

Flaminia Merla

L'INDIRIZZO IP DINAMICO QUALE DATO PERSONALE

Estratto



Milano • Giuffrè Editore

CORTE GIUSTIZIA UE

SEZIONE II

19 OTTOBRE 2016

CAUSA C-582/14

PRESIDENTE: ILESIC

RELATORE: ROSAS

AVV. GENERALE: CAMPOS
SÀNCHEZ-BORDONAPARTI: BREYER
BUNDESREPUBLIK
DEUTSCHLAND

• Trattamento dei dati personali • Direttiva 95/46/CE • Indirizzo IP • Nozione di “dato personale”

L'articolo 2, lettera a), della direttiva 95/46 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, dev'essere interpretato nel senso che un indirizzo di protocollo Internet dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale ai sensi di detta disposizione, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone.

• Trattamento dei dati personali • Direttiva 95/46/CE • Indirizzi IP • Liceità della conservazione da parte di un fornitore di servizi di media online • Interesse legittimo perseguito dal responsabile del trattamento

L'articolo 7, lettera f), della direttiva 95/46 dev'essere interpretato nel senso che osta a una normativa di uno Stato membro ai sensi della quale un fornitore di servizi di media online può raccogliere e impiegare dati personali di un utente di tali servizi, in mancanza del suo consenso, solo nella misura in cui detta raccolta e detto impiego siano necessari per consentire e fatturare l'effettiva fruizione dei suddetti servizi da parte dell'utente in questione, senza che l'obiettivo di assicurare il funzionamento generale dei medesimi servizi possa giustificare l'impiego di tali dati dopo una sessione di consultazione degli stessi.

L'INDIRIZZO IP DINAMICO QUALE DATO PERSONALE

Il sig. Patrick Breyer si oppone innanzi ai giudici tedeschi alla registrazione e alla conservazione del suo indirizzo di protocollo Internet (indirizzo IP)¹ da parte dei siti Internet dei servizi federali tedeschi da lui consultati. Tali servizi registrano e conservano in qualità di soggetti privati, oltre alla data e

* Il testo della sentenza è stato pubblicato su questa *Rivista*, 2016, 748.

¹ L'indirizzo IP (Internet Protocol address) è un indirizzo numerico costituito da un insieme di 32 bit con il valore decimale dei quattro bytes che lo compongono (es. 100.115.180.145) ad ogni indirizzo così rappresentato corrisponde un unico host sulla rete. Per host deve intendersi un computer collegato a una rete di cui costituisce il nodo e un terminale per l'accesso a determinati

servizi. Cfr. P. SAMMARCO, *Il regime giuridico dei «nomi di dominio»*, Milano, 2002; G. PASCUZZI, *Il diritto dell'era digitale*, Bologna, 2010, 272; v. Jon Postel ed., Internet Protocol, RFC 791, settembre 1981, <http://www.faqs.org/rfcs/rfc791.html>. V. anche conclusioni dell'avvocato generale Kokott nella causa C-275/06, Promusicae c/ Telefónica de España, sentenza 29.1.08, paragrafi 30 e 31.

all'ora della consultazione, gli indirizzi IP dei visitatori al fine di difendersi dagli attacchi cibernetici² e di rendere possibili le azioni penali.

La Repubblica federale di Germania si è rivolta alla Corte di giustizia per sapere se gli indirizzi IP dinamici³ costituiscano anch'essi, per il gestore del sito Internet consultato, un dato personale, e godano quindi della tutela prevista per simili dati.

Un indirizzo IP dinamico è un indirizzo IP che cambia a ogni nuova connessione a Internet. A differenza degli indirizzi IP statici⁴ gli indirizzi IP dinamici non consentono di associare, attraverso file accessibili al pubblico, un certo computer al collegamento fisico alla rete utilizzato dal fornitore di accesso a Internet. Pertanto, solo il fornitore di accesso a Internet del sig. Breyer dispone delle informazioni aggiuntive necessarie per identificarlo.

Con la prima questione pregiudiziale, il giudice del rinvio chiede se l'articolo 2, lettera a), della direttiva 95/46 debba essere interpretato nel senso che un indirizzo IP memorizzato da un fornitore di servizi di media online, in relazione ad un accesso al suo sito Internet, costituisce per quest'ultimo un dato personale qualora sia un terzo (nel caso di specie: un fornitore di accesso) a disporre delle informazioni aggiuntive necessarie ai fini dell'identificazione della persona interessata.

