Raccolta della giurisprudenza

CONCLUSIONI DELL'AVVOCATO GENERALE
MACIEJ SZPUNAR
presentate il 4 giugno 2019[1]

Causa C-18/18

Eva Glawischnig-Piesczek
contro
Facebook Ireland Limited

[domanda di pronuncia pregiudiziale proposta dall'Oberster Gerichtshof (Corte Suprema, Austria)]

«Rinvio pregiudiziale – Libera prestazione di servizi – Direttiva 2000/31/CE – Servizi della società dell'informazione – Responsabilità dei prestatori intermediari – Obbligo di un prestatore di servizi di hosting di siti Internet (Facebook) di cancellare informazioni illecite – Portata»

I. Introduzione

1. *Su Internet si scrive con l'inchiostro, non a matita*, constata un personaggio di un film americano uscito nel 2010. Mi riferisco in questo caso, e non è una coincidenza, al film *The Social Network*.

2. Infatti, al centro della causa in esame si trova la questione se un host provider che gestisce una piattaforma di rete sociale in linea possa essere obbligato a far sparire, con l'ausilio di un metaforico correttore per inchiostro, determinati contenuti messi in rete da utenti di tale piattaforma.

3. Più specificamente, con le sue questioni pregiudiziali, il giudice del rinvio invita la Corte a specificare la portata personale e sostanziale degli obblighi che possono essere imposti ad un host provider, senza che ciò porti ad imporre un obbligo generale in materia di sorveglianza, vietato ai sensi dell'articolo 15, paragrafo 1, della direttiva 2000/31/CE[2]. Il giudice del rinvio chiede parimenti alla Corte di dichiarare se, nell'ambito di un'ingiunzione emessa dal giudice di uno Stato membro, un host provider possa essere costretto a rimuovere determinati contenuti non solo per gli utenti di Internet di tale Stato membro, bensì anche a livello mondiale.

II. Contesto normativo

A. Diritto dell'Unione

4. Gli articoli 14 e 15 della direttiva 2000/31 figurano nella sezione 4, intitolata «Responsabilità dei prestatori intermediari», del capo II di tale direttiva.

1 Lingua originale: il francese.

2 Direttiva del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («direttiva sul commercio elettronico») (GU 2000, L 178, pag. 1).

5. L'articolo 14, paragrafi 1 e 3, della direttiva 2000/31, intitolato «"Hosting"», così recita:

«1. Gli Stati membri provvedono affinché, nella prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore:

a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, o

b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.

(…)

3. Il presente articolo lascia impregiudicata la possibilità, per un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici degli Stati membri, di esigere che il prestatore ponga fine ad una violazione o la impedisca nonché la possibilità, per gli Stati membri, di definire procedure per la rimozione delle informazioni o la disabilitazione dell'accesso alle medesime».

6. L'articolo 15, paragrafo 1, della direttiva 2000/31, intitolato «Assenza dell'obbligo generale di sorveglianza», prevede quanto segue:

«Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite».

B. Normativa austriaca

7. Ai sensi dell'articolo 18, paragrafo 1, dell'E-Commerce-Gesetz (legge sul commercio elettronico), con cui il legislatore austriaco ha recepito la direttiva 2000/31, i prestatori di servizi di hosting non hanno un obbligo generale di sorvegliare le informazioni che memorizzano, trasmettono o rendono accessibili, né di ricercare essi stessi fatti o circostanze che indichino la presenza di attività illecite.

8. In conformità all'articolo 1330, paragrafo 1, dell'Allgemeines Bürgerliches Gesetzbuch (codice civile generale; in prosieguo: l'«ABGB»), chiunque abbia subito un danno concreto o un mancato guadagno a causa di una lesione dell'onore, ha diritto di chiedere il risarcimento. Ai sensi del paragrafo 2 di tale articolo, ciò vale anche qualora una persona divulghi fatti lesivi della reputazione, della situazione materiale e delle prospettive future altrui e conoscesse o avesse dovuto conoscere la loro falsità. In tal caso, è possibile anche pretenderne la smentita e pubblicazione.

9. In applicazione dell'articolo 78, paragrafo 1, dell'Urheberrechtsgesetz (legge sul diritto d'autore; in prosieguo: l'«UrhG»), le immagini che rappresentano una persona non devono essere esposte in pubblico né altrimenti divulgate in modo tale da renderle accessibili al pubblico, ove ciò possa comportare la lesione di interessi legittimi dell'interessato ovvero, qualora questo sia deceduto senza averne consentito od ordinato la pubblicazione, quelli di un prossimo congiunto.

III. Fatti

10. La sig.ra Eva Glawischnig-Piesczek era deputata al Nationalrat (Parlamento austriaco), presidente del gruppo parlamentare *die Grünen* («i Verdi») e portavoce nazionale di tale partito.

11. La Facebook Ireland Limited, società registrata in Irlanda con sede a Dublino, è una controllata della società statunitense Facebook Inc. La Facebook Ireland gestisce, per gli utenti situati al di fuori degli Stati Uniti e del Canada, una piattaforma di rete sociale in linea, accessibile all'indirizzo www.facebook.com. Tale piattaforma consente agli utenti di creare pagine di profili e di pubblicare commenti.

12. Il 3 aprile 2016, un utente di detta piattaforma ha condiviso, sulla sua pagina personale, un articolo della rivista di informazione austriaca online *oe24.at* intitolato «I Verdi: a favore del mantenimento di un reddito minimo per i rifugiati». Tale pubblicazione ha avuto come effetto quello di generare su tale piattaforma un «riquadro anteprima» del sito originario, contenente il titolo e un breve riassunto di tale articolo, nonché una fotografia della ricorrente. Tale utente ha inoltre pubblicato, a proposito di tale articolo, un commento degradante nei confronti della ricorrente, contestando a quest'ultima di essere una «brutta traditrice del popolo», un'«imbecille corrotta» e un membro di un «partito di fascisti». I contenuti messi in rete da tale utente potevano essere consultati da qualunque utente della piattaforma in questione.

13. Con lettera del 7 luglio 2016, la ricorrente ha segnatamente chiesto alla Facebook Ireland di cancellare tale commento.

14. Poiché la Facebook Ireland non rimuoveva il commento in questione, la ricorrente ha presentato un ricorso dinanzi al Handelsgericht Wien (tribunale di commercio di Vienna, Austria) e ha chiesto a tale giudice l'emissione di un'ordinanza cautelare che imponesse alla Facebook Ireland di cessare la pubblicazione e/o la diffusione di fotografie raffiguranti la ricorrente ove accompagnate da un messaggio con cui venissero diffuse affermazioni identiche e/o «dal contenuto equivalente», ossia quelle che definivano la ricorrente come una «brutta traditrice del popolo» e/o una «imbecille corrotta» e/o membro di un «partito di fascisti».

15. Il 7 dicembre 2016, il Handelsgericht Wien (tribunale di commercio di Vienna) ha emesso l'ordinanza cautelare richiesta.

16. La Facebook Ireland ha quindi disabilitato l'accesso in Austria al contenuto inizialmente pubblicato.

17. Adito in appello, l'Oberlandesgericht Wien (tribunale superiore del Land, Vienna, Austria) ha confermato l'ordinanza emessa in primo grado con riferimento alle affermazioni identiche. Nel farlo, tale giudice non ha accolto la domanda della Facebook Ireland intesa a limitare l'ordinanza cautelare alla Repubblica d'Austria. Per contro, detto giudice ha dichiarato che l'obbligo di cessare la diffusione di affermazioni dal contenuto equivalente riguardava unicamente quelle portate a conoscenza della Facebook Ireland dalla ricorrente nel procedimento principale, da terzi o in altro modo.

18. I giudici di primo e di secondo grado hanno fondato le loro decisioni sull'articolo 78 dell'UrhG e sull'articolo 1330 dell'ABGB, ritenendo, segnatamente, che il commento pubblicato contenesse dichiarazioni eccessivamente lesive dell'onore della ricorrente e lasciasse intendere che quest'ultima avrebbe tenuto un comportamento penalmente rilevante, senza che a tal proposito fosse fornita alcuna prova. Inoltre, secondo tali giudici, in materia di dichiarazioni formulate nei confronti di un politico, in assenza di un nesso con un dibattito politico o di interesse generale, qualsiasi riferimento al diritto alla libertà di espressione sarebbe parimenti inammissibile.

19. Le due parti nel procedimento principale hanno presentato ricorsi dinanzi all'Oberster Gerichtshof (Corte suprema, Austria), il quale ha ritenuto che le affermazioni in questione avessero lo scopo di offendere la ricorrente nel suo onore, di ingiuriarla e di diffamarla.

20. Il giudice del rinvio è chiamato a statuire sulla questione se il provvedimento inibitorio, emesso nei confronti di un host provider che gestisce un social network con un elevato numero di utenti, possa essere esteso anche, a livello mondiale, alle dichiarazioni testualmente identiche e/o dal contenuto equivalente di cui non sia al corrente.

