Raccolta della giurisprudenza

CONCLUSIONI DELL'AVVOCATO GENERALE
M. CAMPOS SÁNCHEZ-BORDONA
presentate il 12 maggio 2016 [1]

Causa C-582/14

Patrick Breyer
contro
Bundesrepublik Deutschland

[domanda di pronuncia pregiudiziale proposta dal Bundesgerichtshof (Corte federale di giustizia, Germania)]

«Trattamento di dati personali — Direttiva 95/46/CE — Articoli 2, lettera a), e 7, lettera f) — Nozione di "dati personali" — Indirizzi IP — Conservazione da parte di un fornitore di servizi di media elettronici — Normativa nazionale che non consente di tenere conto dell'interesse legittimo perseguito dal responsabile del trattamento»

1. Un indirizzo di protocollo Internet (in prosieguo: l'«indirizzo IP») è una sequenza di numeri binari che, assegnata a un dispositivo (un computer, un tablet o uno smartphone), lo identifica e gli consente di accedere alla rete di comunicazioni elettroniche. Detto dispositivo, per collegarsi a Internet, deve utilizzare la sequenza numerica assegnata dai fornitori del servizio di accesso alla rete. L'indirizzo IP viene trasmesso al server in cui è memorizzata la pagina web oggetto di consultazione.

2. In particolare, i fornitori di accesso alla rete (generalmente le compagnie telefoniche) assegnano ai loro clienti i cosiddetti «indirizzi IP dinamici», temporaneamente, per ogni collegamento a Internet e li modificano in occasione dei successivi collegamenti. Le medesime compagnie tengono un registro in cui sono indicati gli indirizzi IP assegnati, di volta in volta, a un determinato dispositivo [2].

3. Di norma, anche i titolari dei siti Internet ai quali si accede mediante indirizzi IP dinamici tengono un registro in cui è indicato quali pagine sono state consultate, quando e da quale indirizzo IP dinamico. Tali registri possono, tecnicamente, essere conservati senza limiti di tempo al termine del collegamento a Internet di ciascun utente.

4. Un indirizzo IP dinamico, di per sé, non è sufficiente per permettere al prestatore di servizi di identificare l'utente della sua pagina web. Tuttavia, detto prestatore può farlo associando l'indirizzo IP dinamico ad altre informazioni aggiuntive di cui dispone il fornitore di accesso alla rete.

1 — Lingua originale: lo spagnolo.

2 — L'articolo 5 della direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GU 2006, L 105, pag. 54), imponeva, tra altri obblighi, quello di conservare, a fini di indagine, accertamento e perseguimento di reati gravi, «data e ora del log-in e del log-off del servizio di accesso Internet (…) unitamente all'indirizzo IP, dinamico o statico, assegnato dal fornitore di accesso Internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato».

5. La presente controversia verte sulla questione se gli indirizzi IP dinamici siano dati personali ai sensi dell'articolo 2, lettera a), della direttiva 95/46/CE[3]. Per fornire una risposta occorre stabilire, preliminarmente, se a tal fine rilevi il fatto che le informazioni aggiuntive necessarie per l'identificazione dell'utente non sono in possesso del titolare del sito Internet, bensì di un terzo (nello specifico, il fornitore del servizio di accesso alla rete).

6. Si tratta di una questione inedita per la Corte, dato che, al punto 51 della sentenza Scarlet Extended[4], essa ha dichiarato che gli indirizzi IP «costituiscono dati personali protetti, in quanto consentono di identificare in modo preciso i suddetti utenti», ma in un contesto in cui la raccolta e l'identificazione degli indirizzi IP venivano effettuate dal fornitore di accesso alla rete[5], e non da un fornitore di contenuti, come nel presente caso.

7. Qualora gli indirizzi IP dinamici costituissero dati personali per il fornitore di servizi Internet, si dovrebbe allora esaminare se il loro trattamento rientri nell'ambito di applicazione della direttiva 95/46.

8. È possibile che, pur costituendo dati personali, essi non godano della tutela conferita dalla direttiva 95/46 nel caso in cui, ad esempio, lo scopo del loro trattamento sia quello di perseguire penalmente eventuali attacchi informatici. In tal caso, la direttiva 95/46, conformemente al suo articolo 3, paragrafo 2, primo trattino, non sarebbe applicabile.

9. Occorre stabilire, inoltre, se il prestatore di servizi che memorizza gli indirizzi IP dinamici quando un utente accede alle sue pagine web (nel caso di specie, la Repubblica federale di Germania) agisca in veste di pubblica autorità oppure come privato.

10. Infine, qualora la direttiva 95/46 fosse applicabile, si dovrebbe precisare entro quali limiti il suo articolo 7, lettera f), sia compatibile con una normativa nazionale che restringe la portata di una delle condizioni previste da detta disposizione per giustificare il trattamento di dati personali.

I – **Contesto normativo**

A – *Diritto dell'Unione*

11. Il considerando 26 della direttiva 95/46 è così formulato:

«(26) considerando che i principi della tutela si devono applicare ad ogni informazione concernente una persona identificata o identificabile; che, per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona; che i principi della tutela non si applicano a dati resi anonimi in modo tale che la persona interessata non è più identificabile; che i codici di condotta ai sensi dell'articolo 27 possono costituire uno strumento utile di orientamento sui mezzi grazie ai quali [i] dati possano essere resi anonimi e registrati in modo da rendere impossibile l'identificazione della persona interessata».

3 — 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).

4 — Sentenza del 24 novembre 2011 (C-70/10, EU:C:2011:771, punto 51).

5 — Ciò si verificava anche nella causa decisa con sentenza del 19 aprile 2012, Bonnier Audio e a. (C-461/10, EU:C:2012:219, punti 51 e 52).

12. Ai sensi dell'articolo 1 della direttiva 95/46:

«1. Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.

2. Gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri, per motivi connessi alla tutela garantita a norma del paragrafo 1».

13. Secondo l'articolo 2 della direttiva 95/46:

«Ai fini della presente direttiva si intende per:

a) "dati personali": qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero d'identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale;

b) "trattamento di dati personali" ("trattamento"): qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione;

(…)

d) "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario;

(…)

f) "terzi": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che non sia la persona interessata, il responsabile del trattamento, l'incaricato del trattamento e le persone autorizzate all'elaborazione dei dati sotto la loro autorità diretta;

(…)».

14. Sotto la rubrica «Campo d'applicazione», l'articolo 3 della direttiva 95/46 dispone quanto segue:

«1. Le disposizioni della presente direttiva si applicano al trattamento di dati personali interamente o parzialmente automatizzato nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi.

2. Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali[:]

— effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale;

(…)».

15. Il capo II della direttiva 95/46, relativo alle «[c]ondizioni generali di liceità dei trattamenti di dati personali», inizia con l'articolo 5, secondo cui «[g]li Stati membri precisano, nei limiti delle disposizioni del presente capo, le condizioni alle quali i trattamenti di dati personali sono leciti».

16. Ai sensi dell'articolo 6 della direttiva 95/46:

«1. Gli Stati membri dispongono che i dati personali devono essere:

a) trattati lealmente e lecitamente;

b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate;

c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati;

d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati;

e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici.

2. Il responsabile del trattamento è tenuto a garantire il rispetto delle disposizioni del paragrafo 1».

17. Secondo l'articolo 7 della direttiva 95/46:

«Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando:

a) la persona interessata ha manifestato il proprio consenso in maniera inequivocabile, oppure

b) è necessario all'esecuzione del contratto concluso con la persona interessata o all'esecuzione di misure precontrattuali prese su richiesta di tale persona, oppure

c) è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento, oppure

d) è necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure

e) è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati, oppure

f) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1».

18. A tenore dell'articolo 13 della direttiva 95/46:

«1. Gli Stati membri possono adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti dalle disposizioni dell'articolo 6, paragrafo 1, dell'articolo 10, dell'articolo 11, paragrafo 1 e degli articoli 12 e 21, qualora tale restrizione costituisca una misura necessaria alla salvaguardia:

a) della sicurezza dello Stato;

b) della difesa;

c) della pubblica sicurezza;

d) della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate;

e) di un rilevante interesse economico o finanziario di uno Stato membro o dell'Unione europea, anche in materia monetaria, di bilancio e tributaria;

f) di un compito di controllo, ispezione o disciplina connesso, anche occasionalmente, con l'esercizio dei pubblici poteri nei casi di cui alle lettere c), d) ed e);

g) della protezione della persona interessata o dei diritti e delle libertà altrui.

