CORTE DI GIUSTIZIA
DELL'UNIONE EUROPEA

DIREZIONE DELLA RICERCA
E DOCUMENTAZIONE

Scheda tematica

TUTELA DEI DATI PERSONALI

Il diritto alla protezione dei dati di carattere personale è un diritto fondamentale il cui rispetto costituisce un importante obiettivo per l'Unione europea.

Esso è sancito dalla Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta») la quale, all'articolo 8, dispone quanto segue:

«1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

Tale diritto fondamentale è inoltre strettamente connesso al diritto al rispetto della vita privata e della vita familiare sancito all'articolo 7 della Carta.

Il diritto alla protezione dei dati di carattere personale è altresì previsto all'articolo 16, paragrafo 1, del Trattato sul funzionamento dell'Unione europea (TFUE), che ha sostituito in proposito l'articolo 286 CE.

Per quanto attiene al diritto derivato, dalla metà degli anni 90 la Comunità europea si è dotata di vari strumenti destinati a garantire la tutela dei dati personali. La direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[1], adottata sulla base dell'articolo 100 A CE, costituisce in proposito il principale atto giuridico dell'Unione in materia. Essa stabilisce condizioni generali di liceità del trattamento di tali dati nonché i diritti delle persone interessate e prevede, in particolare, l'istituzione negli Stati membri di autorità di controllo indipendenti.

1 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 (GU L 281 del 23.11.1995, pag. 31), versione consolidata al 20.11.2003, abrogata a decorrere dal 25 maggio 2018 (v. nota 5).

La direttiva 2002/58/CE[2] è poi intervenuta a completare la direttiva 95/46/CE, armonizzando le disposizioni normative degli Stati membri relative alla tutela del diritto alla vita privata, per quanto concerne in particolare il trattamento dei dati personali nel settore delle comunicazioni elettroniche[3].

Inoltre, nell'ambito dello spazio di libertà, sicurezza e giustizia (ex-articoli 30 e 31 TUE), la decisione quadro 2008/977/GAI[4] disciplina (fino al mese di maggio del 2018) la protezione dei dati personali nei settori della cooperazione giudiziaria e di polizia in materia penale.

L'Unione europea ha recentemente elaborato una nuova cornice giuridica globale in materia. A tal fine, nel 2016 ha adottato il regolamento (UE) 2016/679[5] relativo alla protezione dei dati, che abroga la direttiva 95/46/CE e che sarà direttamente applicabile a decorrere dal 25 maggio 2018, nonché la direttiva (UE) 2016/680[6] avente ad oggetto la protezione di detti dati in materia penale, che abroga la decisione quadro 2008/977/GAI e la cui data di recepimento da parte degli Stati membri è stata fissata al 6 maggio 2018.

Infine, nel contesto del loro trattamento da parte delle istituzioni e degli organi dell'UE, la tutela dei dati personali è garantita dal regolamento (CE) n. 45/2001[7]. Tale regolamento ha consentito in particolare l'istituzione, nel 2004, del Garante europeo della protezione dei dati. Nel gennaio del 2017 la Commissione ha presentato una proposta[8] di nuovo regolamento che abroga il regolamento n. 45/2001 e la decisione n. 1247/2002/CE con la finalità di modernizzare le norme in materia e di allinearle al nuovo regime istituito dal regolamento (UE) 2016/679.

2 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva «Vita privata e comunicazioni elettroniche») (GU L 201 del 31.7.2002, pag. 37), versione consolidata al 19.12.2009.

3 La direttiva 2002/58/CE è stata modificata dalla 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 L 105 del 13.4.2006, pag. 54). Tale direttiva è stata invalidata dalla Corte, nella sentenza dell'8 aprile 2014, Digital Rights Ireland e Seitlinger e a. (C-293/12 e C-594/12, EU:C:2014:238), per il motivo che arrecava un grave pregiudizio ai diritti al rispetto della vita privata e alla protezione dei dati personali (v. rubrica I.1., intitolata «Conformità del diritto derivato dell'Unione al diritto alla tutela dei dati personali» della presente scheda).

4 Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (GU L 350 del 30.12.2008, pag. 60), abrogata a decorrere dal 6 maggio 2018 (v. nota 6).

5 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GU L 119 del 4.5.2016, pag. 1), applicabile a decorrere dal 25 maggio 2018.

6 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

7 Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

8 Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione, nonché la libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE [COM(2017) 8 final].

I. Il diritto alla protezione dei dati di carattere personale riconosciuto dalla Carta dei diritti fondamentali dell'Unione europea

1. Conformità del diritto derivato dell'Unione al diritto alla tutela dei dati personali

Sentenza del 9 novembre 2010 (Grande Sezione), Volker und Markus Schecke e Eifert (C-92/09 e C-93/09, EU:C:2010:662)[9]

In tale causa, i procedimenti principali vedevano opposti degli agricoltori al Land Hessen, in merito alla pubblicazione sul sito Internet della Bundesanstalt für Landwirtschaft und Ernährung (Ufficio federale per l'agricoltura e l'alimentazione) dei dati personali che li riguardavano in quanto beneficiari di finanziamenti provenienti dal Fondo europeo agricolo di garanzia (FEAGA) e dal Fondo europeo agricolo per lo sviluppo rurale (FEASR). Detti agricoltori si opponevano a tale pubblicazione sostenendo, in particolare, che essa non era giustificata da un interesse pubblico prevalente. Il Land Hessen, per parte sua, considerava che la pubblicazione di detti dati discendeva dai regolamenti (CE) nn. 1290/2005[10] e 259/2008[11], che disciplinano il finanziamento della politica agricola comune e impongono una pubblicazione di informazioni sulle persone fisiche beneficiarie del FEAGA e del FEASR.

In tale contesto il Verwaltungsgericht Wiesbaden (Tribunale amministrativo di Wiesbaden, Germania) ha sottoposto alla Corte di giustizia varie questioni vertenti sulla validità di alcune disposizioni del regolamento (CE) n. 1290/2005 e su quella del regolamento (CE) n. 259/2008, i quali impongono la messa a disposizione del pubblico di siffatte informazioni, in particolare mediante siti Internet gestiti dagli uffici nazionali.

La Corte ha rilevato, riguardo all'adeguamento del diritto alla protezione dei dati di carattere personale riconosciuto dalla Carta e all'obbligo di trasparenza in materia di fondi europei, che la pubblicazione su un sito Internet dei dati nominativi relativi ai beneficiari dei finanziamenti e agli importi da questi percepiti costituisce, in ragione del libero accesso al sito da parte dei terzi, una lesione del diritto dei beneficiari interessati al rispetto della loro vita privata, in generale, e alla protezione dei loro dati personali, in particolare (punti 56-64).