21. A tal riguardo, l'Oberster Gerichtshof (Corte suprema) indica che, secondo la propria giurisprudenza, un obbligo del genere deve essere considerato proporzionato laddove il prestatore sia già venuto a conoscenza di almeno una violazione degli interessi della persona di cui trattasi causata da un contributo di un destinatario del servizio e il rischio che vengano commesse altre violazioni si sia pertanto concretizzato.

IV. Questioni pregiudiziali e procedimento dinanzi alla Corte

22. È in tali circostanze che l'Oberster Gerichtshof (Corte suprema), con decisione del 25 ottobre 2017, pervenuta alla Corte il 10 gennaio 2018, ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se l'articolo 15, paragrafo 1, della direttiva [2000/31] osti in generale a uno degli obblighi sotto descritti imposti a un host provider, che non abbia rimosso tempestivamente informazioni illecite, in particolare all'obbligo di eliminare, non soltanto le suddette informazioni illecite ai sensi dell'articolo 14, paragrafo 1, lettera a), della [suddetta] direttiva, ma anche altre informazioni identiche:

   a) a livello mondiale;

   b) nello Stato membro interessato;

   c) dell'utente interessato a livello mondiale;

   d) dell'utente interessato nello Stato membro interessato.

2) In caso di risposta negativa alla prima questione: se ciò valga rispettivamente anche per informazioni dal contenuto equivalente.

3) Se ciò valga anche per informazioni dal contenuto equivalente, non appena il gestore sia venuto a conoscenza di tale circostanza»

23. Osservazioni scritte sono state depositate dalla ricorrente, dalla Facebook Ireland, dai governi austriaco, lettone, portoghese e finlandese, nonché dalla Commissione europea. Le stesse parti interessate, fatta eccezione per il governo portoghese, sono state rappresentate all'udienza tenutasi il 13 febbraio 2019.

V. Analisi

A. Sulla prima e sulla seconda questione pregiudiziale

24. Con le questioni prima e seconda, le quali devono essere esaminate congiuntamente, il giudice del rinvio chiede alla Corte di determinare la portata sostanziale e personale di un obbligo di sorveglianza che può essere imposto, nell'ambito di un'ingiunzione, al prestatore di un servizio della società dell'informazione consistente nel memorizzare le informazioni fornite da un destinatario di tale servizio (un host provider), senza che ciò porti ad imporre un obbligo generale in materia di sorveglianza, vietato dall'articolo 15, paragrafo 1, della direttiva 2000/31.

25. È vero che queste due prime questioni vertono sulla rimozione delle informazioni diffuse tramite una piattaforma di rete sociale in linea piuttosto che sulla sorveglianza o sul filtraggio delle medesime. Occorre tuttavia osservare che le piattaforme di rete sociale costituiscono dei mezzi di comunicazione, il cui contenuto è generato principalmente non dalle società che le hanno fondate e le gestiscono, bensì dai loro utenti. Inoltre, tale contenuto, nel frattempo riprodotto e modificato, è oggetto di scambi costanti fra gli utenti.

26. Un host provider, per poter cancellare un'informazione diffusa tramite una siffatta piattaforma o per disabilitarne l'accesso, chiunque sia l'autore di siffatta informazione e qualunque sia il suo contenuto, deve, in via preliminare, individuare tale informazione fra quelle memorizzate sui suoi server. Per farlo, esso deve, in un modo o in un altro, sorvegliare o filtrare tali informazioni. Orbene, secondo l'articolo 15, paragrafo 1, della direttiva 2000/31, preso in considerazione nelle questioni pregiudiziali, uno Stato membro non può imporre ad un host provider un obbligo generale in materia di sorveglianza. Tutto ciò comporta che, con le sue due prime questioni, il giudice del rinvio si interroga, in sostanza, sulla portata personale e sulla portata sostanziale di un siffatto obbligo conformi ai requisiti fissati dalla direttiva 2000/31.

27. Con la sua prima questione, il giudice del rinvio chiede parimenti alla Corte di specificare se un host provider possa essere costretto a rimuovere, a livello mondiale, informazioni diffuse tramite una piattaforma di rete sociale.

28. Al fine di rispondere a queste due questioni, esaminerò in primo luogo, da un lato, il regime della direttiva 2000/31 applicabile alla Facebook Ireland in quanto host provider e, dall'altro, le implicazioni della sua qualifica di host provider per quanto riguarda le ingiunzioni rivolte a tale prestatore. In secondo luogo, procederò ad analizzare i requisiti fissati dal diritto dell'Unione in relazione alla portata sostanziale e personale di un obbligo in materia di sorveglianza che può essere imposto ad un host provider nell'ambito di un'ingiunzione, senza che ciò sfoci nell'imposizione di un obbligo generale in tale materia. Infine, in terzo luogo, esaminerò la questione della portata territoriale di un obbligo di rimozione.

1. Le ingiunzioni rivolte agli host provider alla luce della direttiva 2000/31

29. Occorre ricordare che, affinché la memorizzazione effettuata dal prestatore di un servizio della società dell'informazione rientri nella previsione dell'articolo 14 della direttiva 2000/31, il comportamento di tale prestatore deve limitarsi a quello di un «prestatore intermediario» nel senso voluto dal legislatore nell'ambito della sezione 4 di tale direttiva. Inoltre, secondo il considerando 42 di detta direttiva, il suo comportamento è meramente tecnico, automatico e passivo, il che comporta una mancanza di conoscenza o di controllo dei dati che esso memorizza e che il ruolo svolto dal medesimo sia neutro [3].

3 V., segnatamente, sentenza del 23 marzo 2010, Google France e Google (da C-236/08 a C-238/08, EU:C:2010:159, punti 112 e 113).

30. La Corte ha già avuto l'occasione di chiarire che il gestore di una piattaforma di rete sociale che memorizza sui propri server informazioni fornite dagli utenti di tale piattaforma, relative al loro profilo, è un prestatore di servizi di hosting ai sensi dell'articolo 14 della direttiva 2000/31 [4]. Indipendentemente dai dubbi che si potrebbero nutrire a tal riguardo, si evince dalla domanda di pronuncia pregiudiziale che, per il giudice del rinvio, è pacifico che la Facebook Ireland sia un host provider, il cui comportamento si limita a quello di un prestatore intermediario.

31. Nella vigenza della direttiva 2000/31, un host provider, il cui comportamento si limiti a quello di un prestatore intermediario gode di un'immunità relativa in materia di responsabilità per le informazioni che memorizza. Infatti, tale immunità è concessa unicamente se siffatto host provider non era al corrente dell'illiceità delle informazioni memorizzate o dell'attività svolta con tali informazioni e a condizione che, non appena al corrente di tale illiceità, esso agisca immediatamente per rimuovere le informazioni in questione o per disabilitarne l'accesso. Per contro, se tale host provider non soddisfa tali condizioni, ossia se era al corrente dell'illiceità delle informazioni memorizzate ma non ha agito al fine di rimuoverle o di disabilitarne l'accesso, la direttiva 2000/31 non osta a che esso possa essere ritenuto indirettamente responsabile di tali informazioni [5].

32. Inoltre, risulta dall'articolo 14, paragrafo 3, della direttiva 2000/31 che l'immunità accordata ad un prestatore intermediario non osta a che un organo giurisdizionale o un'autorità amministrativa, in conformità agli ordinamenti giuridici degli Stati membri, esiga che tale prestatore ponga fine ad una violazione o la impedisca. Discende da tale disposizione che un prestatore intermediario può essere il destinatario di ingiunzioni, anche se, secondo le condizioni enunciate all'articolo 14, paragrafo 1, di tale direttiva, detto prestatore non è esso stesso responsabile delle informazioni memorizzate sui suoi server [6].

33. Le condizioni e le modalità delle suddette ingiunzioni concernenti prestatori intermediari rientrano nell'ambito di applicazione del diritto nazionale [7]. Le norme sancite dagli Stati membri devono tuttavia rispettare i requisiti fissati dal diritto dell'Unione, segnatamente dalla direttiva 2000/31.

34. Tutto ciò riflette la volontà del legislatore dell'Unione di ponderare, tramite siffatta direttiva, i diversi interessi degli host provider, il cui comportamento si limita a quello di un prestatore intermediario, degli utenti dei loro servizi, nonché delle persone lese da qualsiasi violazione commessa nel corso dell'utilizzazione di tali servizi. Di conseguenza, incombe agli Stati membri, in sede di attuazione delle misure di recepimento della direttiva 2000/31, non solo rispettare i requisiti posti da tale direttiva, ma anche provvedere a non fondarsi su un'interpretazione che entri in conflitto con i diritti fondamentali coinvolti o con gli altri principi generali del diritto dell'Unione, come il principio di proporzionalità [8].

4 V. sentenza del 16 febbraio 2012, SABAM (C-360/10, EU:C:2012:85, punto 27).

5 V. articolo 14 della direttiva 2000/31. V., parimenti, le mie conclusioni nella causa Stichting Brein (C-610/15, EU:C:2017:99, paragrafi 67 e 68).