(…)».

B – *Diritto nazionale*

19. L'articolo 12 del Telemediengesetz (legge sui servizi di telecomunicazione; in prosieguo: il «TMG») [6] così dispone:

«1. Il fornitore di servizi può raccogliere e utilizzare dati personali ai fini della messa a disposizione di servizi di telecomunicazione solo nella misura in cui lo permetta la presente legge o un'altra norma, riguardante espressamente i servizi di telecomunicazione, oppure se l'utente vi abbia prestato consenso.

2. Il fornitore di servizi può utilizzare ad altri fini i dati personali raccolti per la messa a disposizione di servizi di telecomunicazione solo nella misura in cui lo permetta la presente legge o un'altra norma, riguardante espressamente i servizi di telecomunicazione, oppure l'utente vi abbia prestato consenso.

3. Ove non sia diversamente stabilito, le norme rispettivamente vigenti per la tutela dei dati personali trovano applicazione anche nel caso in cui i dati non costituiscano oggetto di trattamento automatizzato».

6 — Legge del 26 febbraio 2007 (BGBl 2007 I, pag. 179).

20. A termini dell'articolo 15 del TMG:

«1. Il fornitore di servizi può raccogliere e utilizzare i dati personali di un utente solo nella misura in cui ciò sia necessario per rendere possibile la fruizione di servizi di telecomunicazione e per fatturarla (dati di utenza). Costituiscono dati di utenza, in particolare:

1) gli elementi per l'identificazione dell'utente,

2) le informazioni su inizio e termine, nonché sulla durata della rispettiva fruizione e

3) le indicazioni sui servizi di telecomunicazione fruiti dall'utente.

2. Il fornitore di servizi può aggregare i dati di utenza di un utente attinenti alla fruizione di diversi servizi di telecomunicazione, laddove ciò sia necessario a fini di fatturazione verso l'utente.

(…)

4. Il fornitore di servizi può utilizzare i dati di utenza oltre il termine della fruizione, ove essi siano necessari a fini di fatturazione verso l'utente (dati di fatturazione). Il fornitore di servizi può bloccare i dati ai fini dell'osservanza dei periodi di conservazione definiti per legge, statuto o contratto. (…)».

21. Conformemente all'articolo 3, paragrafo 1, del Bundesdatenschutzgesetz (legge federale sulla protezione dei dati; in prosieguo: il «BDSG»)[7], «[i] dati personali sono dati particolari su condizioni personali o materiali di una persona fisica identificata o identificabile (interessato). (…)».

II – **Fatti**

22. Il sig. Breyer ha proposto un'azione inibitoria contro la Repubblica federale di Germania a causa della memorizzazione di indirizzi IP.

23. Numerose istituzioni pubbliche tedesche gestiscono portali Internet accessibili al pubblico, in cui esse mettono a disposizione informazioni aggiornate. Al fine di contrastare attacchi e consentire il perseguimento penale dei pirati informatici, nella maggior parte di detti portali tutti gli accessi sono conservati nei file di registro. In essi sono memorizzati, oltre il termine della rispettiva fruizione, il nome del documento ovvero della pagina consultati, le parole inserite nella casella di ricerca, la data e l'ora della richiesta, la quantità di dati trasferiti, il messaggio relativo all'esito della consultazione e l'indirizzo IP del computer che effettua l'accesso.

24. Il sig. Breyer, che ha visitato diversi siti Internet di questo tipo, ha chiesto con il suo ricorso di condannare la Repubblica federale di Germania ad astenersi dal memorizzare o dal far memorizzare da altri l'indirizzo IP del suo sistema di host che effettua l'accesso, salvo che non sia necessario, in caso di guasto, al ripristino della disponibilità del servizio di telecomunicazione.

25. La domanda del sig. Breyer è stata respinta in primo grado. Il suo ricorso di appello, tuttavia, è stato parzialmente accolto e la Repubblica federale di Germania è stata condannata ad astenersi dal memorizzare l'indirizzo IP oltre il termine di ciascuna operazione di accesso. L'inibitoria era subordinata alla condizione che il ricorrente fornisse i propri dati personali nel corso dell'operazione di accesso, anche sotto forma di un indirizzo e-mail, e che la memorizzazione non fosse necessaria al ripristino della disponibilità del servizio di telecomunicazione.

7 — Legge del 20 dicembre 1990 (BGBl 1990 I, pag. 2954).

III – **Questioni sollevate**

26. Entrambe le parti hanno proposto ricorso per cassazione. La Sezione VI del Bundesgerichtshof (Corte federale di giustizia, Germania) ha sollevato le seguenti questioni pregiudiziali, depositate il 17 dicembre 2014:

«1) Se l'articolo 2, lettera a), della direttiva 95/46/CE (…) debba essere interpretato nel senso che un indirizzo di protocollo Internet (indirizzo IP), memorizzato da un fornitore di servizi in relazione ad un accesso al suo sito Internet, costituisce per quest'ultimo un dato personale già nel momento in cui un terzo (nel caso di specie: un fornitore di accesso) disponga delle informazioni aggiuntive necessarie ai fini dell'identificazione della persona interessata.

2) Se l'articolo 7, lettera f), della direttiva sulla tutela dei dati personali osti ad una disposizione di diritto nazionale in forza della quale il fornitore di servizi può raccogliere e utilizzare i dati personali di un utente senza il suo consenso solo nella misura in cui ciò sia necessario per consentire l'effettiva fruizione del servizio di telecomunicazione da parte del rispettivo utente e per fatturarla e secondo la quale il fine di assicurare il funzionamento di detto servizio non può giustificare l'utilizzazione dei dati oltre il termine della rispettiva fruizione».

27. Secondo quanto spiegato dal giudice del rinvio, il ricorrente potrebbe esigere, in forza del diritto tedesco, che gli indirizzi IP non siano memorizzati qualora la loro conservazione costituisse un'ingerenza illecita, conformemente alla normativa in materia di protezione dei dati, nel suo diritto generale di personalità, più specificamente nel suo diritto all'«autodeterminazione informativa» [articoli 1004, paragrafo 1, e 823, paragrafo 1, del Bürgerliches Gesetzbuch (codice civile tedesco), in combinato disposto con gli articoli 1 e 2 del Grundgesetz (Legge fondamentale)].

28. Ciò accadrebbe qualora: a) l'indirizzo IP (comunque associato alla data e all'ora dell'accesso ad un sito Internet) dovesse essere considerato rientrante nei «dati personali» ai sensi dell'articolo 2, lettera a), in combinato disposto con il considerando 26, secondo periodo, della direttiva 95/46, ovvero dell'articolo 12, paragrafi 1 e 3, del TMG in combinato disposto con l'articolo 3, paragrafo 1, del BDSG e b) non ricorra un caso di autorizzazione ai sensi dell'articolo 7, lettera f), della direttiva 95/46, ovvero degli articoli 12, paragrafi 1 e 3, e 15, paragrafi 1 e 4, del TMG.

29. Secondo il Bundesgerichtshof (Corte federale di giustizia), ai fini dell'interpretazione del diritto nazionale (articolo 12, paragrafo 1, del TMG) occorre accertare come debba intendersi la natura personale dei dati ai quali fa riferimento l'articolo 2, lettera a), della direttiva 95/46.

30. Il giudice a quo fa inoltre presente che, poiché, ai sensi dell'articolo 15, paragrafo 1, del TMG, il fornitore di servizi può raccogliere e utilizzare i dati personali di un utente solo nella misura in cui ciò sia necessario per rendere possibile la fruizione di servizi di telecomunicazione e per fatturarla (dati di utenza) [8], l'interpretazione di detta disposizione è legata a quella dell'articolo 7, lettera f), della direttiva 95/46.

IV – **Procedimento dinanzi alla Corte. Argomenti delle parti**

31. Hanno presentato osservazioni scritte i governi tedesco, austriaco e portoghese, nonché la Commissione. Solo detta istituzione e il sig. Breyer sono intervenuti all'udienza pubblica tenutasi il 25 febbraio 2016, alla quale non ha partecipato il governo tedesco.