Con la seconda questione pregiudiziale, il giudice del rinvio chiede se l'articolo 7, lettera f), della direttiva 95/46 debba essere interpretato nel senso che osta a una normativa di uno Stato membro ai sensi della quale un fornitore di servizi di media online può raccogliere e impiegare dati personali di un utente di tali servizi, in mancanza del suo consenso, solo nella misura in cui detta raccolta e detto impiego siano necessari per

² La pirateria su Internet è un problema a cui sono state date risposte diversificate nei vari paesi, per lo più giudiziarie. Cfr. *A&M Records c/ Napster*, 239 F.3d 1004, 2001; *Metro-Goldwyn-Mayer Studios c/ Grokster*, 125 S. Ct. 2764, 2005 negli Stati Uniti; *Kazaa BV e StreamCast Network 2005*, F. C. A. 1242; o talvolta legislative; v. anche la relazione dalla Commissione sull'applicazione 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, del 21 novembre 2003, COM(2003) 702 def., punto 4.7; la relazione della Commissione sull'applicazione della direttiva 2004/48/CE del Parlamento europeo e del Consiglio del 29 aprile 2004 sul rispetto dei diritti di proprietà intellettuale, del 22 dicembre 2010 [COM(2010) 779 def., punto 3.3], nonché la sua comunicazione del 16 luglio 2008, «Una strategia europea in materia di diritti di proprietà industriale», COM (2008) 465 def., punto 5.3.

³ Gli indirizzi IP dinamici sono utilizzati per identificare dispositivi non permanenti in una rete. Un server presente nella

rete assegna dinamicamente e automaticamente l'indirizzo scegliendolo casualmente da un range preimpostato. Si può scegliere l'intervallo di indirizzi a seconda del numero delle utenze della rete impostando la maschera di sotto rete, ossia dicendo al server quanti bit dell'indirizzo sono assegnabili dinamicamente a ogni singolo client che fa accesso. Per esempio, se la maschera di sotto rete ha valore 255.255.255.0 (dove ogni blocco separato da puntini denota un gruppo di 8 bit) solo gli ultimi 8 bit sono assegnabili agli host., reperibile al sito internet https://it.wikipedia.org/wiki/Indirizzo_IP#Indirizzi_dinamici.

⁴ Gli indirizzi IP statici vengono utilizzati per identificare dispositivi semi-permanenti con indirizzo IP permanente. Tipicamente si può ricorrere anche ad un'assegnazione statica anziché dinamica per dispositivi di rete non permanenti se il numero di host della sottorete è contenuto e/o per motivi di sicurezza potendo tenere sotto controllo le azioni di ciascun host e del relativo utente. L'assegnazione di un IP statico rende però il dispositivo più soggetto ad attacchi informatici reperibile al sito internet https://it.wikipedia.org/wiki/Indirizzo_IP#Indirizzi_dinamici.

consentire e fatturare l'effettiva fruizione dei suddetti servizi da parte dell'utente in questione, senza che l'obiettivo di assicurare il funzionamento generale dei medesimi servizi possa giustificare l'impiego di tali dati dopo una sessione di consultazione degli stessi.

1. L'ILLEGITTIMO TRATTAMENTO DEI DATI LAMENTATO DAL SIG. BREYER.

1.1. Il trattamento dei dati del sig. Breyer.

Il sig. Breyer ha consultato alcuni siti Internet, gestiti dai servizi federali tedeschi in qualità di soggetti privati, che forniscono informazioni aggiornate.

Gli accessi a questi siti sono registrati nei file di registro, i dati memorizzati sono il nome del sito, il file consultato, le parole inserite nei campi di ricerca, la data e l'ora della consultazione, il volume dei dati trasferiti, il messaggio relativo all'esito della consultazione e l'indirizzo IP del computer dal quale è stato effettuato l'accesso; tale memorizzazione e conservazione dei dati stessi avviene anche successivamente alla sessione di consultazione dei siti al fine di contrastare attacchi e consentire il perseguimento penale di attacchi cybernetici.

In caso di consultazione di un sito Internet l'indirizzo IP del computer che effettua l'accesso è trasmesso al server che ospita il sito consultato; questa comunicazione è necessaria per inviare i dati richiesti al corretto destinatario. Gli indirizzi IP dinamici, a differenza di quelli statici, non consentono di associare un dato computer al collegamento fisico alla rete utilizzato dal fornitore di accesso a Internet.