6 V. sentenza del 7 agosto 2018, SNB-REACT (C-521/17, EU:C:2018:639, punto 51). V. parimenti, in tal senso, 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, pag. 5.

7 V. le mie conclusioni nella causa Mc Fadden (C-484/14, EU:C:2016:170). V., parimenti, Husovec, M., *Injunctions Against Intermediaires in the European Union*. Accountable But Not *Liable*?, Cambridge University Press, Cambridge, 2017, pag. 57 e 58.

8 V., in tal senso, per quanto attiene al rispetto dei diritti fondamentali e del principio di proporzionalità, sentenza del 29 gennaio 2008, Promusicae (C-275/06, EU:C:2008:54, punto 68).

2. Requisiti relativi alla portata personale e sostanziale di un obbligo in materia di sorveglianza

a) Divieto di un obbligo generale in materia di sorveglianza

35. Occorre osservare che l'articolo 15, paragrafo 1, della direttiva 2000/31 vieta agli Stati membri di imporre, segnatamente ai prestatori di servizi la cui attività consiste nel memorizzare informazioni, un obbligo generale di sorveglianza sulle informazioni che memorizzano o un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. Inoltre, si evince dalla giurisprudenza che tale disposizione osta, segnatamente, a che un host provider, il cui comportamento si limiti a quello di un prestatore intermediario sia costretto a procedere ad una sorveglianza della totalità [9] o della quasi totalità [10] dei dati di tutti gli utenti del suo servizio al fine di prevenire qualsiasi violazione futura.

36. Se, contrariamente a quanto previsto da tale disposizione, uno Stato membro potesse imporre, nell'ambito di un'ingiunzione, un obbligo generale in materia di sorveglianza ad un host provider, non è escluso che quest'ultimo rischierebbe di perdere la qualità di prestatore intermediario, nonché l'immunità ad essa correlata. Infatti, il ruolo di un host provider che eserciti una sorveglianza generale non sarebbe più neutro. L'attività di tale host provider non conserverebbe il suo carattere tecnico, automatico e passivo, il che implicherebbe che detto host provider sarebbe al corrente delle informazioni memorizzate ed eserciterebbe un controllo sulle medesime.

37. Inoltre, anche qualora tale rischio non esistesse, un host provider che esercita una sorveglianza generale potrebbe, in linea di principio, essere ritenuto responsabile di qualsiasi attività o informazione illecita, senza che le condizioni enunciate all'articolo 14, paragrafo 1, lettere a) e b), di tale direttiva siano effettivamente soddisfatte.

38. È vero che l'articolo 14, paragrafo 1, lettera a), della direttiva 2000/31 subordina la responsabilità di un prestatore intermediario alla conoscenza effettiva dell'attività o dell'informazione illecita. Tuttavia, alla luce di un obbligo generale in materia di sorveglianza, si potrebbe ritenere che il carattere illecito di qualsiasi attività o informazione venga portato d'ufficio a conoscenza di tale prestatore intermediario e che quest'ultimo dovrebbe procedere alla rimozione di tali informazioni o disabilitare l'accesso alle medesime, senza che esso abbia compreso il contenuto illecito [11]. Di conseguenza, la logica dell'immunità relativa in materia di responsabilità per le informazioni memorizzate da un prestatore intermediario sarebbe sistematicamente sovvertita, il che arrecherebbe pregiudizio all'effetto utile dell'articolo 14, paragrafo 1, della direttiva 2000/31.

39. Per riassumere, il ruolo di un host provider che esercita una siffatta sorveglianza generale non sarebbe più neutro, dato che l'attività di tale host provider non conserverebbe il suo carattere tecnico, automatico e passivo, il che implicherebbe che detto host provider sia al corrente delle informazioni memorizzate ed eserciti un controllo sulle medesime. Di conseguenza, l'attuazione di un obbligo generale in materia di sorveglianza, imposto ad un host provider nell'ambito di un'ingiunzione autorizzata, a priori, in forza dell'articolo 14, paragrafo 3, della direttiva 2000/31, potrebbe rendere l'articolo 14 di tale direttiva inapplicabile nei confronti di siffatto host provider.

9 V. sentenze del 12 luglio 2011, L'Oréal e a. (C-324/09, EU:C:2011:474, punti 139 e 144), nonché del 24 novembre 2011, Scarlet Extended (C-70/10, EU:C:2011:771, punti 36 e 40).

10 V. sentenza del 16 febbraio 2012, SABAM (C-360/10, EU:C:2012:85, punti 37 e 38).

11 V., in tal senso, conclusioni dell'avvocato generale Jääskinen nella causa L'Oréal e a. (C-324/09, EU:C:2010:757, paragrafo 143).

40. Desumo pertanto dal combinato disposto dell'articolo 14, paragrafo 3, e dell'articolo 15, paragrafo 1, della direttiva 2000/31 che un obbligo imposto ad un prestatore intermediario nell'ambito di un'ingiunzione non può avere come conseguenza che, rispetto alla totalità o alla quasi totalità delle informazioni memorizzate, il ruolo di tale prestatore intermediario non sia più neutro nel senso descritto al paragrafo precedente.

b) Obbligo di sorveglianza in casi specifici

41. Come enunciato dal considerando 47 della direttiva 2000/31, il divieto di imporre obblighi generali, previsto all'articolo 15, paragrafo 1, di tale direttiva, non riguarda gli obblighi di sorveglianza *in casi specifici*. Infatti, dal testo dell'articolo 14, paragrafo 3, della direttiva 2000/31 risulta che un host provider può essere costretto *a prevenire* una violazione, il che implica logicamente, come fatto valere dalla Commissione, una certa forma di sorveglianza nel futuro, senza che siffatta sorveglianza si trasformi in un obbligo di sorveglianza generale [12]. L'articolo 18 di tale direttiva esige inoltre dagli Stati membri che essi provvedano affinché i ricorsi giurisdizionali previsti dal diritto nazionale per quanto concerne le attività dei servizi della società dell'informazione consentano di prendere rapidamente provvedimenti atti, segnatamente, *a impedire ulteriori danni* agli interessi in causa.

42. Inoltre, si evince dalla sentenza L'Oréal e a. [13] che un host provider può essere obbligato ad adottare provvedimenti che contribuiscano ad evitare che abbiano luogo *nuove violazioni* della stessa natura da parte dello stesso destinatario.

43. In tale sentenza, la Corte ha interpretato non solo le disposizioni della direttiva 2000/31, ma anche quelle della direttiva 2004/48/CE [14]. Orbene, nel farlo, la Corte ha definito un obbligo in materia di sorveglianza conforme ai requisiti sanciti da tali direttive in opposizione all'obbligo vietato all'articolo 15, paragrafo 1, della direttiva 2000/31, ossia quello di *sorveglianza attiva della totalità – quasi totalità* dei dati al fine di prevenire qualsiasi futura violazione [15]. Indipendentemente dal contesto specifico della sentenza L'Oréal e a. [16] e dai riferimenti alla direttiva 2004/48, le considerazioni di tale sentenza relative agli obblighi degli host provider conformi al diritto dell'Unione, in funzione del loro carattere generale o meno, hanno natura trasversale e, pertanto, sono trasponibili, a mio avviso, al caso di specie.

44. Di conseguenza, al fine di prevenire qualsiasi futura violazione, un host provider può essere costretto, nell'ambito di un'ingiunzione, a rimuovere informazioni illecite che non sono ancora state diffuse al momento dell'adozione di siffatta ingiunzione, senza che la diffusione di tali informazioni venga portata a sua conoscenza di nuovo e in maniera separata rispetto alla domanda iniziale di rimozione.

45. Tuttavia, per non sfociare nell'imposizione di un obbligo generale, un obbligo di sorveglianza deve essere conforme, come sembra discendere dalla sentenza L'Oréal e a. [17], a requisiti supplementari, ossia avere ad oggetto violazioni della *stessa natura* da parte dello *stesso destinatario nei confronti degli stessi diritti*, nella specie quello dei marchi.

46. Pertanto, ne deduco che la sorveglianza attiva non è inconciliabile con la direttiva 2000/31, diversamente dalla sorveglianza attiva il cui oggetto non è incentrato sul caso specifico di una violazione.

12 V. parimenti, in tal senso, Rosati, E., *Copyright and the Court of Justice of the European Union*, Oxford University Press, Oxford, 2019, pag. 158.

13 Sentenza del 12 luglio 2011 (C-324/09, EU:C:2011:474, punto 144).

14 Direttiva del Parlamento europeo e del Consiglio del 29 aprile 2004 sul rispetto dei diritti di proprietà intellettuale (GU 2004, L 157, pag. 45).

15 Sentenza del 12 luglio 2011, L'Oréal e a. (C-324/09, EU:C:2011:474, punti 139 e 144).

16 Sentenza del 12 luglio 2011 (C-324/09, EU:C:2011:474).

17 Sentenza del 12 luglio 2011, L'Oréal e a. (C-324/09, EU:C:2011:474, punti 141 e 144).

47. In tale ordine di idee, ho indicato nelle mie conclusioni nella causa Mc Fadden [18], relativa ad un fornitore di accesso ad una rete di comunicazione ai sensi dell'articolo 12 della direttiva 2000/31, ispirandomi ai lavori preparatori della direttiva 2000/31, che, affinché un obbligo possa essere considerato applicabile *in casi specifici*, esso dev'essere segnatamente delimitato per quanto concerne *l'oggetto* e *la durata* della sorveglianza.