8 — Secondo il Bundesgerichtshof (Corte federale di giustizia), costituiscono dati di utenza gli elementi per l'identificazione dell'utente, le informazioni su inizio e termine, nonché sulla durata della rispettiva fruizione e le indicazioni sui servizi di telecomunicazione fruiti dall'utente.

A – *Argomenti delle parti relativi alla prima questione*

32. A parere del sig. Breyer, costituirebbero dati personali anche quelli la cui aggregazione sia possibile solo sul piano teorico, vale a dire, partendo dalla premessa di un pericolo potenziale astratto, poco rilevando se a livello pratico tale aggregazione venga effettivamente operata. A suo avviso, il fatto che un organismo possa essere più o meno in grado di identificare una persona attraverso l'indirizzo IP non significherebbe che non esista un rischio per detta persona. Inoltre, a suo parere, sarebbe rilevante il fatto che la Germania conserva i suoi dati IP al fine, se del caso, di rilevare eventuali attacchi o intentare azioni penali, ai sensi dell'articolo 113 della Telekommunikationsgesetz (legge sulla telecomunicazione), come è accaduto in numerose occasioni.

33. Secondo il governo tedesco, si dovrebbe rispondere alla prima questione in senso negativo. A suo avviso, gli indirizzi IP dinamici non rivelerebbero una persona «identificata» ai sensi dell'articolo 2, lettera a), della direttiva 95/46. Per stabilire se essi forniscano informazioni su una persona «identificabile», ai sensi della medesima disposizione, la *identificabilità* andrebbe esaminata secondo un criterio «relativo». Ciò risulterebbe, a suo parere, dal considerando 26 della direttiva 95/46, secondo cui si deve tenere conto solo dei mezzi che possono essere «ragionevolmente» utilizzati dal responsabile del trattamento o da altri per identificare una persona. Tale precisazione indicherebbe che il legislatore dell'Unione non ha inteso includere nell'ambito di applicazione della direttiva 95/46 le situazioni nelle quali l'identificazione sia oggettivamente possibile da parte di qualsiasi terzo.

34. Il governo tedesco ritiene inoltre che la nozione di «dati personali» ai sensi dell'articolo 2, lettera a), della direttiva 95/46 debba essere interpretata alla luce della finalità di detta direttiva, che è quella di garantire il rispetto dei diritti fondamentali. La necessità di tutelare le persone fisiche potrebbe essere vista diversamente a seconda del soggetto che detiene i dati e della circostanza che tale soggetto disponga o meno dei mezzi necessari per utilizzare tali dati al fine di identificarle.

35. Il governo tedesco sostiene che il sig. Breyer non possa essere identificato associando gli indirizzi IP alle altre informazioni conservate dai fornitori di contenuti. A tale scopo sarebbero necessarie le informazioni di cui dispongono i fornitori di accesso a Internet, i quali, in mancanza di una base giuridica, non possono trasmetterle ai fornitori di contenuti.

36. Secondo il governo austriaco, per contro, la risposta dovrebbe essere affermativa. Conformemente al considerando 26 della direttiva 95/46, affinché una persona sia ritenuta identificabile non occorrerebbe che tutti i suoi dati identificativi siano detenuti da un unico soggetto. Così, un indirizzo IP potrebbe costituire un dato personale qualora un terzo (ad esempio il fornitore di accesso a Internet) disponesse dei mezzi necessari per identificare il titolare di tale indirizzo senza eccessivi sforzi.

37. Il governo portoghese propende del pari per una risposta affermativa, ritenendo che l'indirizzo IP, associato alla data della sessione di consultazione, costituisca un dato personale, in quanto può condurre all'identificazione dell'utente da parte di un soggetto diverso da quello che ha conservato l'indirizzo IP.

38. Anche la Commissione propone una risposta affermativa, richiamandosi alla soluzione adottata dalla Corte nella causa Scarlet Extended[9]. A suo parere, poiché la conservazione degli indirizzi IP serve proprio a identificare gli utenti in caso di attacchi informatici, l'utilizzo delle informazioni supplementari memorizzate dai fornitori di accesso a Internet costituirebbe un mezzo che può essere

9 — Sentenza del 24 novembre 2011 (C-70/10, EU:C:2011:771, punto 51).

utilizzato «ragionevolmente», ai sensi del considerando 26 della direttiva 95/46. In definitiva, ad avviso della Commissione, tanto l'obiettivo perseguito da detta direttiva quanto gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta») militerebbero a favore di un'interpretazione estensiva dell'articolo 2, lettera a), della direttiva 95/46.

B – *Argomenti delle parti relativi alla seconda questione*

39. Il sig. Breyer sostiene che l'articolo 7, lettera f), della direttiva 95/46 costituisce una clausola generale la cui applicazione pratica deve essere precisata. Conformemente alla giurisprudenza della Corte, occorrerebbe quindi valutare le circostanze del caso di specie e stabilire se esistano gruppi portatori di un interesse legittimo ai sensi di detta disposizione, cosicché sarebbe non solo lecito, bensì indispensabile prevedere regole specifiche per tali gruppi ai fini dell'applicazione del suddetto articolo. Nel caso di specie, secondo il sig. Breyer, la normativa nazionale sarebbe compatibile con l'articolo 7, lettera f), della direttiva 95/46 nella misura in cui non esista un interesse del portale pubblico alla conservazione dei dati personali, o prevalga l'interesse a tutelare l'anonimato. A suo parere, tuttavia, la conservazione sistematica di dati personali non sarebbe compatibile con una società democratica, né necessaria e proporzionata per garantire il funzionamento dei mezzi elettronici, perfettamente possibile senza la registrazione di tali dati, come dimostrerebbero i siti Internet di alcuni ministeri federali.

40. Il governo tedesco sostiene che non occorre esaminare la seconda questione, sollevata soltanto nell'ipotesi in cui si risponda alla prima in senso affermativo, il che, a suo parere, non dovrebbe accadere, per i suddetti motivi.

41. Il governo austriaco propone di rispondere che la direttiva 95/46 non osta, in generale, alla conservazione di dati come quelli controversi nel procedimento principale, quando sia necessaria per garantire il corretto funzionamento dei mezzi elettronici. Secondo detto governo, una conservazione limitata dell'indirizzo IP, oltre la durata della consultazione di una pagina web, può essere lecita, purché sia rispettato l'obbligo del responsabile del trattamento dei dati personali di applicare le misure di tutela dei medesimi prescritte dall'articolo 17, paragrafo 1, della direttiva 95/46. La lotta contro la pirateria informatica potrebbe legittimare l'analisi dei dati relativi ad attacchi precedenti e il diniego di accesso alla pagina Internet ad alcuni indirizzi IP. La proporzionalità della conservazione di dati come quelli di cui alla causa principale, sotto il profilo oggettivo della garanzia del corretto funzionamento dei mezzi elettronici, dovrebbe essere valutata caso per caso, tenendo conto dei principi enunciati all'articolo 6, paragrafo 1, della direttiva 95/46.

42. Il governo portoghese sostiene che l'articolo 7, lettera f), della direttiva 95/46 non osta alle norme nazionali in discussione nel procedimento principale, in quanto il legislatore tedesco avrebbe già proceduto alla ponderazione, prescritta da detta disposizione, tra gli interessi legittimi del responsabile del trattamento dei dati personali, da un lato, e i diritti e le libertà dei titolari di tali dati, dall'altro.

43. A parere della Commissione, la normativa nazionale che recepisce l'articolo 7, lettera f), della direttiva 95/46 deve definire gli obiettivi del trattamento dei dati personali in modo che siano prevedibili per l'interessato. A suo avviso, la normativa tedesca non rispetterebbe tale requisito in quanto stabilisce, all'articolo 15, paragrafo 1, del TMG, che la conservazione degli indirizzi IP è consentita «nella misura in cui ciò sia necessario per rendere possibile la fruizione di servizi di telecomunicazione».

44. La Commissione propone quindi di rispondere alla seconda questione affermando che l'articolo 7, lettera f), della direttiva 95/46 osta all'interpretazione di una norma nazionale secondo cui un'autorità pubblica che agisce in veste di fornitore di servizi possa raccogliere e utilizzare i dati personali di un utente senza il suo consenso, anche qualora l'obiettivo perseguito sia quello di garantire il corretto funzionamento generale del mezzo elettronico, se la norma nazionale in parola non definisce tale obiettivo in modo sufficientemente chiaro e preciso.