Per essere giustificata, una simile lesione dev'essere prevista dalla legge, deve rispettare il contenuto essenziale di detti diritti e, in applicazione del principio di proporzionalità, dev'essere necessaria e rispondere effettivamente a finalità di interesse generale riconosciute dall'Unione, considerato il fatto che le deroghe e le limitazioni a tali diritti devono operare entro i limiti dello stretto necessario (punto 65). Ciò premesso, la Corte ha ritenuto che, sebbene in una società democratica i contribuenti abbiano diritto ad essere informati sull'impiego delle finanze pubbliche, nondimeno il Consiglio e la Commissione fossero tenuti ad effettuare un contemperamento equilibrato dei differenti interessi in causa, il che richiedeva, prima dell'adozione delle disposizioni di cui si contestava la validità, di verificare se la

9 Tale sentenza è stata presentata nella Relazione annuale 2010, pag. 11.

10 Regolamento (CE) n. 1290/2005 del Consiglio, del 21 giugno 2005, relativo al finanziamento della politica agricola comune (GU L 209 dell'11.8.2005, pag. 1), abrogato dal regolamento (UE) n. 1306/2013 del Parlamento europeo e del Consiglio, del 17 dicembre 2013, sul finanziamento, sulla gestione e sul monitoraggio della politica agricola comune (GU L 347 del 20.12.2013, pag. 549).

11 Regolamento (CE) n. 259/2008 della Commissione, del 18 marzo 2008, recante modalità di applicazione del regolamento (CE) n. 1290/2005 del Consiglio per quanto riguarda la pubblicazione di informazioni sui beneficiari dei finanziamenti provenienti dal FEAGA e dal FEASR (GU L 76 del 19.3.2008, pag. 28), abrogato dal regolamento di esecuzione (UE) n. 908/2014 della Commissione, del 6 agosto 2014, recante modalità di applicazione del regolamento (UE) n. 1306/2013 del Parlamento europeo e del Consiglio per quanto riguarda gli organismi pagatori e altri organismi, la gestione finanziaria, la liquidazione dei conti, le norme sui controlli, le cauzioni e la trasparenza (GU L 255 del 28.8.2014, pag. 59).

pubblicazione di tali dati attraverso un sito Internet unico da parte dello Stato membro non andasse oltre quanto era necessario per la realizzazione degli obiettivi legittimi perseguiti (punti 77, 79, 85, 86).

Pertanto, la Corte ha dichiarato invalide talune disposizioni del regolamento (CE) n. 1290/2005, nonché il regolamento (CE) n. 259/2008 nel suo complesso, nella parte in cui, con riguardo a persone fisiche beneficiarie di aiuti del FEAGA e del FEASR, tali disposizioni impongono la pubblicazione di dati personali relativi ad ogni beneficiario, senza operare distinzioni sulla base di criteri pertinenti come i periodi durante i quali esse hanno percepito simili aiuti, la frequenza o ancora il tipo e l'entità di questi ultimi (punto 92, disp. 1). Tuttavia, la Corte non ha posto in discussione gli effetti della pubblicazione degli elenchi dei beneficiari di siffatti aiuti effettuata dalle autorità nazionali durante il periodo precedente la data di pronuncia della sentenza (punto 94, disp. 2).

Sentenza del 17 ottobre 2013, Schwarz (C-291/12, EU:C:2013:670)

Il sig. Schwarz aveva chiesto il rilascio di un passaporto presso la città di Bochum (Germania), opponendosi a che in tale occasione venissero rilevate le sue impronte digitali. Poiché la città aveva respinto la sua domanda, il sig. Schwarz aveva proposto ricorso dinanzi al Verwaltungsgericht Gelsenkirchen (Tribunale amministrativo di Gelsenkirchen, Germania) perché fosse ingiunto a tale amministrazione di rilasciargli un passaporto senza rilevare le sue impronte digitali. Dinanzi a tale giudice, il sig. Schwarz contestava la validità del regolamento (CE) n. 2252/2004[12] che ha introdotto l'obbligo del rilevamento delle impronte digitali per chi richiede il passaporto, sostenendo, tra l'altro, che tale regolamento violava il diritto alla tutela dei dati personali e il diritto al rispetto della vita privata.

In siffatte circostanze, il Verwaltungsgericht Gelsenkirchen ha adito la Corte di giustizia in via pregiudiziale al fine di sapere se detto regolamento, nella parte in cui obbliga il richiedente un passaporto a fornire le proprie impronte digitali e prevede la loro conservazione nel passaporto, fosse valido, in particolare alla luce della Carta.

La Corte ha risposto affermativamente, dichiarando che, sebbene il prelievo e la conservazione di impronte digitali da parte delle autorità nazionali, disciplinati dall'articolo 1, paragrafo 2, del regolamento (CE) n. 2252/2004, costituiscano un pregiudizio ai diritti al rispetto della vita privata e alla tutela dei dati personali, tale pregiudizio è giustificato dallo scopo di preservare i passaporti da ogni utilizzazione fraudolenta.

Anzitutto, una siffatta limitazione, prevista dalla legge, persegue un obiettivo d'interesse generale riconosciuto dall'Unione, in quanto è volta ad impedire, in particolare, l'ingresso illegale di persone nel territorio dell'Unione (punti 35-38). Inoltre, il prelievo e la conservazione delle impronte digitali sono idonei a raggiungere tale obiettivo. Infatti, da un lato, benché il metodo di verifica dell'identità mediante impronte digitali non sia del tutto affidabile, esso riduce considerevolmente il rischio di accettazione di persone non autorizzate. Dall'altro lato, la discordanza tra le impronte digitali del detentore del passaporto e i dati integrati in tale documento non significa che la persona interessata si veda automaticamente rifiutare l'ingresso nel territorio dell'Unione, ma avrà soltanto la conseguenza di determinare un controllo approfondito per dimostrare in modo definitivo l'identità di detta persona (punti 42-45).

12 Regolamento (CE) n. 2252/2004 del Consiglio, del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri (GU L 385 del 29.12.2004, pag. 1), come modificato dal regolamento (CE) n. 444/2009 del Parlamento europeo e del Consiglio, del 6 maggio 2009 (GU L 142 del 6.6.2009, pag. 1).