48. Tali requisiti generali formulati in maniera astratta mi sembrano trasponibili a circostanze come quelle di cui al procedimento principale, sebbene, all'atto dell'applicazione per analogia agli host provider come la Facebook Ireland di considerazioni in materia di obbligo di sorveglianza relative ai fornitori di accesso ad una rete di comunicazione come Internet, i ruoli svolti da tali prestatori intermediari siano diversi. Ad esempio, se si prende in considerazione un host provider come la Facebook Ireland, i contenuti della sua piattaforma sembrano costituire la totalità dei dati memorizzati, mentre per un fornitore di accesso ad Internet tali contenuti rappresentano soltanto una parte infinitesimale dei dati trasmessi. Per contro, il carattere e l'intensità del coinvolgimento di un siffatto host provider nel trattamento dei contenuti digitali differiscono sensibilmente da quelli di un fornitore di accesso ad Internet. Come osservato dalla Commissione, un host provider si trova in condizioni migliori per adottare misure al fine di ricercare ed eliminare informazioni illecite rispetto ad un fornitore d'accesso.

49. Inoltre, il requisito relativo alla limitazione temporale di un obbligo in materia di sorveglianza riflette diverse sentenze della Corte [19]. Anche se emerge dalla giurisprudenza che la limitazione temporale di un obbligo posto nell'ambito di un'ingiunzione si riferisce piuttosto alla problematica dei principi generali del diritto dell'Unione [20], ritengo che un obbligo di sorveglianza permanente sarebbe difficilmente conciliabile con il concetto di un obbligo applicabile in casi specifici ai sensi del considerando 47 della direttiva 2000/31.

50. Di conseguenza, il carattere mirato di un obbligo in materia di sorveglianza dovrebbe essere previsto prendendo in considerazione la durata di tale sorveglianza, nonché le precisazioni relative alla natura delle violazioni considerate, al loro autore e al loro oggetto. Tutti siffatti elementi sono interdipendenti e connessi gli uni agli altri. Essi devono essere pertanto valutati in maniera globale al fine di rispondere alla questione se un'ingiunzione rispetti o meno il divieto previsto all'articolo 15, paragrafo 1, della direttiva 2000/31.

c) Conclusioni intermedie

51. Per ricapitolare questa parte della mia analisi, in primo luogo, si evince dal combinato disposto dell'articolo 14, paragrafo 3, e dell'articolo 15, paragrafo 1, della direttiva 2000/31 che un obbligo imposto ad un prestatore intermediario nell'ambito di un'ingiunzione non può sfociare in una situazione in cui, rispetto alla totalità o alla quasi totalità delle informazioni memorizzate, il ruolo di tale prestatore intermediario non sia più tecnico, automatico e passivo, il che implicherebbe che l'host provider di cui trattasi sia al corrente di tali informazioni ed eserciti un controllo sulle medesime [21].

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

19 Più specificamente, la Corte ha indicato, nella sentenza del 12 luglio 2011, L'Oréal e a. (C-324/09, EU:C:2011:474, punto 140), che il provvedimento ingiuntivo inteso a prevenire eventuali pregiudizi arrecati a marchi nell'ambito del servizio della società dell'informazione, ossia un mercato online, non può avere l'oggetto o l'effetto di imporre un divieto generale e *permanente* di messa in vendita di prodotti contrassegnati da detti marchi. Nella stessa ottica, la Corte ha rilevato, nella sentenza del 16 febbraio 2012, SABAM (C-360/10, EU:C:2012:85, punto 45), che il diritto dell'Unione osta segnatamente a che un obbligo di sorveglianza, sancito nell'ambito di un'ingiunzione rivolta ad un prestatore, sia *illimitato nel tempo*.

20 Tale approccio è quello adottato dall'avvocato generale Jääskinen nelle sue conclusioni nella causa L'Oréal e a. (C-324/09, EU:C:2010:757, paragrafo 181); queste ultime, a mio avviso, hanno fortemente ispirato la formulazione dei passaggi in questione della sentenza emessa dalla Corte in tale causa.

21 V. paragrafo 39 delle presenti conclusioni.

52. In secondo luogo, la sorveglianza attiva non è inconciliabile con la direttiva 2000/31, contrariamente alla sorveglianza attiva il cui oggetto non è incentrato sul caso specifico di una violazione [22].

53. In terzo luogo, il carattere mirato di un obbligo in materia di sorveglianza dovrebbe essere previsto prendendo in considerazione la durata di tale sorveglianza, nonché le precisazioni relative alla natura delle violazioni considerate, al loro autore e al loro oggetto [23].

54. È alla luce di tali considerazioni che occorre esaminare la portata personale e la portata sostanziale di un obbligo in materia di sorveglianza di un prestatore che gestisce una piattaforma di rete sociale. Esse si riassumono, nella specie, nella ricerca e nell'individuazione, fra i contenuti memorizzati, di informazioni identiche a quella qualificata come illecita dal giudice adito, nonché nella ricerca di informazioni ad essa equivalenti.

d) Applicazione nel caso di specie

1) Le informazioni identiche a quella qualificata come illecita

55. Ad eccezione della Facebook Ireland, tutti gli interessati sostengono che debba essere possibile ordinare ad un host provider di sopprimere o bloccare l'accesso alle dichiarazioni identiche a quella qualificata come illecita pubblicate dallo stesso utente. La ricorrente, i governi austriaco e lettone, nonché la Commissione ritengono, in sostanza, che lo stesso valga per quanto riguarda quelle pubblicate da altri utenti.

56. Dalla domanda di pronuncia pregiudiziale emerge che il giudice di secondo grado ha ritenuto che il riferimento alle «informazioni identiche» riguardasse le pubblicazioni di fotografie raffiguranti la ricorrente *accompagnate dallo stesso testo*. In tale ordine di idee, il giudice del rinvio spiega che i suoi dubbi vertono segnatamente sulla questione se l'ingiunzione emessa nei confronti della Facebook Ireland possa essere estesa alle *dichiarazioni (messaggi di accompagnamento) testualmente identiche* e a quelle dal contenuto equivalente. Intendo pertanto tale riferimento alle «informazioni identiche» nel senso che il giudice del rinvio prende in considerazione le riproduzioni manuali ed esatte dell'informazione da esso qualificata come illecita e, come indicato dal governo austriaco, le riproduzioni automatizzate, effettuate grazie alla funzione di «condivisione».

57. A tal riguardo, ritengo che un host provider che gestisce una piattaforma di rete sociale possa essere costretto, al fine di eseguire un'ingiunzione emessa da un giudice di uno Stato membro, a ricercare e ad individuare tutte le informazioni identiche a quella qualificata come illecita da tale giudice.

58. Infatti, come si evince dalla mia analisi, un host provider può essere costretto a prevenire qualsiasi nuova violazione dello stesso tipo e dello stesso destinatario di un servizio della società dell'informazione [24]. In un caso del genere, siamo effettivamente in presenza di un caso specifico di una violazione individuata in maniera concreta, cosicché l'obbligo di individuare, fra le informazioni provenienti da un unico utente, quelle identiche a quella qualificata come illecita, non costituisce un obbligo generale in materia di sorveglianza.

22 V. paragrafo 46 delle presenti conclusioni.

23 V. paragrafo 50 delle presenti conclusioni.

24 V. paragrafi 42 e 45 delle presenti conclusioni.

59. A mio avviso, lo stesso vale per quanto attiene alle informazioni identiche a quella qualificata come illecita diffuse da altri utenti. Sono consapevole del fatto che tale ragionamento comporta l'inclusione nella portata personale di un obbligo in materia di sorveglianza di tutti gli utenti e, pertanto, della totalità delle informazioni diffuse tramite una piattaforma.

60. Cionondimeno, un obbligo di ricercare e di individuare informazioni identiche a quella qualificata come illecita dal giudice adito riguarda sempre il caso specifico di una violazione. Inoltre, si tratta, nella specie, di un obbligo imposto nell'ambito di un'ordinanza cautelare, il quale esplica i propri effetti fino alla definizione del procedimento. Pertanto, un siffatto obbligo imposto ad un host provider è, per sua natura, limitato nel tempo.

61. Inoltre, la riproduzione dello stesso contenuto da parte di tutti gli utenti di una piattaforma di rete sociale mi sembra rilevabile, di norma, con l'ausilio di strumenti informatici, senza che l'host provider sia obbligato a ricorrere ad un filtraggio attivo e non automatico della totalità delle informazioni diffuse tramite la sua piattaforma.

62. Inoltre, imporre l'obbligo di ricercare e di individuare tutte le informazioni identiche a quella qualificata come illecita consente di assicurare un giusto equilibrio fra i diritti fondamentali coinvolti.