V – **Valutazione**

A – *Prima questione*

1. Delimitazione della questione sollevata

45. La prima questione pregiudiziale, stando ai termini in cui l'ha formulata il Bundesgerichtshof (Corte federale di giustizia), è intesa ad accertare se un indirizzo IP, con il quale si accede a una pagina web, rappresenti per l'ente pubblico titolare di detta pagina un dato personale [ai sensi dell'articolo 2, lettera a), della direttiva 95/46] nel caso in cui il fornitore di accesso alla rete disponga di informazioni aggiuntive necessarie ai fini dell'identificazione dell'interessato.

46. Espressa in questi termini, la questione è sufficientemente precisa per escludere, in via preliminare, altre questioni che si potrebbero sollevare in abstracto circa la natura giuridica degli indirizzi IP nel contesto della protezione dei dati personali.

47. In primo luogo, il Bundesgerichtshof (Corte federale di giustizia) fa riferimento esclusivamente agli «indirizzi IP dinamici», vale a dire quelli che vengono assegnati temporaneamente per ciascun collegamento alla rete e modificati nei successivi collegamenti, che non rientrano pertanto tra gli «indirizzi IP fissi o statici», contraddistinti dal fatto di essere invariabili e di consentire l'identificazione permanente del dispositivo collegato alla rete.

48. In secondo luogo, il giudice del rinvio si è basato sulla presunzione che il fornitore della pagina web non sia in grado, nel procedimento a quo, di identificare, attraverso l'indirizzo IP dinamico, coloro che visitano le sue pagine, né disponga di informazioni aggiuntive che, associate a detto indirizzo IP, consentano di identificarli. Il Bundesgerichtshof (Corte federale di giustizia) sembra ritenere che, in siffatto contesto, l'indirizzo IP dinamico non costituisca un dato personale, ai sensi dell'articolo 2, lettera a), della direttiva 95/46, *per il fornitore della pagina web*.

49. I dubbi del giudice del rinvio riguardano la possibilità che l'indirizzo IP dinamico venga qualificato, per il fornitore della pagina web, come dato personale *qualora un terzo disponga di informazioni aggiuntive* che, associate a detto indirizzo, identifichino coloro che consultano le sue pagine. Tuttavia, e tale precisazione è di maggiore interesse, il Bundesgerichtshof (Corte federale di giustizia) non fa riferimento a qualsiasi terzo che possieda le informazioni aggiuntive, ma solo al fornitore di accesso alla rete (ed esclude, pertanto, altri possibili detentori di questo tipo di informazioni).

50. Esulano quindi dall'analisi, tra l'altro, i seguenti aspetti: a) se gli indirizzi IP statici siano dati personali ai sensi della direttiva 95/46 [10]; b) se gli indirizzi IP dinamici siano, sempre e in qualunque circostanza, dati personali ai sensi di detta direttiva e, infine, c) se la qualificazione degli indirizzi IP come dati personali sia inevitabile fintanto che esista un terzo, chiunque esso sia, che possa utilizzarli per identificare gli utenti della rete.

51. Pertanto, occorre soltanto stabilire se un indirizzo IP dinamico sia un dato personale per il fornitore di un servizio Internet quando la società di comunicazioni che offre l'accesso alla rete (il fornitore di accesso) disponga di informazioni aggiuntive che, associate a tale indirizzo, consentano di identificare coloro che accedono alla pagina web gestita dal primo.

2. Sul merito

52. La questione sollevata dal presente rinvio pregiudiziale è attualmente oggetto, nella dottrina e nella giurisprudenza tedesche, di un intenso dibattito, polarizzato su due correnti di pensiero [11]. Secondo la prima (che opta per un approccio «oggettivo» o «assoluto»), un utente sarebbe identificabile – e, pertanto, l'indirizzo IP costituirebbe un dato personale suscettibile di tutela – se, a prescindere dalle capacità e dai mezzi del fornitore del servizio Internet, l'identificazione può essere effettuata semplicemente associando tale indirizzo IP dinamico ai dati forniti da un terzo (ad esempio, il fornitore di accesso alla rete).

53. Secondo i sostenitori dell'altra corrente (che propugnano un approccio «relativo»), la possibilità di disporre dell'ausilio di un terzo ai fini dell'identificazione finale dell'utente non sarebbe sufficiente per attribuire natura personale all'indirizzo IP dinamico. L'elemento rilevante sarebbe la capacità del soggetto che può accedere al dato di servirsi del medesimo, con i propri mezzi, per identificare una persona.

54. Indipendentemente dai termini di tale controversia nel diritto interno, la risposta della Corte deve limitarsi all'interpretazione delle due disposizioni della direttiva 95/46 alle quali hanno fatto riferimento sia il giudice a quo sia le parti del procedimento, vale a dire l'articolo 2, lettera a) [12], e il considerando 26 [13].

55. Gli indirizzi IP dinamici, semplicemente fornendo informazioni sulla data e sull'ora nelle quali ha avuto luogo l'accesso a una pagina web da un computer (o altro dispositivo), rendono manifesti taluni aspetti del comportamento degli utenti di Internet e, pertanto, implicano una potenziale ingerenza nel diritto alla vita privata [14] garantito dall'articolo 8 della Convenzione europea per la salvaguardia dei

10 — Questione sulla quale la Corte si è pronunciata nelle sentenze del 24 novembre 2011, Scarlet Extended (C 70/10, EU:C:2011:771, punto 51), e del 19 aprile 2012, Bonnier Audio e a. (C 461/10, EU:C:2012:219). Ai punti 51 e 52 di quest'ultima, la Corte ha concluso che la comunicazione, «ai fini della sua identificazione, [del] nome [e del] recapito di un abbonato ad Internet ovvero di un utente Internet che si avvale dell'indirizzo IP a partire dal quale si ritiene che siano stati illecitamente scambiati file contenenti opere protette (…) costituisce un trattamento di dati di carattere personale ai sensi dell'articolo 2, primo comma, della direttiva 2002/58, in combinato disposto con l'articolo 2, lettera b), della direttiva 95/46».

11 — Su entrambe le posizioni dottrinali v., ad esempio, Schreibauer, M., in *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, Esser, M., Kramer, P., e von Lewinski, K. (ed.), Carl Heymanns Verlag/Wolters Kluwer, Colonia, 2014, 4ª ed., § 11 Telemediengesetz (da 4 a 10). Nink, J., e Pohle, J.: «Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze», in *Multimedia und Recht*, 9/2015, pagg. da 563 a 567. Heidrich, J. e Wegener, C.: «Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging», in *Multimedia und Recht*, 8/2015, pagg. da 487 a 492. Leisterer, H.: «Die neuen Pflichten zur Netz – und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr», in *Computer und Recht*, 10/2015, pagg. da 665 a 670.

12 — Cit. al paragrafo 13.

13 — Cit. al paragrafo 11.

14 — È quanto ha rammentato l'avvocato generale Cruz Villalón nelle conclusioni relative alla causa Scarlet Extended (C-70/10, EU:C:2011:255, paragrafo 76) e ha dichiarato il Garante europeo della protezione dei dati nei pareri del 22 febbraio 2010, in merito ai negoziati attualmente condotti dall'Unione europea per il raggiungimento di un accordo commerciale anticontraffazione (ACTA) (GU 2010, C 147, pag. 1, punto 24), e del 10 maggio 2010, sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pedopornografia, che abroga la decisione quadro 2004/68/GAI (GU 2010, C 323, pag. 6, punto 11).

diritti dell'uomo e delle libertà fondamentali, nonché dall'articolo 7 della Carta, alla luce dei quali, nonché alla luce dell'articolo 8 della medesima Carta, deve essere interpretata la direttiva 95/46 [15]. In realtà, le parti del procedimento non mettono in discussione tale premessa, che non è neppure oggetto, di per sé, della questione pregiudiziale.

56. La persona alla quale si riferiscono le suddette informazioni non è una «persona fisica identificata». La data e l'ora di un collegamento, al pari della sua origine numerica, non rivelano, né direttamente né indirettamente, chi sia la persona fisica cui appartiene il dispositivo dal quale viene consultata la pagina web, né l'identità della persona che lo utilizza (potrebbe trattarsi di qualsiasi persona fisica).