Infine, riguardo alla necessità di un trattamento simile, non è stata portata a conoscenza della Corte l'esistenza di misure sufficientemente efficaci, ma meno pregiudizievoli per i diritti riconosciuti dagli articoli 7 e 8 della Carta di quelle derivanti dal metodo basato sulle impronte digitali (punto 53). L'articolo 1, paragrafo 2, del regolamento (CE) n. 2252/2004 non comporta trattamenti delle impronte digitali che eccedano quanto necessario per la realizzazione dell'obiettivo perseguito. Infatti, detto regolamento precisa espressamente che le impronte digitali possono essere utilizzate soltanto allo scopo di verificare l'autenticità del passaporto e l'identità del suo titolare. Per di più, l'articolo 1, paragrafo 2, del regolamento garantisce la tutela contro il rischio di lettura dei dati contenenti impronte digitali da parte di persone non autorizzate e prevede la conservazione delle impronte digitali soltanto all'interno del passaporto, il quale permane di esclusivo possesso del suo titolare (punti 54-57, 60, 63).

Sentenza dell'8 aprile 2014 (Grande Sezione), Digital Rights Ireland e Seitlinger e a. (cause riunite C-293/12 e C-594/12, EU:C:2014:238)[13]

La presente sentenza trova la sua origine in domande di valutazione della validità della direttiva 2006/24/CE riguardante la conservazione di dati, con riferimento ai diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale, sollevate nell'ambito di controversie nazionali dinanzi ai giudici irlandese e austriaco. Nella causa C-293/12, la High Court (Alta Corte, Irlanda) era investita di una controversia tra la società Digital Rights e le autorità irlandesi in merito alla legittimità di misure nazionali riguardanti la conservazione di dati relativi a comunicazioni elettroniche. Nella causa C-594/12, il Verfassungsgerichtshof (Corte costituzionale, Austria) era investito di vari ricorsi in materia costituzionale diretti all'annullamento della disposizione nazionale di recepimento della direttiva 2006/24/CE nel diritto austriaco.

Con le loro domande di pronuncia pregiudiziale, i giudici irlandese e austriaco hanno interpellato la Corte di giustizia sulla validità della direttiva 2006/24/CE alla luce degli articoli 7, 8 e 11 della Carta. Più precisamente, detti giudici hanno chiesto alla Corte se l'obbligo gravante, in forza di detta direttiva, sui fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione elettronica di conservare per un certo periodo dati relativi alla vita privata di una persona e alle sue comunicazioni e di consentirne l'accesso alle autorità nazionali competenti comportasse un'ingerenza ingiustificata in detti diritti fondamentali. I tipi di dati interessati sono, in particolare, i dati necessari per rintracciare e identificare la fonte di una comunicazione e la destinazione della stessa, per stabilire la data, l'ora, la durata e il tipo di una comunicazione, le attrezzature di comunicazione degli utenti nonché per determinare l'ubicazione delle apparecchiature di comunicazione mobile, dati tra i quali figurano, segnatamente, il nome e l'indirizzo dell'abbonato o dell'utente registrato, il numero telefonico chiamante e quello chiamato, nonché un indirizzo IP per i servizi Internet. I suddetti dati permettono, in particolare, di sapere quale sia la persona con cui un abbonato o un utente registrato ha comunicato e con quale mezzo, così come di stabilire il tempo della comunicazione e il luogo dal quale questa è avvenuta. Inoltre, essi permettono di conoscere la frequenza delle comunicazioni dell'abbonato o dell'utente registrato con talune persone nel corso di un determinato periodo.

La Corte ha dichiarato, anzitutto, che le disposizioni della direttiva 2006/24/CE, imponendo siffatti obblighi a tali fornitori, erano costitutive di un'ingerenza particolarmente grave nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale, garantiti dagli articoli 7 e 8 della Carta. Ciò premesso, è vero che la Corte ha rilevato che tale ingerenza poteva essere giustificata dal perseguimento di un obiettivo di interesse generale, come la lotta alla criminalità organizzata. In proposito, la Corte ha rilevato, in primo luogo, che la conservazione dei dati imposta dalla direttiva non era idonea a pregiudicare il contenuto essenziale dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, nella misura in cui non permetteva di venire a conoscenza del

13 Tale sentenza è stata presentata nella Relazione annuale 2014, pag. 60.

contenuto delle comunicazioni elettroniche in quanto tale e prevede che i fornitori di servizi o di reti sono tenuti a rispettare taluni principi di protezione e di sicurezza dei dati. In secondo luogo, la Corte ha osservato che la conservazione dei dati in vista della loro eventuale trasmissione alle autorità nazionali competenti rispondeva effettivamente a un obiettivo di interesse generale, ossia la lotta contro la criminalità grave nonché, in ultima analisi, la sicurezza pubblica (punti 38-44).

Tuttavia, la Corte ha ritenuto che, adottando la direttiva riguardante la conservazione dei dati, il legislatore dell'Unione avesse ecceduto i limiti imposti dal rispetto del principio di proporzionalità. Pertanto, essa ha dichiarato la direttiva invalida considerando che l'ingerenza di vasta portata e di particolare gravità nei diritti fondamentali che essa comportava non era sufficientemente regolamentata al fine di garantire che fosse limitata a quanto strettamente necessario (punto 65). La direttiva 2006/24/CE riguardava infatti in maniera generale qualsiasi persona e qualsiasi mezzo di comunicazione elettronica nonché l'insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi (punti 57-59). La direttiva non prevedeva peraltro alcun criterio oggettivo che permettesse di garantire che le autorità nazionali competenti avessero accesso ai dati e potessero utilizzarli soltanto a fini di prevenzione, di accertamento o di indagini penali riguardanti reati che potessero essere considerati sufficientemente gravi da giustificare siffatta ingerenza, né le condizioni sostanziali e procedurali di un tale accesso o di una tale utilizzazione (punti 60-62). Riguardo infine alla durata di conservazione dei dati, la direttiva imponeva una durata di almeno sei mesi senza che venisse effettuata alcuna distinzione tra le categorie di dati a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate (punti 63, 64).

Peraltro, per quanto concerne i requisiti derivanti dall'articolo 8, paragrafo 3, della Carta, la Corte ha constatato che la direttiva 2006/24/CE non prevedeva garanzie sufficienti che permettessero di assicurare una protezione efficace dei dati contro i rischi di abuso nonché contro l'accesso e l'uso illeciti dei dati e non imponeva neppure una conservazione di questi ultimi sul territorio dell'Unione.

Di conseguenza, detta direttiva non garantiva pienamente il controllo del rispetto dei requisiti di protezione e di sicurezza da parte di un'autorità indipendente, come pure esplicitamente richiesto dalla Carta (punti 66-68).

2. Rispetto del diritto alla protezione dei dati di carattere personale nell'attuazione del diritto dell'Unione

Sentenza del 21 dicembre 2016 (Grande Sezione), Tele2 Sverige (cause riunite C-203/15 e C-698/15, EU:C:2016:970)[14]

A seguito della sentenza Digital Rights Ireland e Seitlinger e a. che ha dichiarato invalida la direttiva 2006/24/CE (v. supra), la Corte di giustizia è stata investita di due cause aventi ad oggetto l'obbligo generalizzato imposto, in Svezia e nel Regno Unito, ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi a tali comunicazioni, la cui conservazione era prevista dalla direttiva invalidata.