Il sig. Breyer ha proposto un ricorso dinanzi ai giudici amministrativi tedeschi chiedendo che alla Repubblica federale di Germania sia inibito di conservare o far conservare da terzi, al termine delle sessioni di consultazione dei siti accessibili al pubblico di media online dei servizi federali tedeschi, l'indirizzo IP del nodo ospite del sig. Breyer, qualora tale conservazione non sia necessaria, in caso di guasto, al ripristino della diffusione di detti media.

Tale domanda è stata rigettata in primo grado e conseguentemente il sig. Breyer ha proposto appello avverso tale decisione. Il giudice di appello ha parzialmente riformato la sentenza condannando la Repubblica federale di Germania ad astenersi dal conservare o dal far conservare da terzi, al termine di ogni consultazione, l'indirizzo IP del nodo ospite del sig. Breyer.

Infatti l'indirizzo IP del sig. Breyer viene trasmesso all'atto della consultazione dei siti di media online dei servizi federali tedeschi e, nel caso in cui tale indirizzo sia conservato unitamente alla data della sessione di consultazione alla quale si riferisce e qualora lo stesso abbia fornito la propria identità — anche semplicemente con un indirizzo di posta elettronica che menzioni la sua identità — ove tale conservazione non sia necessaria in caso di guasto al ripristino della diffusione di media online, essa deve essere inibita.

Il suddetto giudice di appello ha ritenuto che l'indirizzo IP dinamico fosse un dato personale solo ed esclusivamente nel caso in cui l'utente abbia rivelato la sua identità in sede di consultazione, come nel caso del sig. Breyer.

La Repubblica federale di Germania ritiene che, nella sua qualità di fornitore di servizi di media online, l'indirizzo IP non sarebbe un dato

personale neppure se associato alla data della sessione di consultazione alla quale esso si riferisce, dato che l'utente dei siti Internet considerati non sarebbe identificabile da parte di tale Stato membro.

Ciò posto sia il sig. Breyer che la Repubblica federale di Germania hanno proposto un ricorso per "Revision" (cassazione) dinanzi al Bundesgerichtshof (Corte federale di giustizia, Germania) avverso la decisione del giudice di appello.

Il sig. Breyer ha chiesto l'accoglimento integrale della sua domanda inibitoria, di contro la Repubblica federale di Germania chiede il rigetto di tale domanda.

Il giudice del rinvio ha precisato che gli indirizzi IP dinamici del computer del sig. Breyer, conservati dalla Repubblica federale di Germania quando agisce privatamente come fornitore di media online, non consentirebbero di determinare direttamente l'identità del sig. Breyer. Infatti, gli operatori di tali siti Internet potrebbero identificare il sig. Breyer solamente se il fornitore di accesso a Internet del medesimo trasmettesse loro informazioni sull'identità di detto utente. La qualificazione di tali dati come personali dipenderebbe, di conseguenza, dalla possibilità o meno di identificare il sig. Breyer.

La condotta violata, a detta del sig. Breyer, risiede nella circostanza che dalla combinazione dei dati relativi agli indirizzi IP del fornitore di accesso alla rete e quelli del fornitore dei media on-line si potrebbe risalire alla sua identità personale e, conseguentemente, vi sarebbe un trattamento illecito degli stessi.

Il diritto interno di ogni singolo Stato deve offrire una certa protezione contro le violazioni arbitrarie dei diritti ivi garantiti da parte dei pubblici poteri. Tale principio "*comporta che un'ingerenza delle autorità nei diritti di un individuo deve poter essere sottoposta ad un controllo efficace*"; trattasi del noto principio "della preminenza del diritto"⁵ che figura nel preambolo della CEDU⁶, il quale implica che il diritto interno offra una certa protezione da tali ingerenze da parte dei pubblici poteri.

L'avvocato generale sostiene infatti che una limitazione alla libertà personale sarebbe possibile solo nel caso in cui trovi sostegno in un fondamento normativo del diritto interno, fondamento che deve essere accessibile, chiaro e prevedibile, tutte condizioni derivanti dal principio della preminenza del diritto. E da tale principio di preminenza che discenderebbe l'esigenza dell'accessibilità e della prevedibilità della legge per l'interessato⁷.