57. Tuttavia, un indirizzo IP dinamico, nella misura in cui aiuti – di per sé o unitamente ad altri dati – ad accertare chi sia il titolare del dispositivo utilizzato per l'accesso alla pagina web, può essere considerato un'informazione su una «persona identificabile» [16].

58. Secondo l'approccio del Bundesgerichtshof (Corte federale di giustizia), l'indirizzo IP non è sufficiente, di per sé, a identificare l'utente che attraverso tale indirizzo ha consultato una pagina web. Qualora, invece, il fornitore del servizio di Internet potesse identificare l'utente attraverso l'indirizzo IP dinamico, si tratterebbe senza dubbio di un dato personale ai sensi della direttiva 95/46. Non sembra, tuttavia, che sia questo il senso della questione pregiudiziale, alla quale è sotteso che i fornitori di servizi Internet partecipanti alla controversia a qua possano identificare l'utente semplicemente in base all'indirizzo IP dinamico.

59. Associato ad altre informazioni, l'indirizzo IP dinamico consente l'identificazione «indiretta» dell'utente, idea sulla quale concordano tutti. Ci si chiede se l'eventualità che esistano tali informazioni aggiuntive, associabili all'indirizzo IP dinamico, consenta, di per sé, di qualificare quest'ultimo come dato personale ai sensi della direttiva. Si deve stabilire se sia sufficiente a tal fine la mera possibilità, in abstracto, di conoscere tali informazioni o se, al contrario, occorra che le medesime siano accessibili per un soggetto al quale è già noto l'indirizzo IP dinamico, o per un terzo.

60. Le parti hanno concentrato le loro osservazioni sull'interpretazione del considerando 26 della direttiva 95/46, di cui sottolineano l'espressione «mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona». La questione del giudice del rinvio non riguarda le informazioni aggiuntive di cui dispongono i prestatori di servizi che partecipano al procedimento principale. Né si riferisce a qualsiasi terzo che detenga tali informazioni aggiuntive (il cui incrocio con l'indirizzo IP dinamico consente di identificare l'utente), bensì al fornitore di accesso alla rete.

61. Pertanto, nel caso di specie non occorre che la Corte, per accertare se gli indirizzi IP dinamici di cui dispone la convenuta nel procedimento a quo possano essere qualificati come dati personali, esamini tutti i mezzi che la medesima potrebbe «ragionevolmente» utilizzare. Poiché il Bundesgerichtshof (Corte federale di giustizia) fa riferimento solo alle informazioni aggiuntive in

15 — V., in tal senso, sentenza del 20 maggio 2003, Österreichischer Rundfunk (C-465/00, C-138/01 e C-139/01, EU:C:2003:294, punto 68), e conclusioni dell'avvocato generale Kokott nella causa Promusicae (C-275/06, EU:C:2007:454, paragrafi 51 e segg.).

16 — Si deve presumere che, salvo prova contraria, detta persona sia quella che ha navigato su Internet e consultato la corrispondente pagina web. Tuttavia, anche prescindendo da detta presunzione, le informazioni relative alla data, all'ora e all'origine numerica dell'accesso a una pagina web consentirebbero di collegare tale accesso al titolare del dispositivo e di associarlo indirettamente alle sue modalità d'uso della rete. L'eccezione ipotizzabile sarebbe costituita dagli indirizzi IP assegnati ai computer di locali quali i cybercafé, i cui utenti anonimi non sono identificabili e nei quali il traffico generato non fornisce alcuna informazione personale rilevante sui proprietari. Si tratta peraltro dell'unica eccezione al principio secondo cui gli indirizzi IP sono dati personali ammessa dal Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dalla direttiva 95/46 (il cosiddetto «Gruppo articolo 29»). V. il suo parere 4/2007, del 20 giugno 2007, sul concetto di dati personali, WP 136, all'indirizzo http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

possesso di un terzo, si può dedurre: a) che la convenuta non possiede proprie informazioni aggiuntive che consentano l'identificazione dell'utente o b) che la convenuta, ove disponga di dette informazioni, non è in grado di utilizzarle ragionevolmente a tale scopo in qualità di responsabile del loro trattamento, ai sensi del considerando 26 della direttiva 95/46.

62. Entrambe le ipotesi dipendono da una constatazione di natura fattuale che spetta solo al giudice del rinvio. La Corte potrebbe fornirgli criteri di carattere generale per interpretare i termini «mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento», qualora il Bundesgerichtshof (Corte federale di giustizia) nutrisse dubbi in ordine alla capacità della convenuta di utilizzare ragionevolmente proprie informazioni aggiuntive. Poiché tale circostanza non ricorre, non occorre, a mio parere, che la Corte stabilisca in questa sede criteri di interpretazione che non sono necessari per il giudice del rinvio e che quest'ultimo non ha chiesto.

63. Il punto essenziale della questione sollevata è quindi soltanto se sia rilevante, per qualificare gli indirizzi IP dinamici come dati personali, la circostanza che uno specifico terzo – il fornitore di accesso a Internet – disponga di informazioni aggiuntive che, associate a detti indirizzi, siano idonee ad identificare l'utente che ha consultato una determinata pagina web.

64. Occorre nuovamente citare il considerando 26 della direttiva 95/46. I termini «mezzi che possono essere ragionevolmente utilizzati (…) *da altri*» [17] potrebbero militare a favore di un'interpretazione secondo cui sarebbe sufficiente che un terzo possa ottenere informazioni aggiuntive (suscettibili di essere associate a un indirizzo IP dinamico al fine di identificare una persona) per ritenere che tale indirizzo costituisca di per sé un dato personale.

65. Siffatta interpretazione massimalista porterebbe, in pratica, a qualificare come dato personale qualsiasi tipo di informazione, ancorché insufficiente di per sé a consentire l'identificazione di un utente. Non si potrebbe mai escludere con assoluta certezza che non esista un terzo in possesso di informazioni aggiuntive associabili a tale informazione e idonee, pertanto, a rivelare l'identità di una persona.

66. A mio parere, la possibilità che il progresso dei mezzi tecnici agevoli sensibilmente, in un futuro più o meno prossimo, l'accesso a strumenti sempre più sofisticati per ottenere e trattare le informazioni giustifica la cautela con cui si intende predisporre la tutela della vita privata. Si è cercato di fare in modo che, per definire le categorie giuridiche rilevanti nel contesto della protezione dei dati, siano prese in considerazione ipotesi di comportamento sufficientemente ampie e flessibili da garantire la copertura di qualsiasi situazione immaginabile [18].

67. Ritengo, tuttavia, che tale preoccupazione – peraltro legittima – non possa condurre ad ignorare la volontà del legislatore e il fatto che l'interpretazione sistematica del considerando 26 della direttiva 95/46 è circoscritta ai «mezzi che possono essere ragionevolmente utilizzati» *da taluni terzi*.

68. Atteso che il considerando 26 non fa riferimento a qualsiasi mezzo utilizzabile dal responsabile del trattamento (nella fattispecie, il fornitore di servizi Internet), ma solo a quelli che quest'ultimo può utilizzare «ragionevolmente», si deve parimenti ritenere che il legislatore si riferisca agli «altri» che, *in modo altrettanto ragionevole*, possano assistere il responsabile del trattamento che intende ottenere le informazioni aggiuntive ai fini dell'identificazione. Non sarà così quando il contatto con tali altri sia, di fatto, molto costoso in termini umani ed economici, o praticamente irrealizzabile o vietato dalla legge.

17 — Senza corsivo nell'originale.

18 — Tale inclinazione cautelare e preventiva è alla base della posizione assunta dal Gruppo articolo 29, secondo cui, come detto, occorre muovere dal principio secondo cui gli indirizzi IP costituiscono dati personali, ammettendo come unica eccezione l'ipotesi in cui il fornitore del servizio sia in grado di stabilire con assoluta certezza che si tratta di indirizzi corrispondenti a persone non identificabili, quali possono essere gli utenti di un cybercafé. V. supra, nota 16 in fine.

Diversamente ragionando, come ho rilevato in precedenza, sarebbe praticamente impossibile distinguere un mezzo dall'altro, in quanto si potrebbe sempre prospettare l'ipotesi contingente di un terzo che, per quanto inaccessibile al prestatore di servizi Internet, possa disporre - attualmente o in futuro – di informazioni aggiuntive pertinenti per concorrere all'identificazione di un utente.