All'indomani della pronuncia della sentenza Digital Rights Ireland e Seitlinger e a., l'impresa di telecomunicazioni Tele2 Sverige ha notificato all'autorità svedese di sorveglianza delle poste e delle telecomunicazioni la propria decisione di cessare di procedere alla conservazione dei dati nonché la propria intenzione di cancellare i dati già registrati (causa C-203/15). Il diritto svedese obbligava infatti i fornitori di servizi di comunicazione elettronica a conservare in maniera sistematica e continua, senza alcuna eccezione, l'insieme dei dati sul traffico e dei dati relativi all'ubicazione di tutti i loro abbonati e

14 Tale sentenza è stata presentata nella Relazione annuale 2016, pag. 62.

utenti iscritti, riguardante tutti i mezzi di comunicazione elettronica. Nella causa C-698/15, tre persone avevano presentato ricorsi contro il regime britannico di conservazione dei dati che consentiva al Ministro dell'Interno di obbligare gli operatori di telecomunicazioni pubbliche a conservare tutti i dati relativi a comunicazioni per una durata massima di dodici mesi, pur essendo la conservazione del contenuto di tali comunicazioni esclusa.

Adita dal Kammarrätten i Stockholm (Corte d'appello amministrativa di Stoccolma, Svezia) e dalla Court of Appeal (England and Wales) (Civil Division) [Corte d'appello (Inghilterra e Galles) (Sezione civile), Regno Unito)], la Corte di giustizia era invitata a pronunciarsi sull'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58/CE, detta «Vita privata e comunicazioni elettroniche», che consente agli Stati membri di introdurre talune eccezioni all'obbligo, enunciato in tale direttiva, di garantire la riservatezza delle comunicazioni elettroniche e dei dati relativi al traffico a queste correlati.

Nella propria sentenza, la Corte ha anzitutto dichiarato che l'articolo 15, paragrafo 1, della direttiva 2002/58/CE, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, osta ad una normativa nazionale, come quella svedese, la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica. Secondo la Corte, una siffatta normativa travalica i limiti dello stretto necessario e non può essere considerata giustificata, in una società democratica, così come richiede detto articolo 15, paragrafo 1, letto alla luce dei citati articoli della Carta (punti 99-105, 107, 112, disp. 1).

La medesima disposizione, letta alla luce degli stessi articoli della Carta, osta altresì ad una normativa nazionale, la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione (punti 118-122, 125, disp. 2).

La Corte ha invece considerato che l'articolo 15, paragrafo 1, della direttiva 2002/58/CE non osta a una normativa la quale consenta, a titolo preventivo, la conservazione mirata di dati di tale natura, per finalità di lotta contro la criminalità grave, a condizione che detta conservazione sia limitata allo stretto necessario per quanto riguarda le categorie di dati considerati, i mezzi di comunicazione interessati, le persone coinvolte, nonché la durata di conservazione prevista. Per soddisfare tali requisiti, detta normativa nazionale deve, in primo luogo, prevedere norme chiare e precise che permettano di proteggere efficacemente i dati contro i rischi di abuso. Essa deve in particolare indicare in quali circostanze e a quali condizioni una misura di conservazione dei dati può, a titolo preventivo, essere adottata, garantendo così che una misura siffatta sia limitata allo stretto necessario. In secondo luogo, per quanto riguarda le condizioni sostanziali che devono essere soddisfatte dalla normativa nazionale, al fine di garantire che essa sia limitata allo stretto necessario, la conservazione dei dati deve rispondere sempre a criteri oggettivi, istituendo un rapporto tra i dati da conservare e l'obiettivo perseguito. In particolare, tali condizioni devono risultare, in pratica, idonee a delimitare effettivamente la portata della misura e, di conseguenza, il pubblico interessato. Per quanto riguarda tale delimitazione, la normativa nazionale deve essere fondata su elementi oggettivi, che permettano di prendere in considerazione un pubblico i cui dati sono idonei a rivelare una connessione, almeno indiretta, con atti di criminalità grave, a contribuire in un modo o in un altro alla lotta contro la criminalità grave, o a prevenire un grave rischio per la sicurezza pubblica (punti 108-111).

II. Il trattamento dei dati personali ai sensi della direttiva n. 95/46/CE

1. Trattamenti di dati personali esclusi dall'ambito di applicazione della direttiva n. 95/46/CE

Sentenza del 30 maggio 2006 (Grande Sezione), Parlamento/Consiglio (C-317/04 e C-318/04, EU:C:2006:346)

A seguito degli attacchi terroristici dell'11 settembre 2001, gli Stati Uniti avevano adottato una normativa che disponeva che i vettori aerei che assicuravano collegamenti con destinazione o partenza nel territorio degli Stati Uniti ovvero traversanti tale territorio fossero tenuti a fornire alle autorità statunitensi un accesso elettronico ai dati contenuti nel loro sistema di prenotazione e di controllo delle partenze, denominati Passenger Name Records (PNR).

Ritenendo che tali disposizioni potessero essere in contrasto con la legislazione europea e con quella degli Stati membri in materia di tutela dei dati, la Commissione aveva avviato negoziati con le autorità statunitensi. In seguito a tali negoziati, il 14 maggio 2004 la Commissione aveva adottato la decisione 2004/535/CE[15], la quale constata che l'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti (United States Bureau of Customs and Border Protection; in prosieguo: il «CBP») è in grado di garantire un livello di protezione adeguato dei dati PNR trasmessi dalla Comunità (in prosieguo: la «decisione sull'adeguatezza»). Successivamente, il 17 maggio 2004, il Consiglio aveva adottato la decisione 2004/496/CE[16] che approva la conclusione di un accordo tra la Comunità europea e gli Stati Uniti sul trattamento e il trasferimento al CBP di dati PNR da parte di vettori aerei stabiliti nel territorio degli Stati membri della Comunità.

Il Parlamento europeo ha chiesto alla Corte di giustizia di annullare le due menzionate decisioni sostenendo, in particolare, che la decisione sull'adeguatezza era stata adottata ultra vires, che l'articolo 95 CE (divenuto l'articolo 114 TFUE) non costituiva un fondamento giuridico corretto per la decisione che approva la conclusione dell'accordo e, in entrambi i casi, che vi era una violazione dei diritti fondamentali.