63. Anzitutto, la ricerca e l'individuazione delle informazioni identiche a quella qualificata come illecita da parte di un giudice adito non esigono strumenti tecnici sofisticati, idonei a rappresentare un onere straordinario. Pertanto, un siffatto obbligo non risulta eccessivamente lesivo del diritto alla libertà d'impresa di cui beneficia un host provider che gestisce una piattaforma di rete sociale come la Facebook Ireland ai sensi dell'articolo 16 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»).

64. Alla luce, poi, della facilità di riproduzione delle informazioni nell'ambiente di Internet, la ricerca e l'individuazione delle informazioni identiche a quella qualificata come illecita risulta necessaria per assicurare la protezione efficace della vita privata e dei diritti della personalità.

65. Infine, un siffatto obbligo rispetta il diritto fondamentale degli utenti di Internet alla libertà di espressione e di informazione, garantito all'articolo 11 della Carta, nella misura in cui la tutela di tale libertà non deve essere necessariamente garantita in modo assoluto, ma deve essere ponderata con altri diritti fondamentali. Per quanto riguarda le informazioni identiche a quella qualificata come illecita, esse costituiscono, a priori e di norma, ripetizioni di una violazione qualificata concretamente come illecita. Tali ripetizioni dovrebbero essere oggetto di una qualificazione identica; quest'ultima può tuttavia essere attenuata in funzione, segnatamente, del contesto di una dichiarazione asseritamente illecita. Per inciso, occorre rilevare che i terzi che possono subire indirettamente un pregiudizio a causa di ingiunzioni sono estranei ai procedimenti, nell'ambito dei quali tali ingiunzioni vengono emesse. È segnatamente per questo motivo che deve essere garantita la possibilità, per tali terzi, di contestare dinanzi ad un giudice le misure di esecuzione adottate da un host provider sulla base di un'ingiunzione [25], non dovendo tale possibilità essere condizionata dal fatto di essere qualificati come parte in un procedimento principale [26].

25 V., per analogia, sentenza del 27 marzo 2014, UPC Telekabel Wien (C-314/12, EU:C:2014:192, punto 57).

26 V., per analogia, sentenze del 25 maggio 2016, Meroni (C-559/14, EU:C:2016:349, punti 49 e 50), e del 21 dicembre 2016, Biuro podróży «Partner» (C-119/15, EU:C:2016:987, punto 40). Sulla problematica del principio della tutela giurisdizionale effettiva nei confronti dei terzi, v. parimenti 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, pag. 222 e 223.

2) Le informazioni equivalenti

66. Per quanto riguarda la portata sostanziale di un obbligo in materia di sorveglianza, la ricorrente sostiene che un host provider può essere assoggettato all'obbligo di rimuovere le dichiarazioni di contenuto equivalente a quella qualificata come illecita pubblicate dallo stesso utente. Per contro, il governo austriaco e la Commissione ritengono che la possibilità di imporre un siffatto obbligo dipenda dal risultato della ponderazione degli interessi in gioco. Solo la ricorrente è dell'avviso che sia possibile intimare ad un host provider la rimozione di dichiarazioni dal contenuto equivalente a quella qualificata come illecita pubblicate da altri utenti.

67. Il riferimento alle «informazioni equivalenti» o a quelle «dal contenuto equivalente» dà luogo a difficoltà di interpretazione nei limiti in cui il giudice del rinvio non specifica il significato di tali espressioni. È tuttavia possibile desumere dalla domanda di pronuncia pregiudiziale che il riferimento alle informazioni «dal contenuto equivalente» riguarda le informazioni che *divergono a malapena* dall'informazione iniziale o le situazioni in cui *il messaggio resta, in sostanza, immutato*. Intendo tali indicazioni nel senso che una riproduzione dell'informazione qualificata come illecita, la quale contenga un errore di battitura, nonché quella che presenti una sintassi o una punteggiatura diverse, costituisce un'«informazione equivalente». Non è tuttavia evidente che l'equivalenza di cui alla seconda questione non ecceda tali casi.

68. È vero che si evince dalla sentenza L'Oréal e a.[27] che il prestatore di un servizio della società dell'informazione può essere costretto ad adottare provvedimenti che contribuiscono a prevenire *nuove violazioni* della *stessa natura* nei confronti degli stessi diritti.

69. Non deve tuttavia essere perso di vista il contesto fattuale nel quale è stata elaborata la giurisprudenza rilevante, ossia quello delle violazioni del diritto di proprietà intellettuale. Di norma, siffatte violazioni consistono nella diffusione dello stesso contenuto di quello tutelato o, quantomeno, di un contenuto simile a quello tutelato, mentre che le eventuali modifiche del medesimo, talvolta difficili da apportare, esigono un intervento specifico.

70. Per contro, è insolito che un atto diffamatorio riprenda i termini esatti di uno atto della stessa natura. Ciò è dovuto, in parte, al carattere personalizzato del modo di esprimere le idee. Inoltre, contrariamente alle violazioni del diritto di proprietà intellettuale, gli atti diffamatori successivi all'atto diffamatorio iniziale riproducono il fatto di effettuare dichiarazioni lesive dell'onore di una persona piuttosto che la forma dell'atto iniziale. Per questo motivo, in materia di diffamazione, il mero riferimento ad atti della stessa natura non potrebbe svolgere lo stesso ruolo che in materia di violazione del diritto di proprietà intellettuale.

71. In ogni caso, l'interpretazione data al riferimento alle «informazioni equivalenti» è idoneo ad incidere sulla portata di un obbligo in materia di sorveglianza e sull'esercizio dei diritti fondamentali coinvolti. Un giudice che, nell'ambito di un'ingiunzione, statuisca sulla rimozione delle «informazioni equivalenti» deve pertanto rispettare il principio della certezza del diritto e garantire che gli effetti di tale ingiunzione siano chiari, precisi e prevedibili. Nel farlo, tale giudice deve ponderare i diritti fondamentali coinvolti e tenere conto del principio di proporzionalità.

72. Fatte salve tali considerazioni, ispirandomi nuovamente alla sentenza L'Oréal e a.[28], ritengo che, a fortiori, un host provider possa essere costretto ad individuare informazioni equivalenti a quella qualificata come illecita provenienti dallo stesso utente. Anche in questo caso, a tale utente, dovrebbe essere garantita la possibilità di contestare, dinanzi ad un giudice, le misure di esecuzione adottate da un host provider nel corso dell'esecuzione di un'ingiunzione.

27 Sentenza del 12 luglio 2011 (C-324/09, EU:C:2011:474).

28 Sentenza del 12 luglio 2011 (C-324/09, EU:C:2011:474).

73. Per contro, l'individuazione di informazioni equivalenti a quella qualificata come illecita provenienti da altri utenti richiederebbe la sorveglianza della totalità delle informazioni diffuse attraverso una piattaforma di rete sociale. Orbene, a differenza delle informazioni identiche a quella qualificata come illecita, le informazioni equivalenti a quest'ultima non possono essere individuate senza che un host provider ricorra a soluzioni sofisticate. Di conseguenza, non soltanto il ruolo di un prestatore che esercita una sorveglianza generale non sarebbe più neutro, nel senso che non sarebbe soltanto tecnico, automatico e passivo, ma tale prestatore, esercitando una forma di censura, diverrebbe un contributore attivo di tale piattaforma.

74. Inoltre, un obbligo di individuare informazioni equivalenti a quella qualificata come illecita provenienti da qualsiasi utente non assicurerebbe un giusto equilibrio fra la protezione della vita privata e dei diritti della personalità, quella della libertà d'impresa, nonché quella della libertà di espressione e di informazione. Da un lato, la ricerca e l'individuazione di siffatte informazioni richiederebbero soluzioni costose, le quali dovrebbero essere elaborate e introdotte da un host provider. Dall'altro, l'attuazione di siffatte soluzioni darebbe luogo ad una censura, con la conseguenza che la libertà di espressione e di informazione potrebbe essere sistematicamente limitata.

75. Alla luce delle considerazioni che precedono, propongo di rispondere alla prima e alla seconda questione, nei limiti in cui vertono sulla portata personale e sostanziale di un obbligo di sorveglianza, che l'articolo 15, paragrafo 1, della direttiva 2000/31 deve essere interpretato nel senso che esso non osta a che un host provider che gestisce una piattaforma di rete sociale sia costretto, nell'ambito di un'ingiunzione, a ricercare e ad individuare, fra tutte le informazioni diffuse dagli utenti di tale piattaforma, le informazioni identiche a quella qualificata come illecita dal giudice che ha emesso tale ingiunzione. Nell'ambito di una siffatta ingiunzione, un host provider può essere costretto a ricercare e ad individuare le informazioni equivalenti a quella qualificata come illecita soltanto fra informazioni diffuse dall'utente che ha divulgato tale informazione. Un giudice che statuisce sulla rimozione di siffatte informazioni equivalenti deve garantire che gli effetti della sua ingiunzione siano chiari, precisi e prevedibili. Nel farlo, esso deve ponderare i diritti fondamentali coinvolti e tenere conto del principio di proporzionalità.