69. Come ho anticipato, il terzo cui fa riferimento il Bundesgerichtshof (Corte federale di giustizia) è un fornitore di accesso alla rete. Certamente, è ragionevole pensare che sia questo il terzo cui il fornitore di servizi si rivolgerà per ottenere le informazioni aggiuntive necessarie, se vuole identificare in modo efficace, pratico e diretto l'utente che ha consultato la sua pagina web attraverso l'indirizzo IP dinamico. Non si tratta affatto di un terzo ipotetico, ignoto e inaccessibile, bensì di uno degli attori principali nell'ambito di Internet, di cui si sa con certezza che detiene le informazioni necessarie al prestatore di servizi per identificare un utente. Di fatto, come indicato dal giudice del rinvio, è a tale specifico terzo che la convenuta intende rivolgersi nel procedimento principale per ottenere le informazioni aggiuntive che le occorrono.

70. Il fornitore di accesso a Internet è, generalmente, il terzo cui fa riferimento il considerando 26 della direttiva 95/46, al quale può rivolgersi nel modo più «ragionevole» il prestatore di servizi di cui al procedimento a quo. Resta da stabilire, tuttavia, se l'ottenimento delle informazioni aggiuntive di cui dispone detto terzo possa essere considerato «ragionevolmente» possibile o realizzabile.

71. Il governo tedesco sostiene che, poiché le informazioni di cui dispone il fornitore di accesso a Internet sono dati personali, quest'ultimo non può trasmetterle incondizionatamente, ma solo rispettando la normativa che disciplina il trattamento di tali dati [19].

72. Ciò è senz'altro vero, dato che, per utilizzare tali informazioni, occorre attenersi alla normativa applicabile ai dati personali. Si possono ottenere le informazioni «ragionevolmente» solo se rispettano le condizioni relative all'accesso a questo tipo di dati, la prima delle quali è la possibilità giuridica di conservarli e trasmetterli ad altri. Certamente, il fornitore di accesso a Internet può rifiutarsi di fornire i dati in questione, ma può anche accadere il contrario. La possibilità di trasmissione dei dati, perfettamente «ragionevole», trasforma di per sé stessa l'indirizzo IP dinamico in un dato personale per il prestatore di servizi Internet, ai sensi del considerando 26 della direttiva 95/46.

73. Si tratta di un'eventualità possibile *nei limiti della legge* e, pertanto, «ragionevole». I mezzi di accesso ragionevoli ai quali fa riferimento la direttiva 95/46 devono essere, per definizione, mezzi leciti [20]. Tale è la premessa da cui muove, ovviamente, il giudice del rinvio, come ha ricordato il governo tedesco [21]. Si riducono così in misura significativa le modalità di accesso giuridicamente rilevanti, che possono essere esclusivamente quelle lecite. Ma se tali modalità esistono, per quanto restrittiva possa esserne l'applicazione pratica, esse presuppongono un «mezzo ragionevole» ai sensi della direttiva 95/46.

74. Di conseguenza, ritengo che si debba rispondere in senso affermativo alla prima questione, come formulata dal Bundesgerichtshof (Corte federale di giustizia). L'indirizzo IP dinamico deve essere qualificato, per il fornitore di servizi Internet, come un dato personale, tenuto conto dell'esistenza di un terzo (il fornitore di accesso alla rete) al quale detto fornitore può ragionevolmente rivolgersi per ottenere informazioni aggiuntive che, incrociate con tale dato, consentono l'identificazione di un utente.

19 — Punti 40 e 45 delle sue osservazioni scritte.

20 — Nel presente contesto è irrilevante la circostanza che sia possibile, de facto, accedere al dato personale violando le leggi sulla protezione dei dati.

21 — Punti 47 e 48 delle sue osservazioni scritte.

75. Credo che il risultato cui condurrebbe la soluzione contraria corrobori quella da me proposta. Se gli indirizzi IP dinamici non costituissero dati personali per il fornitore di servizi Internet, quest'ultimo potrebbe conservarli indefinitamente e chiedere in qualsiasi momento al fornitore di accesso a Internet le informazioni aggiuntive per associarle a detti indirizzi e identificare l'utente. In tali circostanze, come riconosce il governo tedesco [22], l'indirizzo IP dinamico diventerebbe un dato personale, in quanto sarebbero già disponibili le informazioni aggiuntive necessarie per identificare l'utente, e si applicherebbe al riguardo la normativa in materia di protezione dei dati.

76. Orbene, si tratterebbe di un dato la cui conservazione sarebbe possibile solo nella misura in cui esso non sia stato considerato, fino a quel momento, come un dato personale per il prestatore di servizi. Sarebbe quindi quest'ultimo a determinare la qualificazione giuridica dell'indirizzo IP dinamico come dato personale, qualora decida, in un successivo momento, di utilizzarlo per identificare l'utente associandolo alle informazioni aggiuntive che dovrà ottenere da un terzo. A mio parere, tuttavia, l'elemento decisivo, ai sensi della direttiva 95/46, è la possibilità - ragionevole – dell'esistenza di un terzo «accessibile», che disponga dei mezzi necessari per l'identificazione di una persona, e non il fatto che la possibilità di ricorrere a tale terzo si realizzi.

77. Si potrebbe anche riconoscere, con il governo tedesco, che l'indirizzo IP dinamico diventa un dato personale solo nel momento in cui viene ricevuto dal fornitore di accesso a Internet. In tal caso, tuttavia, si dovrebbe accettare che tale qualificazione abbia efficacia retroattiva ai fini della decorrenza del termine di conservazione dell'indirizzo IP e, pertanto, considerarla inesistente qualora sia stato superato il periodo per il quale detto indirizzo avrebbe potuto essere conservato ove fosse stato qualificato fin dal principio come dato personale. In tal caso, il risultato sarebbe contrario allo spirito della legislazione in materia di protezione dei dati personali. La ragione che giustifica la conservazione solo temporanea di tali dati sarebbe vanificata dall'eventuale perdurare della rilevanza di una qualità che è loro inerente fin dall'inizio: la possibilità di costituire un mezzo di identificazione – di per sé o mediante l'aggregazione con altri dati – di una persona fisica. Anche per questo motivo, di pura economia, è più ragionevole attribuire loro tale natura fin dal principio.

78. Pertanto, come prima conclusione, ritengo che l'articolo 2, lettera a), della direttiva 95/46 debba essere interpretato nel senso che un indirizzo IP memorizzato da un prestatore di servizi in relazione a un accesso alla sua pagina web costituisce per quest'ultimo un dato personale se un fornitore di accesso alla rete (Internet) dispone delle informazioni aggiuntive necessarie ai fini dell'identificazione della persona interessata.

B – *Seconda questione*

79. Con la seconda questione pregiudiziale, il Bundesgerichtshof (Corte federale di giustizia) intende sapere se l'articolo 7, lettera f), della direttiva 95/46 osti a una normativa nazionale che ammette la raccolta e l'utilizzo dei dati personali di un utente, senza il suo consenso, solo nella misura in cui ciò sia necessario per consentire l'effettiva fruizione del servizio di telecomunicazione da parte del rispettivo utente e per fatturarla, senza che il fine di assicurare il funzionamento in generale di detto servizio possa giustificare l'utilizzazione dei dati oltre il termine della rispettiva fruizione.

80. Prima di rispondere, occorre formulare una precisazione circa le informazioni fornite dal Bundesgerichtshof (Corte federale di giustizia), secondo le quali i dati controversi vengono conservati per garantire il corretto funzionamento dei siti Internet di cui al procedimento principale, il che rende possibile, ove necessario, reprimere penalmente gli attacchi informatici di cui detti siti siano eventualmente oggetto.

22 — Punto 36 delle sue osservazioni scritte.

81. Occorre quindi chiedersi, anzitutto, se il trattamento degli indirizzi IP ai quali si riferisce la questione pregiudiziale rientri nella deroga prevista dall'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46 [23].

1. Sull'applicabilità della direttiva 95/46 al trattamento dei dati controversi

82. Nel procedimento principale, la Repubblica federale di Germania agisce, a quanto sembra, in qualità di mero fornitore di servizi Internet, vale a dire in veste di privato (e, pertanto, sine imperio). Se ne deduce che, in linea di principio, il trattamento dei dati controversi non esula dall'ambito di applicazione della direttiva 95/46.