L'ingerenza dei pubblici poteri deve quindi, per essere legittima, essere sottoposta ad un controllo efficace, ovvero che l'ingerenza delle autorità amministrative nei diritti di un individuo dovrebbe essere assicurata dall'autorità giudiziaria affinché vengano rispettate le migliori garanzie di

⁵ Cfr. Corte eur. D. U., sentenza 6 settembre 1978, Klass e a./Germania, ricorso n. 5029/71, Serie A n. 28, pagg. 25 e 26.

⁶ Cfr. CEDU, convenzione europea dei diritti dell'uomo, reperibile al sito internet http://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=fre#n1359128122487_pointer

⁷ Cfr. conclusioni avvocato generale dello Stato, sentenza 24 novembre 2011, Scarlet Extended, C 70-2010, punto 96, reperibile al sito internet <http://curia.europa.eu/juris/liste.jsf?language=it&num=C-70/10>

indipendenza, imparzialità e regolarità delle procedure; tale livello minimo di protezione verrebbe infatti negato nel caso in cui il potere discrezionale conferito al potere esecutivo fosse illimitato ⁸, o se il potere discrezionale conferito ad un giudice fosse illimitato ⁹.

1.2. *La scelta tra il criterio oggettivo e il criterio relativo per stabilire se una persona sia identificabile o meno operata dal Bundesgerichtshof.*

La controversia relativa alla scelta di un criterio oggettivo oppure di quello relativo al fine stabilire se una persona sia identificabile o meno verte, principalmente, sulla distinzione che applicando un criterio “oggettivo” i dati quali gli indirizzi IP potrebbero essere qualificati, al termine delle sessioni di consultazione dei siti Internet, come dati personali anche qualora solamente un terzo sia in grado di determinare l'identità della persona interessata: terzo che, nel caso di specie, è il fornitore di accesso a Internet del sig. Breyer che conserva tali dati aggiuntivi per fini di fatturazione.

Applicando invece il criterio “relativo” tali dati potrebbero essere qualificati come dati personali solo nei confronti del fornitore di accesso a Internet del sig. Breyer, poiché altro operatore web, quale il gestore dei siti consultati dallo stesso, non disporrebbe dei dati identificativi del sig. Breyer a meno che quest'ultimo non li abbia rivelati nel corso delle sessioni, nel caso in cui non fossero state fornite tali informazioni identificative al gestore del sito di consultazione, per risalire all'identità personale dell'utente, sarebbe soggetto ad un enorme dispendio di risorse economiche ¹⁰.

1.3. *Limiti della Repubblica federale tedesca alla conservazione degli indirizzi IP dinamici dopo la consultazione dei siti.*

Il giudice del rinvio chiede se la conservazione di tali indirizzi IP al termine di detta sessione sia autorizzata ai sensi dell'articolo 7, lettera f), della medesima direttiva.

Il Bundesgerichtshof (Corte federale di giustizia) precisa che i fornitori di servizi di media online possono, ai sensi dell'articolo 15, paragrafo 1, del TMG, raccogliere e impiegare dati personali di un utente solo nella misura in cui ciò sia necessario per consentire e fatturare la fruizione di

⁸ Cfr. sull'art. 8 della CEDU cfr. Corte eur. D. U., sentenze 4 maggio 2000, Rotaru/Roumania, ricorso n. 28341/95, Racc. 2000-V, 55; 6 giugno 2006, Segerstedt-Wiberg e a./Svezia, ricorso n. 62332/00, Racc. 2006-VII, 76; 8 giugno 2006, Lupsa/Romania, ricorso n. 10337/04, Racc. 2006-VII, 34; decisione 29 giugno 2006, Weber e Saravia/Germania, ricorso n. 54934/00, Racc. 2006-XI, 94; sull'art. 10 della CEDU, sentenza Sanoma Uitgevers, cit., 82.

⁹ Cfr. Corte eur. D. U., sentenza 24 aprile 1990, Huvig/Francia, ricorso n. 11105/84, Serie A n. 176-B, pag. 55, 29; decisione 10 marzo 2009, Bykov/Russia, ricorso n. 4378/02, 78.