Per quanto concerne la decisione sull'adeguatezza, la Corte ha verificato, anzitutto, se la Commissione potesse validamente adottare la propria decisione sulla base della direttiva 95/46/CE. In tale contesto, essa ha constatato che dalla decisione sull'adeguatezza risultava che il trasferimento dei dati PNR al CBP costituisce un trattamento avente come oggetto la pubblica sicurezza e le attività dello Stato in materia di diritto penale. Secondo la Corte, benché i dati PNR fossero inizialmente raccolti dalle compagnie aeree nell'ambito di un'attività che rientra nel diritto dell'Unione, ossia la vendita di un biglietto aereo che dava diritto ad una prestazione di servizi, il trattamento dei dati che veniva preso in considerazione nella decisione sull'adeguatezza, tuttavia, possedeva una natura del tutto diversa. Infatti, tale decisione non riguardava un trattamento di dati necessario alla realizzazione di una prestazione di servizi, ma un trattamento di dati ritenuto necessario per salvaguardare la pubblica sicurezza e a fini repressivi (punti 56, 57).

15 Decisione 2004/535/CE della Commissione, del 14 maggio 2004, relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti United States' Bureau of Customs and Border Protection (GU L 235 del 6.7.2004, pag. 11).

16 Decisione 2004/496/CE del Consiglio, del 17 maggio 2004, relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (Passenger Name Record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti (GU L 183 del 20.5.2004, pag. 83, e rettifiche GU L 255 del 30.9.2005, pag. 168).

A tal proposito, la Corte ha rilevato che il fatto che i dati PNR fossero stati raccolti da operatori privati a fini commerciali e che fossero questi ultimi ad organizzarne il trasferimento ad uno Stato terzo non ostava a che tale trasferimento fosse considerato un trattamento di dati escluso dall'ambito di applicazione della direttiva. Infatti, il trasferimento rientrava in un ambito istituito dai poteri pubblici e attinente alla pubblica sicurezza. Pertanto, la Corte ha concluso che la decisione sull'adeguatezza non rientrava nell'ambito di applicazione della direttiva in quanto riguardava un trattamento di dati personali che ne è escluso. La Corte, di conseguenza, ha annullato la decisione sull'adeguatezza (punti 58, 59).

Riguardo alla decisione del Consiglio, la Corte ha rilevato che l'articolo 95 CE, in combinato disposto con l'articolo 25 della direttiva 95/46/CE, non può costituire il fondamento della competenza della Comunità a concludere l'accordo in esame con gli Stati Uniti. Infatti, tale accordo riguardava lo stesso trasferimento di dati della decisione sull'adeguatezza e quindi trattamenti di dati che erano esclusi dall'ambito di applicazione della direttiva. Di conseguenza, la Corte ha annullato la decisione del Consiglio che approvava la conclusione dell'accordo (punti 67-69).

Sentenza dell'11 dicembre 2014, Ryneš (C-212/13, EU:C:2014:2428)

In risposta a ripetute aggressioni, il sig. Ryneš aveva installato sulla propria casa una telecamera di sorveglianza. A seguito di un nuovo attacco avente di mira la sua casa, le registrazioni di detta telecamera avevano permesso di identificare due persone sospette, nei cui confronti erano stati avviati procedimenti penali. Poiché la legalità del trattamento dei dati registrati dalla telecamera di sorveglianza era stata contestata da una delle persone sospette dinanzi all'Ufficio ceco per la tutela dei dati personali, quest'ultimo aveva constatato che il sig. Ryneš aveva violato le norme in materia di tutela dei dati personali e gli aveva inflitto un'ammenda.

Investito di un ricorso proposto dal sig. Ryneš avverso una decisione del Městský soud v Praze (Corte municipale di Praga, Repubblica ceca) che aveva confermato la decisione dell'Ufficio, il Nejvyšší správní soud (Corte suprema amministrativa) ha chiesto alla Corte di giustizia se la registrazione realizzata dal sig. Ryneš alla scopo di proteggere la sua vita, la sua salute e la sua proprietà costituisse un trattamento di dati non rientrante nella direttiva 95/46/CE, per il motivo che tale registrazione era stata effettuata da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico, ai sensi dell'articolo 3, paragrafo 2, secondo trattino di detta direttiva.

La Corte ha dichiarato che l'utilizzo di un sistema di videocamera, che porta a una registrazione video delle persone immagazzinata in un dispositivo di registrazione continua quale un disco duro, installato da una persona fisica sulla sua abitazione familiare per proteggere i beni, la salute e la vita dei proprietari dell'abitazione, sistema che sorveglia parimenti lo spazio pubblico, non costituisce un trattamento dei dati effettuato per l'esercizio di attività a carattere esclusivamente personale o domestico (punto 35 e disp.).

In proposito, essa ha ricordato che la tutela del diritto fondamentale alla vita privata, garantito dall'articolo 7 della Carta, impone che le deroghe alla tutela dei dati personali e le limitazioni della stessa avvengano nei limiti dello stretto necessario. Posto che le disposizioni della direttiva 95/46/CE, in quanto disciplinano il trattamento di dati personali suscettibile di ledere le libertà fondamentali e, in particolare, il diritto alla vita privata, devono necessariamente essere interpretate alla luce dei diritti fondamentali sanciti da detta Carta, la deroga prevista dall'articolo 3, paragrafo 2, secondo trattino, di tale direttiva dev'essere interpretata in senso restrittivo (punti 27-29). Inoltre, il dettato stesso di tale disposizione sottrae all'applicazione della direttiva 95/46/CE il trattamento dei dati effettuato per l'esercizio di attività «esclusivamente» personali o domestiche. Orbene, posto che una videosorveglianza si estende, anche se solo parzialmente, allo spazio pubblico, e pertanto è diretta verso l'esterno della sfera privata della persona che procede al trattamento dei dati con tale modalità, essa non può essere considerata un'attività esclusivamente «personale o domestica» ai sensi di detta disposizione (punti 30, 31, 33).

2. Nozione di «dati personali»

Sentenza del 19 ottobre 2016, Breyer (C-582/14, EU:C:2016:779)[17]

Il sig. Breyer aveva proposto un ricorso dinanzi ai giudici civili tedeschi, chiedendo che alla Repubblica federale di Germania fosse inibito di conservare o far conservare da terzi dati informatici trasmessi al termine di ogni consultazione dei siti Internet dei servizi federali tedeschi. Infatti, al fine di contrastare attacchi e consentire il perseguimento penale dei «pirati informatici», il fornitore di servizi di media online dei servizi federali tedeschi registrava dati consistenti in un indirizzo IP «dinamico» – ossia un indirizzo IP che cambia a ogni nuova connessione a Internet – nonché nella data e nell'ora della sessione di consultazione del sito. A differenza degli indirizzi IP statici, gli indirizzi IP dinamici non consentivano, a priori, di associare, attraverso file accessibili al pubblico, un dato computer al collegamento fisico alla rete utilizzato dal fornitore di accesso a Internet. I dati registrati non offrivano, di per sé, al fornitore di servizi di media online la possibilità di identificare l'utente. Invece, il fornitore di accesso a Internet disponeva, quanto a lui, di informazioni aggiuntive che, se combinate con il suddetto indirizzo IP, avrebbero consentito di identificare l'utente in parola.