83. Per riprendere i termini utilizzati dalla Corte nella sentenza Lindqvist [24], le attività di cui all'articolo 3, paragrafo 2, della direttiva 95/46 «sono, in tutti i casi, attività proprie degli Stati o delle autorità statali ed estranee ai settori di attività dei singoli» [25]. Poiché il responsabile del trattamento dei dati controversi è un soggetto che, nonostante la sua qualità di pubblica autorità, agisce in realtà come privato, è applicabile la direttiva 95/46.

84. Il giudice del rinvio, ponendo in rilievo lo scopo principale perseguito dall'Amministrazione tedesca mediante la memorizzazione degli indirizzi IP dinamici, sottolinea che essa mira a «garantire e mantenere la sicurezza e il funzionamento dei suoi servizi di telecomunicazione», in particolare favorire «l'individuazione e il contrasto di attacchi del tipo "denial of service" che si verificano frequentemente, per effetto dei quali l'infrastruttura di telecomunicazione viene bloccata da un flusso mirato e coordinato proveniente da singoli web server attraverso una molteplicità di richieste di accesso» [26]. La conservazione a tale scopo degli indirizzi IP dinamici è comune a qualsiasi titolare di siti Internet di una certa importanza e non implica, né direttamente né indirettamente, l'esercizio di pubblici poteri, cosicché la sua inclusione nell'ambito della direttiva 95/46 non solleva troppe difficoltà.

85. Il Bundesgerichtshof (Corte federale di giustizia) afferma, tuttavia, che la conservazione degli indirizzi IP dinamici da parte dei prestatori di servizi che partecipano al procedimento principale risponde altresì all'obiettivo di perseguire penalmente, se del caso, gli autori di eventuali attacchi informatici. Siffatto obiettivo è sufficiente per escludere il trattamento di tali dati dall'ambito di applicazione della direttiva 95/46?

86. A mio parere, se per «perseguimento penale» si intende l'esercizio dello ius puniendi dello Stato da parte dei prestatori di servizi convenuti nel procedimento principale, ci troviamo di fronte a un'«attività dello Stato in materia di diritto penale» e, pertanto, ad una delle eccezioni previste dall'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46.

87. In tali circostanze, conformemente alla giurisprudenza elaborata dalla Corte nella causa Huber [27], il trattamento dei dati personali da parte dei prestatori di servizi, ai fini della sicurezza e del funzionamento tecnico dei loro servizi di telecomunicazione, rientrerebbe nel campo di applicazione della direttiva 95/46, mentre il trattamento dei dati connesso all'attività dello Stato in materia di diritto penale ne resterebbe escluso.

23 — Non rientrano nell'ambito di applicazione della direttiva 95/46 i «trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (…) e le *attività dello Stato in materia di diritto penale*» (senza corsivo nell'originale).

24 — Sentenza del 6 novembre 2003 (C-101/01, EU:C:2003:596, punto 43).

25 — V., nello stesso senso, sentenza del 16 dicembre 2008, Satakunnan Markkinapörssi e Satamedia (C-73/07, EU:C:2008:727, punto 41).

26 — Punto 36 dell'ordinanza di rinvio.

27 — Sentenza del 16 dicembre 2008 (C-524/06, EU:C:2008:724, punto 45).

88. Allo stesso modo, quand'anche l'attività in materia di diritto penale propriamente detta non spettasse alla Repubblica federale di Germania, in quanto mero prestatore di servizi privo di potere d'imperio, e quest'ultima si limitasse, al pari di qualsiasi privato, a trasmettere gli indirizzi IP controversi ad un organo statale affinché eserciti un'azione repressiva, il trattamento degli indirizzi IP dinamici avrebbe comunque ad oggetto un'attività che esula dall'ambito della direttiva 95/46.

89. Ciò emerge dalla sentenza Parlamento/Consiglio e Commissione [28], in cui la Corte ha dichiarato che il fatto che determinati dati personali «sono raccolti da operatori privati a fini commerciali e che sono questi ultimi ad organizzarne il trasferimento ad uno Stato terzo» non implica che tale trasferimento «non rientri nell'ambito di applicazione» dell'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46 quando il trasferimento riguardi le attività dello Stato in materia di diritto penale, dato che, in tal caso, detto trasferimento «rientra in un ambito istituito dai poteri pubblici e attinente alla pubblica sicurezza» [29].

90. Al contrario, se, come credo, per «perseguimento penale» si deve intendere, come si evince dall'ordinanza di rinvio, quella propria di un singolo in quanto soggetto legittimato a chiedere l'esercizio dello ius puniendi dello Stato, mediante l'azione corrispondente, allora non si può sostenere che il trattamento degli indirizzi IP dinamici attenga all'attività dello Stato in materia di diritto penale, che esula dall'ambito di applicazione della direttiva 95/46.

91. Infatti, la memorizzazione e la conservazione di tale dato servirebbero come ulteriore mezzo di prova con cui il titolare della pagina web chiede allo Stato di reprimere, su istanza di parte, un comportamento illecito. Si tratterebbe, in definitiva, di un mezzo per tutelare, penalmente, i diritti conferiti dall'ordinamento a uno specifico soggetto (nella fattispecie, a un ente pubblico che agisce in regime di diritto privato). Tale strumento non si differenzia, sotto quest'aspetto, dall'iniziativa di qualsiasi altro fornitore di servizi Internet che chieda la protezione dello Stato secondo le modalità di esercizio dell'azione penale previste dall'ordinamento.

92. Di conseguenza, se l'Amministrazione tedesca agisce in qualità di fornitore di servizi Internet, privo di pubblici poteri, circostanza la cui valutazione spetta al giudice del rinvio, il suo trattamento degli indirizzi IP dinamici, in quanto dati personali, rientra nell'ambito di applicazione della direttiva 95/46.

2. Sul merito

93. L'articolo 15, paragrafo 1, del TMG consente la raccolta e l'utilizzo dei dati personali di un utente solo nella misura in cui ciò sia necessario per offrire e fatturare l'effettiva fruizione del servizio di telecomunicazione. Più esattamente, il fornitore di servizi può raccogliere e utilizzare i cosiddetti «dati di utenza», vale a dire i dati personali di un utente, necessari per rendere possibile «la fruizione di servizi di telecomunicazione e per fatturarla». Tali dati devono essere eliminati al termine dell'operazione (cioè al termine della fruizione del servizio di telecomunicazione), salvo che debbano essere conservati «a fini di fatturazione» ai sensi del paragrafo 4 del medesimo articolo 15 del TMG.

28 — Sentenza del 30 maggio 2006 (C-317/04 e C-318/04, EU:C:2006:346, punti da 54 a 59).

29 — Ibidem, punto 59. Detta causa verteva su dati personali il cui trattamento era necessario per la prestazione di servizi costituente l'attività degli operatori privati interessati (compagnie aeree), ma che questi ultimi dovevano trasmettere alle autorità statunitensi a fini di prevenzione e lotta contro il terrorismo.

94. L'articolo 15 del TMG sembra escludere la possibilità che, una volta concluso il collegamento, i dati di utenza possano essere conservati per altri motivi, anche qualora ciò servisse a garantire «la fruizione dei servizi di telecomunicazione» in generale. Dal momento che menziona esclusivamente i fini di fatturazione come motivo idoneo a giustificare la conservazione dei dati, la suddetta disposizione del TMG potrebbe essere intesa (anche se la sua interpretazione definitiva spetta al giudice del rinvio) nel senso che i dati di utenza possono essere utilizzati solo per rendere possibile uno specifico rapporto e devono essere eliminati al termine dello stesso.

95. L'articolo 7, lettera f), della direttiva 95/46 [30] legittima il trattamento di dati personali in termini che definirei più generosi (per il responsabile del trattamento) rispetto a quelli del testo dell'articolo 15 del TMG. La norma tedesca può essere considerata, sotto tale aspetto, più restrittiva di quella dell'Unione, in quanto non contempla, in linea di principio, il perseguimento di interessi legittimi diversi da quello connesso alla fatturazione del servizio, mentre la Repubblica federale di Germania, in qualità di fornitore di servizi Internet, potrebbe avere anche un interesse legittimo a garantire il corretto funzionamento delle sue pagine web oltre il termine di ciascuna fruizione [31].