¹⁰ Cfr. sent. sentenza del 24 novembre 2011, Scarlet Extended, C 70/10, punto 51 “Da un lato, infatti, è pacifico che l'ingiunzione di predisporre il sistema di filtraggio controverso implicherebbe un'analisi sistematica di tutti i contenuti, nonché la raccolta e l'identificazione degli indirizzi IP degli utenti all'origine dell'invio dei contenuti illeciti sulla rete, indirizzi che costituiscono dati personali protetti, in quanto consentono di identificare in modo preciso i suddetti utenti”, reperibile al sito intenet. <http://curia.europa.eu/juris/liste.jsf?language=it&num=C-70/10>

detti media. Dall'altro, il giudice del rinvio indica che, secondo la Repubblica federale di Germania, la conservazione di tali dati è necessaria per garantire la sicurezza e la continuità del funzionamento dei siti dei servizi di media online che essa rende accessibili al pubblico, consentendo, in particolare, di riconoscere e difendersi dagli attacchi informatici.

Pare opportuno soffermarsi sulla annosa questione se l'indirizzo IP possa essere definito quale dato personale a prescindere dalla sua connessione ad un nome¹¹. Il garante europeo della protezione dei dati personale, in più occasioni, ha affermato che *“il controllo del comportamento degli utenti di Internet, sommato alla raccolta dei loro indirizzi IP, costituisce un'interferenza nel loro diritto al rispetto della vita privata e della corrispondenza”*¹².

L'art. 5 della direttiva 2006/24/CE¹³, obbliga i fornitori di accesso ad Internet a conservare alcuni dati ai fini della ricerca, dell'accertamento e del perseguimento di gravi reati. I dati che necessitano la conservazione sono i nomi e l'indirizzo dell'abbonato o dell'utente registrato al quale è stato attribuito un indirizzo IP, i dati necessari per determinare data e ora del log-in e del log-off del servizio di accesso Internet sulla base di un determinato fuso orario, unitamente all'indirizzo IP, dinamico o statico, assegnato dal fornitore di accesso.

In questa prospettiva un indirizzo IP è stato considerato un dato personale in quanto consente l'identificazione di una persona, mediante riferimento ad un numero di identificazione o a qualsiasi altro elemento che gli appartenga¹⁴.

Nel caso che ci occupa è necessario stabilire se, a quali condizioni e per quali scopi essi possano essere raccolti, a quali condizioni si possa procedere alla loro comunicazione e quando essi possano essere combinati con altri dati personali. La Corte europea dei diritti dell'uomo si è pronunciata sulla compatibilità della CEDU con specifiche misure di controllo delle comunicazioni elettroniche, ovvero con un sistema di filtraggio e di blocco dei contenuti, disponendo che vi è l'assenza di un

¹¹ Cfr. Sentenza Promusicac, cit. (punto 45), e ordinanza 19 febbraio 2009, causa C-557/07, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten (Racc. pag. I-1227), la stessa sentenza punto 54, 55 e 58 ha anche stabilito che l'autorità giudiziaria competente possa ordinare a soggetti privati che siano fornite informazioni ed anche dati personali relativi all'origine delle attività che violano un diritto di proprietà intellettuale.

¹² Cr. Corte europea dei diritti dell'uomo, decisione 29 giugno 2006, Weber e Saravia/Germania, ricorso n. 54934/00, Racc. 2006-XI, e sentenza 1 luglio 2008, Liberty e a./Regno Unito, ricorso n. 58243.

¹³ Cfr. Direttiva del Parlamento europeo e del Consiglio 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 L 105, pag. 54).

¹⁴ Cfr. sent. sentenza del 24 novembre 2011, Scarlet Extended, C 70/10, in questo caso la questione era differente in quanto si dibatteva sull'identificazione di un utente nel contesto delle violazioni del copyright, e la Corte concluse che l'indirizzo IP raccolto e conservato da un provider è dato personale in quanto permette l'identificazione dell'utente. Per l'orientamento contrario cfr. High Court irlandese nel 2010, causa EMI Records & Ors contro Eircom Ltd, la quale sentenziò che gli indirizzi IP raccolti a fini di contrasto al copyright non costituiscono dati personali, reperibile al sito internet <http://brunosaetta.it/privacy/indirizzo-ip-dinamico-dato-personale.html>.

obbligo generale di sorvegliare le informazioni trasmesse¹⁵. A tale conclusione la Corte è arrivata anche in materia di intercettazioni telefoniche¹⁶, che sono state ritenute ingerenze ai sensi dell'art. 8 della CEDU¹⁷.