Ciò premesso, il Bundesgerichtshof (Corte federale di giustizia, Germania), investito di un ricorso per «Revision» (cassazione), ha chiesto alla Corte di giustizia se un indirizzo IP memorizzato da un fornitore di servizi di media online in relazione ad un accesso al suo sito Internet costituisca per quest'ultimo un dato personale.

La Corte ha anzitutto rilevato che perché un dato possa essere qualificato come «dato personale» ai sensi dell'articolo 2, lettera a), della direttiva 95/46/CE, non si richiede che tutte le informazioni che consentono di identificare la persona interessata siano in possesso di una sola persona. Il fatto che le informazioni aggiuntive necessarie per identificare l'utente di un sito Internet siano detenute non dal fornitore di servizi di media online, ma dal fornitore di accesso a Internet di tale utente non pare quindi idoneo a escludere che gli indirizzi IP dinamici registrati dal fornitore di servizi di media online costituiscano, per quest'ultimo, dati personali ai sensi dell'articolo 2, lettera a), della direttiva 95/46/CE (punti 43, 44).

Di conseguenza, la Corte ha constatato che un indirizzo IP 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 dell'articolo 2, lettera a), della direttiva 95/46/CE, qualora detto fornitore disponga di mezzi giuridici che gli consentono di far identificare la persona interessata grazie alle informazioni aggiuntive relative a quest'ultima di cui il fornitore di accesso a Internet di detta persona dispone (punto 49, disp. 1).

Sentenza del 20 dicembre 2017, Nowak (C-434/16, ECLI:EU:C:2017:582)

Il sig. Nowak, un esperto contabile tirocinante, non aveva superato l'esame organizzato dall'organizzazione professionale irlandese degli esperti contabili. Egli aveva presentato una domanda di accesso, ai sensi dell'articolo 4 della legge sulla protezione dei dati, che si riferiva a tutti i dati personali che lo riguardavano, detenuti dall'organizzazione professionale degli esperti contabili. Quest'ultima aveva trasmesso al sig. Nowak alcuni documenti ma aveva rifiutato di trasmettergli la sua prova di esame, con la motivazione che l'elaborato non conteneva dati personali che lo riguardassero, ai sensi della legge sulla protezione dei dati.

17 Tale sentenza è stata presentata nella Relazione annuale 2016, pag. 61.

Poiché neppure il garante per la protezione dei dati personali aveva dato seguito alla sua domanda di accesso per le stesse ragioni, il sig. Nowak si è rivolto ai giudici nazionali. La Supreme Court (Corte suprema, Irlanda), investita di un'impugnazione proposta dal sig. Nowak, ha posto alla Corte di giustizia la questione se l'articolo 2, lettera a), della direttiva 95/46/CE debba essere interpretato nel senso che, in circostanze come quelle di cui al procedimento principale, le risposte scritte fornite da un candidato durante un esame professionale e le eventuali annotazioni dell'esaminatore ad esse relative costituiscano dati personali concernenti il candidato, ai sensi di tale disposizione.

In primo luogo, la Corte ha rilevato che, affinché un dato possa essere qualificato come «dato personale», ai sensi dell'articolo 2, lettera a), della direttiva 95/46/CE, non si richiede che tutte le informazioni che consentono di identificare la persona interessata siano in possesso di una sola persona. Peraltro, nell'ipotesi in cui l'esaminatore non conosca l'identità del candidato al momento della valutazione delle risposte da esso fornite nell'ambito di un esame, l'ente che ha organizzato l'esame, nella fattispecie l'organizzazione professionale degli esperti contabili, dispone, per contro, delle informazioni necessarie che gli consentono di identificare senza difficoltà o dubbi tale candidato mediante il suo numero di identificazione, apposto sulla prova d'esame o sulla pagina di copertina di tale prova, e quindi di attribuirgli le sue risposte.

In secondo luogo, la Corte ha constatato che le risposte scritte fornite da un candidato a un esame professionale costituiscono informazioni connesse alla sua persona. Infatti, il contenuto di tali risposte riflette il livello di conoscenza e di competenza del candidato in un dato settore nonché, se del caso, i suoi processi di riflessione, il suo giudizio e il suo spirito critico. La raccolta di tali risposte ha, poi, la funzione di valutare le capacità professionali del candidato e la sua idoneità a esercitare il mestiere di cui trattasi. Inoltre, l'uso di tali informazioni, che si traduce, segnatamente, nel successo o nel fallimento del candidato all'esame di cui trattasi, può avere un effetto sui diritti e interessi dello stesso, in quanto può determinare o influenzare, per esempio, le sue possibilità di accedere alla professione o all'impiego desiderati. La constatazione che le risposte scritte fornite da un candidato a un esame professionale costituiscono informazioni concernenti tale candidato in ragione del loro contenuto, della loro finalità e del loro effetto vale, peraltro, anche quando si tratti di un esame con libera consultazione di materiale.

In terzo luogo, per quanto riguarda le annotazioni dell'esaminatore relative alle risposte del candidato, la Corte ha considerato che esse costituiscono, proprio come le risposte fornite dal candidato durante l'esame, informazioni concernenti tale candidato, dato che riflettono l'opinione o la valutazione dell'esaminatore sulle prestazioni individuali del candidato durante l'esame, e in particolare sulle sue conoscenze e competenze nel settore di cui trattasi. Dette annotazioni hanno, peraltro, appunto lo scopo di documentare la valutazione fatta dall'esaminatore delle prestazioni del candidato e possono produrre effetti per quest'ultimo.

In quarto luogo, la Corte ha dichiarato che le risposte scritte fornite dal candidato durante un esame professionale e le eventuali annotazioni dell'esaminatore ad esse relative possono essere assoggettate a una verifica, in particolare, della loro esattezza e della necessità della loro conservazione, ai sensi dell'articolo 6, paragrafo 1, lettere d) ed e), della direttiva 95/46/CE, e possono essere oggetto di una rettifica o di una cancellazione, ai sensi dell'articolo 12, lettera b), della stessa. Il fatto di dare al candidato un diritto di accesso a tali risposte e a tali annotazioni, ai sensi dell'articolo 12, lettera a), di tale direttiva, è conforme all'obiettivo della stessa consistente nel garantire la tutela del diritto alla vita privata di tale candidato rispetto al trattamento dei dati che lo riguardano e ciò indipendentemente dalla questione se detto candidato disponga o no di un tale diritto di accesso anche in forza della normativa nazionale applicabile al procedimento di esame. Tuttavia, la Corte ha sottolineato che i diritti di accesso e di rettifica, ai sensi dell'articolo 12, lettere a) e b), della direttiva 95/46/CE, non si estendono alle domande poste in sede di esame, le quali non costituiscono in quanto tali dati personali del candidato.