96. La giurisprudenza elaborata dalla Corte nella sentenza ASNEF e FECEMD [32] offre la chiave per rispondere alla seconda questione pregiudiziale. La Corte ha dichiarato in quell'occasione che dall'obiettivo perseguito dalla direttiva 95/46 «deriva che l'[articolo] 7 della direttiva 95/46 prevede un elenco esaustivo e tassativo dei casi in cui il trattamento dei dati personali può essere considerato lecito» [33]. Ne consegue che «gli Stati membri non possono né aggiungere nuovi principi relativi alla legittimazione del trattamento dei dati personali all'[articolo] 7 della direttiva 95/46, né prevedere requisiti supplementari che vengano a modificare la portata di uno dei sei principi previsti da detto articolo» [34].

97. L'articolo 15 del TMG non aggiunge un requisito supplementare a quelli cui l'articolo 7 della direttiva 95/46 subordina la liceità del trattamento dei dati – come accadeva nelle cause ASNEF e FECEMD - [35], ma, ove sia interpretato nel senso restrittivo indicato dal giudice a quo, riduce il contenuto della condizione di cui alla lettera f) del medesimo articolo: mentre il legislatore dell'Unione fa riferimento, in generale, al perseguimento «(…) dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati», l'articolo 15 del TMG contempla solo la necessità di «rendere possibile la [effettiva] fruizione di servizi di telecomunicazione e di fatturarla».

98. Come accadeva nelle cause ASNEF e FECEMD [36], anche nel presente caso una misura nazionale – sempre che la si interpreti nel senso restrittivo sopra illustrato – modificherebbe la portata di un principio stabilito dall'articolo 7 della direttiva 95/46, anziché limitarsi a precisarlo, che è l'unico aspetto sul quale le autorità degli Stati membri dispongono di un certo margine di discrezionalità, in virtù dell'articolo 5 della direttiva 95/46.

30 — Cit. supra, al paragrafo 17.

31 — V. supra, paragrafo 84. Certamente, i titolari delle pagine web hanno un interesse legittimo a prevenire e contrastare le «denials of service» menzionate dal giudice del rinvio, vale a dire attacchi massicci lanciati occasionalmente contro alcuni siti web per saturarli e renderli inoperanti.

32 — Sentenza del 24 novembre 2011 (C-468/10 e C-469/10, EU:C:2011:777).

33 — Ibidem (punto 30).

34 — Ibidem (punto 32).

35 — Fattispecie in cui la normativa nazionale aggiungeva ai requisiti previsti dall'articolo 7, lettera f), della direttiva 95/46 la condizione secondo la quale i dati oggetto del trattamento dovevano essere contenuti in fonti accessibili al pubblico.

36 — Sentenza del 24 novembre 2011 (C-468/10 e C-469/10, EU:C:2011:777).

99. Infatti, secondo quest'ultima disposizione, «[g]li Stati membri precisano, nei limiti delle disposizioni del presente capo [37], le condizioni alle quali i trattamenti di dati personali sono leciti». Tuttavia, come è stato dichiarato nelle cause ASNEF e FECEMD[38], «a norma [di detta disposizione], gli Stati membri non possono neppure introdurre principi relativi alla legittimazione del trattamento dei dati personali diversi da quelli enunciati all'[articolo] 7 di tale direttiva, né modificare con requisiti supplementari la portata dei sei principi previsti dal detto [articolo] 7».

100. L'articolo 15 del TMG ridurrebbe in misura sostanziale, rispetto all'articolo 7, lettera f), della direttiva 95/46, il perimetro dell'interesse legittimo idoneo a giustificare il trattamento dei dati, anziché limitarsi a precisarlo o modularlo entro i limiti consentiti dall'articolo 5 della medesima direttiva. Lo farebbe, inoltre, in modo categorico e assoluto, senza permettere che la tutela e la garanzia della fruizione in generale del servizio di telecomunicazione possano essere raffrontate con «l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1» della direttiva 95/46, come previsto dall'articolo 7, lettera f), della stessa.

101. In definitiva, come nelle cause ASNEF e FECEMD[39], il legislatore federale tedesco avrebbe stabilito «per [talune categorie di dati personali], in modo definitivo, il risultato della ponderazione dei diritti e degli interessi contrapposti, senza consentire un diverso risultato in ragione delle circostanze specifiche del caso concreto», cosicché la normativa in parola «non può essere definita in termini di precisazione, ai sensi [dell'articolo] 5» della direttiva 95/46.

102. Ciò posto, ritengo che il Bundesgerichtshof (Corte federale di giustizia) debba interpretare la normativa nazionale in modo conforme alla direttiva 95/46, il che implica: a) che si possa includere tra i motivi che giustificano il trattamento dei cosiddetti «dati di utenza» l'interesse legittimo del fornitore di servizi di telecomunicazione a tutelare la fruizione di tali servizi in generale e b) che si possa ponderare, ad casum, tale interesse del fornitore del servizio, raffrontandolo con l'interesse o con i diritti e le libertà fondamentali dell'utente per stabilire quale sia quello meritevole di tutela ai sensi dell'articolo 1, paragrafo 1, della direttiva 95/46[40].

103. Non occorre aggiungere altro, a mio avviso, sul modo in cui tale ponderazione va effettuata nel procedimento che ha dato origine al rinvio pregiudiziale. Nulla chiede al riguardo il Bundesgerichtshof (Corte federale di giustizia), cui preme risolvere una questione preliminare a tale giudizio di ponderazione, vale a dire se siffatto giudizio sia possibile.

104. Infine, è appena il caso di rilevare che il giudice a quo potrà tenere conto delle eventuali disposizioni di legge adottate dallo Stato membro nell'ambito dell'autorizzazione di cui all'articolo 13, paragrafo 1, lettera d), della direttiva 95/46, per restringere la portata degli obblighi e dei diritti previsti dall'articolo 6 della medesima direttiva, qualora ciò sia necessario per la salvaguardia, tra altri interessi, «(…) della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali (…)». Il giudice del rinvio, indubbiamente consapevole dell'esistenza delle due disposizioni, non fa riferimento neppure a tale ipotesi.

105. Di conseguenza, suggerisco di rispondere alla seconda questione pregiudiziale dichiarando che l'articolo 7, lettera f), della direttiva 95/46 osta a una norma nazionale la cui interpretazione impedisca a un prestatore di servizi di raccogliere e trattare i dati personali di un utente, senza il suo consenso, al termine di ciascuna fruizione, al fine di garantire il funzionamento del servizio di telecomunicazione.

37 — Capo II, intitolato «Condizioni generali di liceità dei trattamenti di dati personali», che contiene gli articoli da 5 a 21 della direttiva 95/46.

38 — Sentenza del 24 novembre 2011 (C-468/10 e C-469/10, EU:C:2011:777, punto 36).

39 — Ibidem (punto 47).

40 — All'udienza, il difensore del sig. Breyer ha negato che la memorizzazione degli indirizzi IP dinamici sia necessaria per tutelare il corretto funzionamento dei servizi Internet contro eventuali attacchi. Non credo che si possa rispondere in termini assoluti a tale questione, la cui soluzione, al contrario, dovrebbe essere preceduta, in ciascun caso di specie, dal raffronto tra l'interesse del titolare del sito Internet e i diritti e interessi degli utenti.

VI – **Conclusione**

106. Alla luce di quanto sopra, propongo alla Corte di rispondere nei termini seguenti alle questioni sollevate:

«1) Ai sensi dell'articolo 2, lettera a), della direttiva 95/46/CE 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, un indirizzo IP dinamico, mediante il quale un utente ha visitato la pagina web di un fornitore di servizi di telecomunicazione, costituisce per quest'ultimo un "dato personale" se un fornitore di accesso alla rete dispone di informazioni aggiuntive che, associate all'indirizzo IP dinamico, consentono l'identificazione dell'utente.

2) L'articolo 7, lettera f), della direttiva 95/46 deve essere interpretato nel senso che l'obiettivo di garantire il funzionamento del servizio di telecomunicazione può, in linea di principio, essere considerato un interesse legittimo, il cui perseguimento giustifica il trattamento del suddetto dato personale, qualora sia ritenuto prevalente rispetto all'interesse o ai diritti fondamentali dell'interessato. Una disposizione nazionale che non permettesse di prendere in considerazione tale interesse legittimo sarebbe incompatibile con la suddetta disposizione».