Apeldoorn, 2012, p. 132.

⁴³ It is therefore a matter here of jurisdiction known as 'global' or 'general'. See 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, pp. 550 and 551.

⁴⁴ See judgment of 26 February 2013, *Åkerberg Fransson* (C-617/10, EU:C:2013:105, paragraph 19). See also my Opinion in *Google (Territorial scope of de-referencing)* (C-507/17, EU:C:2019:15, point 55).

91. Last, although Regulation No 1215/2012 may prove helpful as regards the effects of injunctions in the Member States, that is not the case as regards the effects produced outside the Union. In fact, that regulation does not require that an injunction issued by the court of a Member State also produce effects in third States. In addition, the fact that a court has jurisdiction to adjudicate on the substance under a jurisdiction rule of EU law does not mean that in doing so it is applying only material rules which come within the scope of EU law and therefore of the Charter.

92. For those reasons, both the question of the extraterritorial effects of an injunction imposing a removal obligation and the question of the territorial scope of such an obligation should be analysed not by reference to EU law but, in particular, by reference to public and private international law, which is not harmonised at EU level.⁴⁵ In fact, there is nothing to indicate that the situation forming the subject matter of the main proceedings may come within the scope of EU law and therefore of the rules of international law that influence the interpretation of EU law.⁴⁶

93. Consequently, as regards the territorial scope of a removal obligation imposed on a host provider in the context of an injunction, it should be considered that that obligation is not regulated either by Article 15(1) of Directive 2000/31 or by any other provision of that directive and that that provision therefore does not preclude that host provider from being ordered to remove worldwide information disseminated via a social network platform. Nor is that territorial scope regulated by EU law, since in the present case the applicant's action is not based on EU law.

94. That being so, both in the interest of completeness and in case the Court should not follow my proposal, I shall make a few additional observations as regards the removal of information disseminated worldwide via a social network platform.

95. In international law, it is not precluded that an injunction may have what are known as 'extraterritorial' effects.⁴⁷ As I stated in point 80 of this Opinion, such an approach would have the consequence that the finding that the information concerned was illegal would be extended to the territories of other Member States, irrespective of whether or not that information was legal under the law designated as applicable according to the conflict-of-law rules of those Member States.

96. It might therefore be argued that the Court has already implicitly accepted such an approach in the judgment in *Bolagsupplysningen and Ilsjan*.⁴⁸ It is true that in that judgment the Court did not adjudicate on the law applicable to a request to remove content placed online. However, it held that, in the light of *the ubiquitous nature of the information and content placed online on a website* and the fact that *the scope of their distribution is, in principle, universal*, an application for, inter alia, the removal of such content must be made before a court with jurisdiction to rule on the entirety of an application for compensation for damage. In doing so, in my view, that court would apply the law or laws designated under its conflict rules.⁴⁹ It cannot be precluded that a court of a Member State would apply, in that context, a single law designated as applicable.

⁴⁵ As regards the extraterritorial effects of judicial decisions, it is sometimes difficult to draw a line between public and private international law. See 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, and Svantesson, D.J.B., *Solving the Internet Jurisdiction Puzzle*, Oxford University Press, Oxford, 2017, p. 40.

⁴⁶ See to that effect order of 12 July 2012, *Curà and Others* (C-466/11, EU:C:2012:465, paragraph 19).

⁴⁷ See 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 Judgment of 17 October 2017 (C-194/16, EU:C:2017:766, paragraph 44).

⁴⁹ See, also, as regards the implications of that judgment, 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, and 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, paragraph 59.

97. However, if such a court could not adjudicate on the removal of content placed online at worldwide level, the question would then arise as to which court would be better placed to rule on such removal. In fact, each court would be faced with the inconveniences described in the preceding point. Furthermore, should a claimant be required, in spite of the practical difficulties, to prove that the information characterised as illegal according to the law designated as applicable under the conflict rules of the Member State in which he brought the action is illegal according to all the potentially applicable laws?

98. Even if it were accepted that the considerations relating to the territorial nature of the protection available under the material rules on harm to the private life and to personality rights do not preclude such a requirement, it would still be necessary to take into account the fundamental rights recognised throughout the world.

99. As I have pointed out in a different context, the legitimate public interest in having access to information will necessarily vary, depending on its geographic location, from one third State to another.⁵⁰ Thus, as regards removal worldwide, there is a danger that its implementation will prevent persons established in States other than that of the court seised from having access to the information.

100. To conclude, it follows from the foregoing considerations that the court of a Member State may, in theory, adjudicate on the removal worldwide of information disseminated via the internet. However, owing to the differences between, on the one hand, national laws and, on the other, the protection of the private life and personality rights provided for in those laws, and in order to respect the widely recognised fundamental rights, such a court must, rather, adopt an approach of self-limitation. Therefore, in the interest of international comity,⁵¹ to which the Portuguese Government refers, that court should, as far as possible, limit the extraterritorial effects of its judgments concerning harm to private life and personality rights.⁵² The implementation of a removal obligation should not go beyond what is necessary to achieve the protection of the injured person. Thus, instead of removing the content, that court might, in an appropriate case, order that access to that information be disabled with the help of geo-blocking.