Anche l'art. 5 della direttiva 2002/58¹⁸ garantisce la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione, o servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. Tale disposizione vieta agli stati membri qualsiasi sorveglianza o intercettazione di comunicazioni al di fuori dei casi previsti

¹⁵ Cfr. CG sent. sentenza del 24 novembre 2011, *Scarlet Extended*, C 70/10, "le direttive: del Parlamento europeo e del Consiglio 8 giugno 2000, 2000/31/CE, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»); del Parlamento europeo e del Consiglio 22 maggio 2001, 2001/29/CE, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione; del Parlamento europeo e del Consiglio 29 aprile 2004, 2004/48/CE, sul rispetto dei diritti di proprietà intellettuale; del Parlamento europeo e del Consiglio 24 ottobre 1995, 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e del Parlamento europeo e del Consiglio 12 luglio 2002, 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), lette nel loro combinato disposto e interpretate alla luce delle condizioni che la tutela dei diritti fondamentali applicabili implica, devono essere interpretate nel senso che ostano ad un'ingiunzione rivolta ad un fornitore di accesso ad Internet di predisporre un sistema di filtraggio: - di tutte le comunicazioni elettroniche che transitano per i suoi servizi, in particolare mediante programmi «peer-to-peer»; - che si applica indistintamente a tutta la sua clientela; a titolo preventivo; - a sue spese esclusive, e - senza limiti nel tempo, idoneo ad identificare nella rete di tale fornitore la circolazione di file contenenti un'opera musicale, cinematografica o audiovisiva rispetto alla quale il richiedente afferma di vantare diritti di proprietà intellettuale, onde bloccare il trasferimento di file il cui scambio pregiudichi il diritto d'autore".

¹⁶ Cfr. Corte eur. D. U., sentenza 31 maggio 2005, *Vetter/Francia*, ricorso n. 59842/00, punto 27.

¹⁷ Cfr. CEDU art. 8, "Diritto al rispetto della vita privata e familiare 1. Ogni persona ha diritto al rispetto della propria

vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui", reperibile al sito internet http://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=#n1359128122487_pointer.

¹⁸ Cfr. Direttiva 2002/58, art. 5 "Riservatezza delle comunicazioni. 1. Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza. 2. Il paragrafo 1 non pregiudica la registrazione legalmente autorizzata di comunicazioni e dei relativi dati sul traffico se effettuata nel quadro di legittime prassi commerciali allo scopo di fornire la prova di una transazione o di una qualsiasi altra comunicazione commerciale. 3. Gli Stati membri assicurano che l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la

dalla legge conformemente all'art. 15 della detta direttiva¹⁹. Quest'ultima disposizione consente agli Stati membri di adottare disposizioni legislative volte a limitare la portata del diritto alla riservatezza delle comunicazioni, qualora tale limitazione costituisca una misura necessaria per assicurare, in particolare, la ricerca, l'accertamento e il perseguimento dei reati; tali misure devono comunque essere «conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea²⁰».

Alla luce di quanto sopra esposto non sorprende che la Corte abbia risposto alla prima questione pregiudiziale affermando che l'indirizzo IP dinamico costituisce, nei confronti del fornitore del servizio, un dato personale qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detto soggetto dispone.

Tale affermazione deve però essere posta in dubbio ogni qualvolta si consideri che l'indirizzo IP dinamico non consente l'identificazione di un soggetto determinato, come invece nel caso di IP statico, bensì di un terminale da cui trae origine; ciò posto se è pur vero che tale indirizzo può essere successivamente combinato con i dati forniti dal fornitore di accesso alla rete, quali ad es. data e ora di scambio dei file, e in tal modo assoggetto ad un terminale esattamente determinato e anche vero che tale terminale non sempre è assegugettabile all'uso di un utente determinato,

possibilità di rifiutare tale trattamento da parte del responsabile del trattamento. Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente". reperibile al sito internet <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/35284>.

¹⁹ Direttiva 2002/58, art. 15 "Applicazione di alcune disposizioni della direttiva 95/46/CE. 1. Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non au-

torizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono, tra l'altro, adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea. 2. Le disposizioni del capo III della direttiva 95/46/CE relative ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni si applicano relativamente alle disposizioni nazionali adottate in base alla presente direttiva e con riguardo ai diritti individuali risultanti dalla stessa. 3. Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE, svolge i compiti di cui all'articolo 30 della direttiva stessa anche per quanto concerne materie disciplinate dalla presente direttiva, segnatamente la tutela dei diritti e delle libertà fondamentali e degli interessi legittimi nel settore delle comunicazioni elettroniche.