Alla luce di tali elementi, la Corte ha concluso che, in circostanze come quelle di cui al procedimento principale, le risposte scritte fornite da un candidato durante un esame professionale e le eventuali

annotazioni dell'esaminatore relative a tali risposte costituiscono dati personali, ai sensi dell'articolo 2, lettera a), della direttiva 95/46/CE.

3. Nozione di «trattamento di dati personali»

Sentenza del 6 novembre 2003 (Seduta plenaria), Lindqvist (C-101/01, EU:C:2003:596)

La sig.ra Lindqvist, lavoratrice volontaria in una parrocchia della Chiesa protestante di Svezia, aveva creato, dal suo personal computer, pagine Internet pubblicandovi dati personali relativi a varie persone che, come lei, lavoravano in qualità di volontari in detta parrocchia. La sig.ra Lindqvist è stata condannata al pagamento di un'ammenda, per il motivo che aveva utilizzato dati personali nel contesto di un trattamento automatizzato senza prima informarne per iscritto la Datainspektion svedese (ente pubblico per la tutela dei dati trasmessi per via informatica), che li aveva trasferiti, in assenza di autorizzazione, verso paesi terzi e che aveva trattato dati personali sensibili.

Nell'ambito dell'impugnazione proposta dalla sig.ra Lindqvist avverso tale decisione dinanzi al Göta hovrätt (Corte d'appello, Svezia), quest'ultimo aveva adito la Corte di giustizia in via pregiudiziale al fine, in particolare, di sapere se la sig.ra Lindqvist avesse effettuato un «trattamento di dati personali interamente o parzialmente automatizzato», ai sensi della direttiva 95/46/CE.

La Corte ha constatato che l'operazione consistente nel fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, ad esempio indicando il loro numero di telefono o informazioni relative alla loro situazione lavorativa e ai loro passatempi, costituisce un «trattamento di dati personali interamente o parzialmente automatizzato» ai sensi di tale direttiva (punto 27, disp. 1). Infatti, un siffatto trattamento di dati personali effettuato per l'esercizio di attività a titolo religioso o di volontariato non rientra in alcuna delle eccezioni all'ambito di applicazione della direttiva, nella misura in cui non rientra né nella categoria delle attività aventi ad oggetto la pubblica sicurezza né in quella delle attività a carattere esclusivamente personale o domestico che esulano dal campo di applicazione della direttiva (punti 38, 43-48, disp. 2).

Sentenza del 13 maggio 2014 (Grande Sezione), Google Spain e Google (C-131/12, EU:C:2014:317)

Nel 2010 un cittadino spagnolo aveva presentato dinanzi all'Agencia Española de Protección de Datos (Agenzia spagnola di protezione dei dati; in prosieguo: l'«AEPD») un reclamo contro La Vanguardia Ediciones SL, editore di un quotidiano di larga diffusione in Spagna, nonché contro Google Spain e Google. Tale persona sosteneva che, allorché un utente di Internet introduceva il suo nome nel motore di ricerca del gruppo Google, l'elenco dei risultati mostrava link verso due pagine del quotidiano di La Vanguardia, datate 1998, che annunciavano in particolare una vendita all'asta di immobili organizzata a seguito di un pignoramento volto alla riscossione di suoi debiti. Con il proprio reclamo, tale persona chiedeva, da un lato, che fosse ordinato a La Vanguardia di sopprimere o modificare le pagine interessate, oppure di ricorrere a taluni strumenti forniti dai motori di ricerca per proteggere tali dati. Dall'altro lato, chiedeva fosse ingiunto a Google Spain o a Google di eliminare o di occultare i suoi dati personali, in modo che sparissero dai risultati di ricerca e dai link di La Vanguardia.

L'AEPD aveva respinto il reclamo contro La Vanguardia, ritenendo che le informazioni in questione fossero state pubblicate legalmente dall'editore, ma l'aveva, invece, accolto nella parte relativa a Google Spain e a Google e aveva chiesto alle due società di adottare le misure necessarie per rimuovere i dati dai propri indici e per renderne impossibile l'accesso in futuro. Avendo dette società proposto due ricorsi

dinanzi all'Audiencia Nacional (Corte centrale, Spagna) al fine di ottenere l'annullamento della decisione dell'AEPD, il giudice spagnolo ha deferito una serie di questioni alla Corte di giustizia.

La Corte di giustizia ha quindi avuto l'occasione di precisare la nozione di «trattamento di dati personali» in Internet con riferimento alla direttiva 95/46/CE.

La Corte ha così dichiarato che l'attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come trattamento di dati personali qualora tali informazioni contengano dati personali (disp. 1). La Corte, inoltre, ha ricordato che le operazioni contemplate dalla direttiva devono essere considerate come un trattamento anche nell'ipotesi in cui riguardino esclusivamente informazioni già pubblicate tali e quali nei media. Una deroga generale all'applicazione della direttiva in un'ipotesi siffatta avrebbe l'effetto di privare in larga parte del suo significato tale direttiva (punti 29, 30).

4. Condizioni di liceità di un trattamento di dati personali con riferimento all'articolo 7 della direttiva n. 95/46/CE

Sentenza del 16 dicembre 2008 (Grande Sezione), Huber (C-524/06, EU:C:2008:724)[18]

L'Ufficio federale per l'immigrazione e i rifugiati (Bundesamt für Migration und Flüchtlinge, Germania), provvedeva alla gestione di un registro centralizzato degli stranieri che raccoglieva taluni dati personali relativi agli stranieri soggiornanti nel territorio tedesco per un periodo superiore a tre mesi. Il registro era utilizzato a fini statistici e in occasione dell'esercizio, da parte dei servizi di sicurezza e di polizia nonché delle autorità giudiziarie, delle loro competenze in materia di azioni giudiziarie e ricerche relative a comportamenti criminali o pericolosi per la pubblica sicurezza.

Il sig. Huber, cittadino austriaco, si è stabilito in Germania nel 1996 per esercitarvi la professione di agente assicurativo indipendente. Ritenendosi discriminato a causa del trattamento dei suoi dati contenuti nel registro in parola, poiché non esiste una banca dati corrispondente per i cittadini tedeschi, il sig. Huber ha richiesto la cancellazione di tali dati.