101. Those considerations cannot be called into question by the applicant's argument that the geo-blocking of the illegal information could be easily circumvented by a proxy server or by other means.

102. To take an observation formulated in the context of situations coming under EU law: the protection of private life and of personality rights need not necessarily be ensured in absolute terms but must be weighed against the protection of other fundamental rights.⁵³ It is thus necessary to avoid excessive measures that would disregard the need to strike a fair balance between the different fundamental rights.⁵⁴

103. Without prejudice to the foregoing additional observations, as regards the territorial scope of a removal obligation, I maintain the position which I put forward in point 93 of this Opinion.

⁵⁰ See my Opinion in *Google (Territorial scope of de-referencing)* (C-507/17, EU:C:2019:15, point 60).

⁵¹ See, in particular, on the practical implications of that international comity, Maier, H.G, op. cit., p. 283.

⁵² See the literature cited in footnote 47. See, also, in contexts very different from that of the present case, Scott, J., "The New EU "Extraterritoriality", *Common Market Law Review*, 2014, Vol. 51, No 5, p. 1378.

⁵³ See, by analogy, as regards the balance to be struck between intellectual property law and the right to respect for private and family life, guaranteed in Article 7 of the Charter, judgment of 18 October 2018, *Bastei Lübbe* (C-149/17, EU:C:2018:841, paragraphs 44 to 47). See also my Opinion in *Bastei Lübbe* (C-149/17, EU:C:2018:400, points 37 to 39).

⁵⁴ See to that effect, as regards the protection of intellectual property, judgment of 27 March 2014, *UPC Telekabel Wien* (C-314/12, EU:C:2014:192, paragraphs 58 to 63). See also Opinion of Advocate General Cruz Villalón in *UPC Telekabel Wien* (C-314/12, EU:C:2013:781, points 99 to 101), and also my Opinion in *Stichting Brein* (C-610/15, EU:C:2017:99, points 69 to 72).

B. The third question

104. By its third question, the referring court seeks to ascertain whether Article 15 of Directive 2000/31 precludes an injunction being addressed to a host provider that imposes on the latter an obligation to remove from its platform information equivalent to the information that was held to be illegal in the context of judicial proceedings after it has become aware of that information.

105. The applicant and the Austrian, Latvian, Portuguese and Finnish Governments maintain, in essence, that Article 15(1) of Directive 2000/31 does not preclude a host provider from being ordered to remove information having content equivalent to that held to be illegal, where it has become aware of that information. Having regard to its analysis of the first question, Facebook Ireland maintains that there is no need to answer the third question.

106. I support the viewpoint shared, in essence, by the applicant and all of the governments.

107. In fact, since a removal obligation does not imply the general monitoring of the information stored by a host provider, but is the consequence of awareness resulting from the notification made by the person concerned or by third parties, there is no breach of the prohibition laid down in Article 15(1) of Directive 2000/31.

108. I therefore propose that the answer to the third question be that Article 15(1) of Directive 2000/31 must be interpreted as meaning that it does not preclude a host provider from being ordered to remove information equivalent to the information characterised as illegal, provided that a removal obligation does not entail general monitoring of the information stored, and is the consequence of awareness resulting from the notification made by the person concerned, third parties or another source.

VI. Conclusion

109. In the light of all of the foregoing considerations, I propose that the Court answer the questions referred by the Oberster Gerichtshof (Supreme Court, Austria) as follows:

- (1) Article 15(1) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('the Directive on electronic commerce') must be interpreted as meaning that it does not preclude a host provider which operates a social network platform from being ordered, in the context of an injunction, to seek and identify, among all the information disseminated by users of that platform, the information identical to the information that has been characterised as illegal by a court that issued that injunction. In the context of such an injunction, a host provider may be ordered to seek and identify the information equivalent to that characterised as illegal only among the information disseminated by the user that disseminated that illegal information. A court adjudicating on the removal of such equivalent information must ensure that the effects of its injunction are clear, precise and foreseeable. In doing so, it must weigh up the fundamental rights involved and take account of the principle of proportionality.
- (2) As regards the territorial scope of a removal obligation imposed on a host provider in the context of an injunction, it should be considered that that obligation is not regulated either by Article 15(1) of Directive 2000/31 or by any other provision of that directive and that that provision therefore does not preclude that host provider from being ordered to remove worldwide information disseminated via a social network platform. Nor is that territorial scope regulated by EU law, since in the present case the applicant's action is not based on EU law.

- (3) Article 15(1) of Directive 2000/31 must be interpreted as meaning that it does not preclude a host provider from being ordered to remove information equivalent to the information characterised as illegal, provided that a removal obligation does not entail general monitoring of the information stored, and is the consequence of awareness resulting from the notification made by the person concerned, third parties or another source.