²⁰ Cfr Conclusioni dell'avvocato generale, presentate il 14 aprile 2011, Causa C-70/10 Scarlet Extended SA / Sabam, punto 69.

come nel caso di un nucleo familiare o di un ufficio di grandi o piccole dimensioni.²¹

La Corte di Giustizia UE, in numerose occasioni²², ha ritenuto legittima la richiesta di informazioni personali sugli utenti ai provider, fornitori di accesso, richiesta espletata per garantire la tutela del diritto d'autore e che, in quanto tale, rientrasse nell'ambito di applicazione della direttiva 2004/48²³ sul rispetto dei diritti di proprietà intellettuale.

Negli Stati Uniti si è la giurisprudenza in materia di diritto d'autore è incline nel ritenere che il diritto alla riservatezza possa essere "sacrificato" innanzi ad acclerate violazioni del diritto d'autore, tant'è che i provider che si sono rifiutati di fornire l'identità dei propri utenti, sono stati accusati di violare il copyright proprio dal titolare del diritto d'autore violato²⁴.

1.4. *Il ruolo dei servizi federali tedeschi, fornitori di servizi di media online e responsabili del trattamento degli indirizzi IP dinamici, che agiscono in qualità di soggetti privati quindi al di fuori dell'ambito delle attività dello Stato.*

L'ulteriore quesito posto alla Corte rileva che la questione relativa al trattamento dei dati, nel caso di specie gli indirizzi IP, da parte di uno Stato in materia di diritto penale non sia escluso dalla direttiva 95/46 in forza dell'articolo 3, paragrafo 2, primo trattino²⁵; sul punto la giurisprudenza della Corte è pacifica²⁶ in tutti i casi in cui si tratti di attività proprie degli Stati o delle autorità statali, estranee quindi ai settori di attività dei privati.

Nel caso che ci occupa i servizi federali tedeschi, fornitori del servizio di consultazione, agiscono in qualità di soggetti privati e, quindi, al di fuori dell'ambito delle attività dello Stato in materia di diritto penale.

L'articolo 7, lettera f), della direttiva sulla tutela dei dati personali²⁷, stabilisce che un trattamento dei dati è legittimo a condizione che non

²¹ Cfr. P. SAMMARCO, *Alla ricerca del giusto equilibrio da parte della Corte di Giustizia UE nel confronto tra diritti fondamentali nei casi di impiego di sistemi tecnici di filtraggio*, in questa Rivista, 2012 n. 2, 304 e ss.

²² Cfr. CG, sentenza 24 novembre 2011, Scarlet Extended SA / Sabam, causa C-70/10, punto 69.

²³ Cfr. Direttiva 2004/48/CE reperibile al sito internet [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0048R\(01\):IT:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0048R(01):IT:HTML).

²⁴ Cfr. P. SAMMARCO, *Alla ricerca del giusto equilibrio da parte della Corte di Giustizia UE nel confronto tra diritti fondamentali nei casi di impiego di sistemi tecnici di filtraggio*, in questa Rivista, 2012 n. 2, 297 ss.

²⁵ Cfr. Direttiva 95/46 art. 3, paragrafo 2, primo trattino esclude dal suo ambito di applicazione i trattamenti "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".

²⁶ Cfr. CG sentenza del 6 novembre 2003, Lindqvist, C 101/01, EU:C:2003:596, punto 43; CG sentenza e del 16 dicembre 2008, Satakunnan Markkinapörssi e Satakunta, C 73/07, EU:C:2008:727, punto 41.

²⁷ Cfr. direttiva 95/46, art. 7, lett. f) stabilisce che il trattamento da parte degli Stati membri può essere effettuato se "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 fonamen-

prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata tutelati dall'articolo 1, paragrafo 1²⁸ della stessa.

La Corte ha anche dichiarato che l'articolo 7 della direttiva sui dati personali prevede un elenco esaustivo e tassativo dei casi in cui il trattamento dei dati personali può essere considerato lecito, e che gli Stati membri non possono né aggiungere nuovi principi relativi alla legittimazione del trattamento, né prevedere requisiti supplementari²⁹.