3. Sulla rimozione a livello mondiale

a) Osservazioni preliminari

76. Esaminerò adesso i dubbi del giudice del rinvio concernenti la portata territoriale di un obbligo di rimozione. Essi riguardano, in sostanza, la questione se un host provider possa essere costretto a rimuovere contenuti che sono stati qualificati come illeciti in forza del diritto nazionale di uno Stato membro, non solo a livello di tale Stato membro, bensì anche a livello mondiale.

77. In via preliminare, è vero che la Facebook Ireland gestisce, quale controllata della Facebook, una piattaforma elettronica soltanto per gli utenti situati al di fuori degli Stati Uniti e del Canada. Tuttavia, tale circostanza non sembra essere idonea ad escludere la rimozione a livello mondiale delle informazioni diffuse tramite tale piattaforma. Infatti, la Facebook Ireland non contesta il fatto di essere in grado di assicurare una siffatta rimozione a livello mondiale.

78. Occorre tuttavia osservare che il legislatore dell'Unione non ha armonizzato le norme sostanziali in materia di pregiudizio alla vita privata e ai diritti della personalità, inclusa la diffamazione [29]. Inoltre, in assenza di consenso a livello dell'Unione [30], il legislatore dell'Unione non ha neanche armonizzato le norme di conflitto in materia [31]. Pertanto, al fine di conoscere delle azioni per diffamazione, ciascun giudice dell'Unione ricorre alla legge designata come applicabile in forza delle norme nazionali di conflitto.

79. La situazione di cui al procedimento principale è diversa, a priori, da quella che costituiva il punto di partenza della mia analisi relativa alla portata territoriale di una cancellazione dei risultati di un motore di ricerca nella causa Google (Portata territoriale della cancellazione) [32], menzionata dalla Facebook Ireland e dal governo lettone. Tale causa riguarda la direttiva 95/46/CE [33], la quale armonizza, a livello dell'Unione, talune norme sostanziali relative alla protezione dei dati. È segnatamente il fatto che le norme in tale materia sono armonizzate che mi ha indotto a concludere che un prestatore doveva essere tenuto a cancellare i risultati visualizzati a seguito di una ricerca effettuata non soltanto a partire da un solo Stato membro ma a partire da un luogo all'interno dell'Unione [34]. Tuttavia, nelle mie conclusioni presentate in tale causa, non escludevo che possano sussistere casi in cui l'interesse dell'Unione esige un'applicazione delle disposizioni di tale direttiva al di fuori del territorio dell'Unione [35].

80. Pertanto, per quanto riguarda le violazioni risultanti da atti diffamatori, l'imposizione in uno Stato membro di un obbligo consistente nel rimuovere talune informazioni a livello mondiale, per tutti gli utenti di una piattaforma elettronica, a causa dell'illiceità di tali informazioni accertata in forza di una legge applicabile, avrebbe come conseguenza che l'accertamento del loro carattere illecito esplichi effetti in altri Stati. In altre parole, l'accertamento del carattere illecito delle informazioni in questione si estenderebbe ai territori di questi altri Stati. Tuttavia, non è escluso che, secondo le leggi designate come applicabili in forza delle norme nazionali di conflitto di tali Stati, tale informazione potrebbe essere considerata lecita.

81. Come mostra il dibattito fra gli interessati, da un lato, la reticenza a conferire siffatti effetti extraterritoriali alle ingiunzioni riflette la posizione della Facebook Ireland, nonché quella dei governi lettone, portoghese e finlandese. Dall'altro, ad eccezione del governo portoghese, tali interessati sembrano parimenti nutrire dubbi sulla portata territoriale della competenza dei giudici di uno Stato membro. In sostanza, detti interessati sembrano ritenere che il giudice di uno Stato membro non possa statuire, nell'ambito di un'ingiunzione rivolta ad un host provider, sulla rimozione di contenuti al di fuori del territorio di tale Stato membro. Occorre pertanto analizzare queste due questioni, ossia la portata territoriale di un obbligo di rimozione e la portata della competenza dei giudici di uno Stato membro, esaminando anzitutto quella della competenza, la quale è, di norma, preliminare a quella del merito.

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

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

31 V. articolo 1, paragrafo 2, del regolamento (CE) n. 864/2007 del Parlamento europeo e del Consiglio, dell'11 luglio 2007, sulla legge applicabile alle obbligazioni extracontrattuali («Roma II») (GU 2007, L 199, pag. 40).

32 Mi riferisco qui alle mie conclusioni nella causa Google (Portata territoriale della cancellazione) (C-507/17, EU:C:2019:15).

33 Direttiva del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU 1995, L 281, pag. 31).

34 V. le mie conclusioni nella causa Google (Portata territoriale della cancellazione) (C-507/17, EU:C:2019:15, paragrafi 47, 55, 76 e 77).

35 V. le mie conclusioni nella causa Google (Portata territoriale della cancellazione) (C-507/17, EU:C:2019:15, paragrafo 62).

b) Sulla portata territoriale della competenza

82. La direttiva 2000/31 non disciplina la competenza a statuire sulle ingiunzioni. Per contro, come risulta dalla sentenza eDate Advertising e a.[36], in caso di asserita lesione dei diritti della personalità attraverso contenuti messi in rete su un sito Internet, una persona che si ritiene lesa ha la facoltà di adire i giudici degli Stati membri competenti ai sensi del regolamento (UE) n. 1215/2012[37]. Infatti, mentre le norme di conflitto in materia di diffamazione non sono armonizzate a livello dell'Unione, la situazione è diversa per quanto riguarda le norme sulla competenza.

83. A tal riguardo, occorre aggiungere che le norme sulla competenza del regolamento n. 1215/2012 si applicano parimenti alle controversie in materia di rimozione dei contenuti diffamatori messi in rete[38]. Inoltre, poco importa che, nella specie, una siffatta domanda sia diretta non nei confronti di un emittente bensì nei confronti di un host provider dei contenuti messi in rete. Tutto ciò premesso, non proporrò alla Corte di riformulare le questioni pregiudiziali, poiché solo gli interessati nutrono dubbi sulla portata territoriale della competenza. Desidererei cionondimeno formulare talune osservazioni al riguardo.

84. Secondo la sentenza eDate Advertising e a.[39], una persona che si ritiene lesa può adire, segnatamente, i giudici dello Stato membro in cui si trova il proprio centro d'interessi. Tali giudici sono competenti a pronunciarsi sulla totalità del danno cagionato. Mi sembra che, nella specie, il giudice adito dalla ricorrente sia quello del luogo in cui si trova il suo centro d'interessi[40].

85. È vero che, nella sentenza eDate Advertising e a.[41], la Corte ha indicato che una persona che si ritiene lesa poteva adire un foro, a seconda del luogo di concretizzazione del danno cagionato nell'Unione, per la totalità di tale danno. Certamente, ciò può far pensare che la portata territoriale della competenza di tale foro non includa i fatti che si riferiscono ai territori degli Stati terzi. Tuttavia, tale considerazione riflette piuttosto il fatto che un foro, per essere competente ai sensi del regolamento n. 1215/2012, a titolo di luogo in cui si è verificato il danno, deve essere un giudice di uno Stato membro. Inoltre, fatta salva tale considerazione, la Corte ha affermato più volte in siffatta sentenza che tale foro era competente a statuire sui danni derivanti dalla diffamazione nella loro integralità[42].

36 Sentenza del 25 ottobre 2011 (C-509/09 e C-161/10, EU:C:2011:685, punti 43 e 44).

37 Regolamento del Parlamento europeo e del Consiglio, del 12 dicembre 2012, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (GU 2012, L 35, pag. 1).

38 Sentenza del 17 ottobre 2017, Bolagsupplysningen e Ilsjan (C-194/16, EU:C:2017:766, punto 44).

39 Sentenza del 25 ottobre 2011 (C-509/09 e C-161/10, EU:C:2011:685, punto 48).

40 Di conseguenza, sebbene il giudice del rinvio sia chiamato a statuire su un'ordinanza cautelare, non occorre interrogarsi sulle implicazioni dell'articolo 35 del regolamento n. 1215/2012 sulla portata territoriale della competenza e sulla portata territoriale di un obbligo di rimozione imposto nell'ambito di un'ingiunzione.

41 Sentenza del 25 ottobre 2011 (C-509/09 e C-161/10, EU:C:2011:685, punto 48).

42 Sentenza del 25 ottobre 2011, eDate Advertising e a. (C-509/09 e C-161/10, EU:C:2011:685, punti 48, 51 e 52). V., parimenti, sentenza del 17 ottobre 2017, Bolagsupplysningen e Ilsjan (C-194/16, EU:C:2017:766, punti 38 e 47). Inoltre, secondo le interpretazioni dottrinali di tale sentenza, il foro del luogo del centro degli interessi può statuire in tutto il mondo su danni cagionati. V. Mankowski, P., in Magnus, U., e Mankowski, P. (a cura di), Brussels I bis Regulation – Commentary, Otto Schmidt, Colonia, 2016, Art. 7, punto 364. Lo stesso vale per la portata territoriale della competenza generale del foro del convenuto. Nella sentenza del 1º marzo 2005, Owusu (C-281/02, EU:C:2005:120, punto 26), la Corte ha ritenuto che la convenzione di Bruxelles [convenzione del 27 settembre 1968 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (GU 1972, L 299, pag. 32)] sia applicabile quando il ricorrente e il convenuto sono domiciliati in uno Stato membro, mentre i fatti controversi sono localizzati in un paese terzo. Ne deduco che, in un caso del genere, il foro del debitore è competente a statuire su tali fatti controversi. V., parimenti, Van Calster, G., Luks, Ch., Extraterritoriality and private international law, Recht in beweging - 19de VRG Alumnidag 2012, MAKLU, Anvers – Apeldoorn, 2012, pag. 132.

86. Ne deduco che, contrariamente a quanto sostenuto dalla Facebook Ireland, nonché dai governi lettone e finlandese, il giudice di uno Stato membro può statuire, in linea di principio, sulla rimozione di contenuti al di fuori del territorio di tale Stato membro, poiché la portata territoriale della sua competenza ha carattere universale [43]. Ad un giudice di uno Stato membro può essere impedito di pronunciarsi su una rimozione a livello mondiale non a causa di una questione di competenza, bensì, eventualmente, a causa di una questione di merito.

87. Occorre adesso analizzare la questione degli effetti extraterritoriali delle ingiunzioni rivolte agli host provider, la quale, nella specie, come ho indicato al paragrafo 81 delle presenti conclusioni, si riduce alla questione della portata territoriale di un obbligo di rimozione.

c) Sulla portata territoriale di un obbligo di rimozione

88. Anzitutto, occorre osservare che, come ammesso dal governo finlandese, l'articolo 15, paragrafo 1, della direttiva 2000/31 non disciplina gli effetti territoriali delle ingiunzioni rivolte ai prestatori dei servizi della società dell'informazione. Inoltre, fatto salvo il rispetto dei requisiti prescritti dalla direttiva 2000/31, gli obblighi di rimozione imposti a tali prestatori nell'ambito delle ingiunzioni rientrano nel campo di applicazione del diritto nazionale.

89. È poi difficile, in assenza di una normativa dell'Unione in materia di pregiudizio alla vita privata e ai diritti della personalità, giustificare gli effetti territoriali di un'ingiunzione invocando la tutela dei diritti fondamentali garantiti agli articoli 1, 7 e 8 della Carta. Infatti, il campo di applicazione della Carta segue il campo di applicazione del diritto dell'Unione e non viceversa [44] e, nella specie, quanto al merito, il ricorso della ricorrente non è basato sul diritto dell'Unione.

90. A tal riguardo, occorre osservare che la ricorrente non sembra far valere diritti in materia di tutela dei dati personali e che essa non contesta alla Facebook Ireland di aver «proceduto» ad un trattamento illecito dei suoi dati, poiché la sua domanda è fondata sulle disposizioni generali del diritto civile. Inoltre, il giudice del rinvio non invoca strumenti giuridici del diritto dell'Unione pertinenti in tale materia. Esso invoca unicamente la direttiva 2000/31. Orbene, risulta dall'articolo 1, paragrafo 5, lettera b), di tale direttiva che quest'ultima non si applica alle questioni relative ai servizi della società dell'informazione oggetto delle direttive relative alla tutela dei dati personali.

91. Infine, se è possibile ricavare dal regolamento n. 1215/2012 insegnamenti in relazione agli effetti prodotti dalle ingiunzioni negli Stati membri, così non è per quanto riguarda quelli prodotti al di fuori dell'Unione. Infatti, tale regolamento non esige che un'ingiunzione emessa dal giudice di uno Stato membro esplichi effetti anche in Stati terzi. Inoltre, il fatto che un giudice sia competente a statuire nel merito in forza di una norma sulla competenza del diritto dell'Unione non implica che, nel farlo, essa applichi unicamente norme sostanziali che ricadono nell'ambito di applicazione del diritto dell'Unione e, pertanto, della Carta.

43 Si tratta pertanto, in tal caso, di una competenza cosiddetta «globale» o «generale», V. Larsen, T.B., «The extent of jurisdiction under the forum delicti rule in European trademark litigation», *Journal of Private International Law*, 2018, vol. 14, n. 3, pag. 550 e 551.

44 V. sentenza del 26 febbraio 2013, Åkerberg Fransson (C-617/10, EU:C:2013:105, punto 19). V., parimenti, le mie conclusioni nella causa Google (Portata territoriale della cancellazione) (C-507/17, EU:C:2019:15, paragrafo 55).

92. Per siffatti motivi, tanto la questione degli effetti extraterritoriali di un'ingiunzione che impone un obbligo di rimozione quanto quella della portata territoriale di un simile obbligo dovrebbero essere oggetto di un'analisi effettuata alla luce non del diritto dell'Unione ma, segnatamente, del diritto internazionale pubblico e privato non armonizzato a livello dell'Unione [45]. Infatti, non c'è nulla che evidenzi che la situazione oggetto del procedimento principale possa rientrare nella sfera di applicazione del diritto dell'Unione e, pertanto, delle norme di diritto internazionale che possono incidere sull'interpretazione del diritto dell'Unione [46].

93. Di conseguenza, per quanto riguarda la portata territoriale di un obbligo di rimozione imposto ad un host provider nell'ambito di un'ingiunzione, si deve ritenere che quest'ultimo non sia disciplinato né dall'articolo 15, paragrafo 1, della direttiva 2000/31 né da nessun altra disposizione di siffatta direttiva e, pertanto, che tale disposizione non osti a che un host provider sia costretto a rimuovere informazioni diffuse a mezzo di una piattaforma di rete sociale a livello mondiale. Inoltre, detta portata territoriale non è neanche disciplinata dal diritto dell'Unione, nella misura in cui, nella specie, il ricorso della ricorrente non è fondato sul medesimo.

94. Ciò premesso, sia a fini di completezza sia per il caso in cui la Corte non dovesse aderire alla mia proposta, formulerò alcune osservazioni supplementari per quanto attiene alla rimozione delle informazioni diffuse a mezzo di una piattaforma di rete sociale a livello mondiale.

95. In forza del diritto internazionale, non è escluso che un'ingiunzione possa esplicare effetti cosiddetti «extraterritoriali» [47]. Orbene, come ho indicato al paragrafo 80 delle presenti conclusioni, un siffatto approccio comporterebbe l'estensione dell'accertamento del carattere illecito delle informazioni di cui trattasi ai territori di altri Stati membri, indipendentemente dal carattere lecito o meno di tali informazioni in forza della legge designata come applicabile secondo le norme di conflitto di tali Stati membri.

96. Pertanto, si potrebbe sostenere che la Corte abbia già implicitamente ammesso un siffatto approccio nella sentenza Bolagsupplysningen e Ilsjan [48]. È vero che, in tale sentenza, la Corte non si è affatto pronunciata sulla legge applicabile ad una domanda di rimozione dei contenuti messi in rete. Tuttavia, la Corte ha dichiarato che, alla luce dell'*ubiquità dei contenuti messi in rete su un sito Internet* e del fatto che *la portata della loro diffusione è in linea di principio universale*, una domanda diretta segnatamente alla rimozione di siffatti contenuti deve essere proposta dinanzi a un giudice competente a conoscere della totalità di una domanda di risarcimento del danno. Nel farlo, a mio avviso, tale giudice applicherebbe la legge o le leggi designate come applicabili in forza delle sue norme di conflitto [49]. Non si può escludere che un giudice di uno Stato membro applichi, in tale contesto, una sola legge designata come applicabile.

45 Per quanto riguarda gli effetti extraterritoriali delle decisioni giudiziarie, è talvolta difficile tracciare un confine fra il diritto internazionale pubblico e privato. V. Maier, H.G, «Extraterritorial Jurisdiction at a Crossroads: An Intersection between Public and Private International Law», *The American Journal of International Law*, vol. 76, n. 2, pag. 280; e Svantesson, D.J.B., *Solving the Internet Jurisdiction Puzzle*, Oxford Univerity Press, Oxford, 2017, pag. 40.

46 V., in tal senso, ordinanza del 12 luglio 2012, Currà e a. (C-466/11, EU:C:2012:465, punto 19).

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

48 Sentenza del 17 ottobre 2017 (C-194/16, EU:C:2017:766, punto 44).

49 V. parimenti, per quanto riguarda le implicazioni della suddetta sentenza, Lundstedt, L., «Putting Right Holders in the Centre: Bolagsupplysningen and Ilsjan (C-194/16): What Does It Mean for International Jurisdiction over Transborder Intellectual Property Infringement Disputes?», *International Review of Intellectual Property and Competition Law*, 2018, vol. 49, n. 9, pag. 1030, e Svantesson, D.J.B., «European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments», *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2018, vol. 9, n. 2, pag. 122, punto 59.