Nella vicenda che ci occupa la normativa nazionale tedesca, art. 15 TMG³⁰, autorizza la raccolta e l'impiego dei dati personali di un utente di un servizio della società dell'informazione, ove non vi sia stato il consenso dello stesso, soltanto nel caso in cui esso si renda necessario ai fini della fatturazione del servizio e che l'obiettivo di garantire il funzionamento generale del medium online non possa giustificare l'impiego dei suddetti dati dopo la sessione di consultazione del servizio.

Anche se gli Stati membri hanno un margine discrezionale nello stabilire quali trattamenti siano legittimi o meno, essi possono usare tale margine solo in conformità all'obiettivo della direttiva suddetta, ovvero quello di mantenere un giusto equilibrio tra la libera circolazione dei dati personali e la tutela della vita privata.

La Corte rileva che l'art. 15 della TMG osterebbe alla conservazione, al termine di una sessione di consultazione, dei dati personali per garantire la fruizione di tali media, l'interesse legittimo dei servizi federali tedeschi, in qualità di soggetti privati, è ravvisabile nella continuità del funzionamento di detti siti.

Il legislatore federale tedesco, sostanzialmente, ha stabilito per alcune 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'art. 5" della direttiva 95/46.³¹

La normativa tedesca, sul trattamento di dati personali degli utenti di siti di media online, riduce la portata del principio previsto all'articolo 7, lettera f), della direttiva 95/46, escludendo che l'obiettivo di garantire il funzionamento generale di tale medium online possa essere oggetto di

tali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1".

²⁸ Cfr. direttiva 95/46, art. 1, paragrafo 1) prevede che "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".

²⁹ Cfr. CG. sentenza del 24 novembre 2011, ASNEF e FECEMD, C 468/10 e C 469/10, EU:C:2011:777, punti 33, 34 e 36.

³⁰ Cfr. TMG, art. 15 "1) Il fornitore di servizi può raccogliere e impiegare i dati personali di un utente solo nella misura in cui ciò sia necessario per rendere possibile la fruizione di media online 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 di ciascuna fruizione e 3. le indicazioni sui media online fruiti dall'utente. 2) Il fornitore di servizi può aggregare i dati di utenza di un utente attinenti alla fruizione di diversi media online, laddove ciò sia necessario a fini di fatturazione verso l'utente.(...). 4) Il fornitore di servizi può impiegare 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 (...)".

³¹ Cfr. sent. in commento, conclusioni dell'avvocato generale ai paragrafi 100 e 101.

ponderazione con l'interesse o i diritti e le libertà fondamentali di detti utenti, diritti e libertà che richiedono, conformemente alla disposizione in parola, tutela ai sensi dell'articolo 1, paragrafo 1, di tale direttiva.

Da ciò la Corte stabilisce che l'articolo 7, lettera f), della direttiva 95/46 deve essere interpretato nel senso che "osta a una normativa di uno Stato membro ai sensi della quale un fornitore di servizi di media online può raccogliere e impiegare dati personali di un utente di tali servizi, in mancanza del suo consenso, solo nella misura in cui detta raccolta e detto impiego siano necessari per consentire e fatturare l'effettiva fruizione dei suddetti servizi da parte dell'utente in questione, senza che l'obiettivo di assicurare il funzionamento generale dei medesimi servizi possa giustificare l'impiego di tali dati dopo una sessione di consultazione degli stessi ³²".

Sostanzialmente la Corte europea ha stabilito che un indirizzo IP dinamico, registrato da un fornitore di servizi di media online durante la consultazione dello stesso, non è riferibile ad una persona fisica identificabile e, pertanto, non rappresenta un dato personale. Nel caso in cui però il gestore del sito disponga di mezzi giuridici che gli consentano di identificare l'utente, grazie alle informazioni aggiuntive in possesso del fornitore di accesso a Internet che, combinate, consentono l'identificazione dell'utente devono essere considerati dati personali e trova quindi applicazione Direttiva 95/46/CE.

Aggiunge successivamente che tali dati non possono essere conservati dal fornitore del servizio di media online, senza il consenso del soggetto, al di fuori della finalità per la quale sono stati raccolti, ovvero quella di fatturare l'effettiva fruizione del servizio dell'utente, e che l'esigenza di garantire il funzionamento del sito stesso, quale quella di prevenire attacchi informatici, non può giustificare la conservazione di tali dati oltre il tempo necessario alla consultazione del sito.

FLAMINIA MERLA

³² Cfr. sentenza in commento.