97. Tuttavia, se un siffatto giudice non potesse statuire sulla cancellazione dei contenuti messi in rete a livello mondiale, si porrebbe allora la questione di quale giudice si trovi nella posizione migliore per pronunciarsi su una siffatta cancellazione. Infatti, ciascun giudice si troverebbe di fronte agli inconvenienti descritti al paragrafo precedente. Si pone inoltre la questione se si debba esigere da un richiedente, malgrado tali difficoltà pratiche, che egli dimostri che l'informazione qualificata come illecita secondo la legge designata come applicabile in forza delle norme di conflitto dello Stato membro adito sia illecita secondo tutte le leggi potenzialmente applicabili.

98. Anche qualora si ammettesse che le considerazioni relative al carattere territoriale della tutela derivante dalla norme sostanziali in materia di pregiudizio alla vita privata e ai diritti della personalità non ostino ad un siffatto requisito, occorrerebbe inoltre tenere conto dei diritti fondamentali riconosciuti a livello mondiale.

99. Infatti, come ho già affermato in un contesto differente, l'interesse legittimo del pubblico ad accedere ad un'informazione varia necessariamente da uno Stato terzo all'altro, a seconda della sua collocazione geografica [50]. Per questo motivo, nel caso di una rimozione a livello mondiale, esisterebbe il rischio che la sua attuazione impedisca a persone stabilite in Stati diversi da quello del giudice adito di accedere all'informazione.

100. Per concludere, risulta dalle considerazioni che precedono che il giudice di uno Stato membro può, in teoria, statuire sulla rimozione di informazioni diffuse a mezzo Internet a livello mondiale. Tuttavia, a causa delle differenze esistenti fra le leggi nazionali, da un lato, e la tutela della vita privata e dei diritti della personalità da esse prevista, dall'altro, e al fine di rispettare i diritti fondamentali ampiamente diffusi, un siffatto giudice deve adottare piuttosto un atteggiamento di autolimitazione. Di conseguenza, nel rispetto della cortesia internazionale [51], menzionata dal governo portoghese, tale giudice dovrebbe limitare, per quanto possibile, gli effetti extraterritoriali delle sue ingiunzioni in materia di pregiudizio alla vita privata e ai diritti della personalità [52]. L'attuazione di un obbligo di rimozione non dovrebbe eccedere quanto necessario ad assicurare la protezione della persona lesa. Pertanto, invece di cancellare il contenuto, detto giudice potrebbe, se del caso, ordinare la disabilitazione dell'accesso a tali informazioni con l'ausilio del blocco geografico.

101. Tali considerazioni non possono essere rimesse in discussione dall'argomento della ricorrente, secondo il quale il blocco geografico delle informazioni illecite potrebbe essere agevolmente eluso tramite un server proxy o altri strumenti.

102. Per riprendere una riflessione formulata nel contesto di situazioni che rientrano nel diritto dell'Unione: la protezione della vita privata e dei diritti della personalità non deve necessariamente essere assicurata in maniera assoluta, ma deve essere ponderata con la protezione di altri diritti fondamentali [53]. Occorre pertanto evitare misure esorbitanti, le quali trascurerebbero il compito di assicurare un giusto equilibrio fra i diversi diritti fondamentali [54].

103. Fatta salve le suesposte osservazioni supplementari, mantengo, in relazione alla portata territoriale di un obbligo di rimozione, la posizione sostenuta al paragrafo 93 delle presenti conclusioni.

50 V. le mie conclusioni nella causa Google (Portata territoriale della cancellazione) (C-507/17, EU:C:2019:15, paragrafo 60).

51 V., segnatamente, sulle implicazioni pratiche di tale cortesia internazionale, Maier, H.G, op. cit., pag. 283.

52 V. dottrina citata alla nota 47. V. parimenti, in contesti ben diversi da quello della causa in esame, Scott, J., «The New EU "Extraterritoriality"», *Common Market Law Review*, 2014, vol. 51, n. 5, pag. 1378.

53 V., per analogia, per quanto attiene alla ponderazione del diritto di proprietà intellettuale e del diritto al rispetto della vita privata e familiare, garantito all'articolo 7 della Carta, sentenza del 18 ottobre 2018, Bastei Lübbe (C-149/17, EU:C:2018:841, punti da 44 a 47). V., parimenti, le mie conclusioni nella causa Bastei Lübbe (C-149/17, EU:C:2018:400, paragrafi da 37 a 39).

54 V., in tal senso, per quanto riguarda la tutela della proprietà intellettuale, sentenza del 27 marzo 2014, UPC Telekabel Wien (C-314/12, EU:C:2014:192, punti da 58 a 63). V., parimenti, conclusioni dell'avvocato generale Cruz Villalón nella causa UPC Telekabel Wien (C-314/12, EU:C:2013:781, paragrafi da 99 a 101), nonché le mie conclusioni nella causa Stichting Brein (C-610/15, EU:C:2017:99, paragrafi da 69 a 72).

B. Sulla terza questione pregiudiziale

104. Con la terza questione, il giudice del rinvio chiede se l'articolo 15 della direttiva 2000/31 osti a che ad un host provider venga rivolta un'ingiunzione che lo obblighi a rimuovere dalla sua piattaforma informazioni equivalenti a quella dichiarata illecita nel corso di un procedimento giudiziario dopo che lo stesso è venuto a conoscenza di tali informazioni.

105. La ricorrente, nonché i governi austriaco, lettone, portoghese e finlandese ritengono, in sostanza, che l'articolo 15, paragrafo 1, della direttiva 2000/31 non osti a che venga ingiunto ad un host provider di rimuovere informazioni dal contenuto equivalente a quella dichiarata illecita, allorché ne abbia avuto conoscenza. Alla luce della sua analisi della prima questione, la Facebook Ireland ritiene che non occorra rispondere alla terza questione.

106. Aderisco alla posizione condivisa, in sostanza, dalla ricorrente e da tutti i governi.

107. Infatti, qualora un obbligo di rimozione non implichi una sorveglianza generale delle informazioni memorizzate da un host provider, ma discenda da una conoscenza risultante dalla notifica effettuata dalla persona interessata o dai terzi, non sussiste una violazione del divieto previsto all'articolo 15, paragrafo 1, della direttiva 2000/31.

108. Di conseguenza, propongo di rispondere alla terza questione pregiudiziale dichiarando che l'articolo 15, paragrafo 1, della direttiva 2000/31 deve essere interpretato nel senso che esso non osta a che un host provider sia costretto a rimuovere informazioni equivalenti a quella qualificata come illecita, qualora un obbligo di rimozione non implichi una sorveglianza generale delle informazioni memorizzate e discenda da una conoscenza risultante dalla notifica effettuata dalla persona interessata, dai terzi o da un'altra fonte.

VI. Conclusione

109. Alla luce delle suesposte considerazioni, suggerisco alla Corte di rispondere come segue alle questioni pregiudiziali proposte dall'Oberster Gerichtshof (Corte Suprema, Austria):

1) L'articolo 15, paragrafo 1, della direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell' 8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («direttiva sul commercio elettronico»), deve essere interpretato nel senso che esso non osta a che un host provider che gestisce una piattaforma di rete sociale sia costretto, nell'ambito di un'ingiunzione, a ricercare e ad individuare, fra tutte le informazioni diffuse dagli utenti di tale piattaforma, le informazioni identiche a quella qualificata come illecita dal giudice che ha emesso tale ingiunzione. Nell'ambito di una siffatta ingiunzione, un host provider può essere costretto a ricercare e ad individuare le informazioni equivalenti a quella qualificata come illecita soltanto fra informazioni diffuse dall'utente che ha divulgato tale informazione. Un giudice che statuisce sulla rimozione di siffatte informazioni equivalenti deve garantire che gli effetti della sua ingiunzione siano chiari, precisi e prevedibili. Nel farlo, esso deve ponderare i diritti fondamentali coinvolti e tenere conto del principio di proporzionalità.

2) Per quanto riguarda la portata territoriale di un obbligo di rimozione imposto ad un host provider nell'ambito di un'ingiunzione, si deve ritenere che quest'ultima non sia disciplinata né dall'articolo 15, paragrafo 1, della direttiva 2000/31 né da nessun altra disposizione di siffatta direttiva e, pertanto, che tale disposizione non osti a che un host provider sia costretto a rimuovere informazioni diffuse a mezzo di una piattaforma di rete sociale a livello mondiale. Inoltre, detta portata territoriale non è neanche disciplinata dal diritto dell'Unione, nella misura in cui, nella specie, il ricorso della ricorrente non è fondato sul medesimo.

3) L'articolo 15, paragrafo 1, della direttiva 2000/31 deve essere interpretato nel senso che esso non osta a che un host provider sia costretto a rimuovere informazioni equivalenti a quella qualificata come illecita, qualora un obbligo di rimozione non implichi una sorveglianza generale delle informazioni memorizzate e discenda da una conoscenza risultante dalla notifica effettuata dalla persona interessata, dai terzi o da un'altra fonte.