In tali circostanze, l'Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Tribunale amministrativo superiore del Land della Renania Settentrionale-Vestfalia, Germania), investito della controversia, ha chiesto alla Corte di pronunciarsi in merito alla compatibilità con il diritto dell'Unione del trattamento di dati personali effettuato nell'ambito del registro di cui trattasi.

La Corte ha ricordato, anzitutto, che il diritto di soggiorno di un cittadino dell'Unione nel territorio di uno Stato membro di cui egli non ha la nazionalità non è incondizionato, ma può essere subordinato a limitazioni. Di conseguenza, l'impiego di un siffatto registro al fine di coadiuvare le autorità incaricate di applicare la normativa in materia di soggiorno risulta in linea di principio legittimo considerata la sua natura, compatibile con il divieto di discriminazioni fondate sulla nazionalità contenuto nell'articolo 12, paragrafo 1, CE (divenuto l'articolo 18, primo comma, TFUE). Tuttavia, siffatto registro non può contenere informazioni diverse da quelle a tal fine necessarie ai sensi della direttiva sulla tutela dei dati personali (punti 54, 58, 59).

18 Tale sentenza è stata presentata nella Relazione annuale 2008, pag. 45.

Riguardo alla nozione di necessità del trattamento ai sensi dell'articolo 7, lettera e), della direttiva 95/46/CE, la Corte ha anzitutto ricordato che si trattava di una nozione autonoma del diritto dell'Unione che deve essere interpretata in maniera tale da rispondere pienamente alla finalità della direttiva 95/46/CE come definita dal suo articolo 1, paragrafo 1. Essa ha poi constatato che un sistema di trattamento di dati personali è conforme al diritto dell'Unione se contiene unicamente i dati necessari per l'applicazione, da parte di tali autorità, di detta normativa e il suo carattere centralizzato consente un'applicazione più efficace di tale normativa per quanto riguarda il diritto di soggiorno dei cittadini dell'Unione non aventi la nazionalità di detto Stato membro.

In ogni caso, la conservazione e il trattamento di dati personali nominativi a fini statistici nell'ambito di un tale registro non possono essere considerati necessari ai sensi dell'articolo 7, lettera e), della direttiva 95/46/CE (punti 52, 66, 68).

Peraltro, riguardo alla questione dell'impiego dei dati contenuti nel registro per finalità di lotta alla criminalità, la Corte ha rilevato in particolare che tale obiettivo riguarda la repressione dei reati commessi, a prescindere dalla cittadinanza dei loro autori. Pertanto, per uno Stato membro, la situazione dei suoi cittadini non può differire da quella dei cittadini degli altri Stati membri dell'Unione soggiornanti nel suo territorio per quanto riguarda l'obiettivo della lotta alla criminalità. Di conseguenza, la disparità di trattamento tra i cittadini di tale Stato membro e gli altri cittadini dell'Unione, occasionata dal trattamento sistematico, a fini di lotta alla criminalità, dei dati personali dei soli cittadini dell'Unione non aventi la nazionalità dello Stato membro in questione, costituisce una discriminazione vietata dall'articolo 12, paragrafo 1, CE (punti 78-80).

Sentenza del 24 novembre 2011, ASNEF e FECEMD (C-468/10 e C-469/10, EU:C:2011:777)

L'Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), da una parte, e la Federación de Comercio Electrónico y Marketing Directo (FECEMD), dall'altra, avevano proposto dinanzi al Tribunal Supremo (Spagna) un contenzioso amministrativo contro diversi articoli del regio decreto 1720/2007 che aveva dato attuazione alla legge organica 15/1999 che recepisce la direttiva 95/46/CE.

In particolare, l'ASNEF e la FECEMD osservavano che il diritto spagnolo, per permettere il trattamento dei dati personali, senza il consenso della persona interessata, aggiungeva una condizione che non esiste nella direttiva 95/46/CE, esigendo che detti dati comparissero in «fonti accessibili al pubblico», come elencate all'articolo 3, lettera j), della legge organica 15/1999. In proposito, avevano sostenuto che tale legge e il regio decreto 1720/2007 restringessero la portata dell'articolo 7, lettera f), della direttiva 95/46/CE, che subordina il trattamento di dati personali, in assenza del consenso della persona interessata, a una condizione che attiene unicamente all'interesse legittimo perseguito dal responsabile del trattamento oppure dal o dai terzi cui vengono comunicati i dati.

In proposito, la Corte ha anzitutto rilevato che l'articolo 7 della direttiva 95/46/CE prevede un elenco esaustivo e tassativo dei casi in cui il trattamento dei dati personali può essere considerato lecito in assenza del consenso della persona interessata. Gli Stati membri non possono, di conseguenza, introdurre, ai sensi dell'articolo 5 di detta direttiva, principi relativi alla legittimazione del trattamento dei dati personali diversi da quelli enunciati all'articolo 7, né modificare con requisiti supplementari la portata dei principi previsti da detto articolo 7. Infatti, l'articolo 5 autorizza gli Stati membri soltanto a precisare, nei limiti delle disposizioni del capo II di detta direttiva e, quindi, dell'articolo 7 della stessa, le condizioni alle quali i trattamenti dei dati personali sono leciti (punti 30, 32, 33).

In particolare, al fine di effettuare la necessaria ponderazione dei diritti e degli interessi contrapposti in gioco, prevista all'articolo 7, lettera f), di detta direttiva, gli Stati membri possono fissare linee direttrici. Essi possono altresì prendere in considerazione il fatto che la gravità della violazione dei diritti

fondamentali della persona interessata da tale trattamento possa variare in funzione della circostanza che i dati di cui trattasi figurino già, o no, in fonti accessibili al pubblico (punti 44 e 46).

Tuttavia, la Corte ha considerato che se una normativa nazionale esclude per talune categorie di dati personali la possibilità di essere trattati, stabilendo per tali categorie, 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, essa non può essere definita in termini di precisazione ai sensi dell'articolo 5 della direttiva 95/46/CE. Di conseguenza, la Corte ha concluso che l'articolo 7, lettera f), della direttiva 95/46/CE osta a che uno Stato membro escluda in modo categorico e generalizzato la possibilità che talune categorie di dati personali siano oggetto di trattamento, senza consentire la ponderazione dei diritti e degli interessi contrapposti in gioco nel caso specifico (punti 47, 48).

Sentenza del 19 ottobre 2016, Breyer (C-582/14, EU:C:2016:779)

In tale sentenza (v. altresì la rubrica II.2., intitolata «Nozione di "dati personali"»), la Corte di giustizia si è, altresì, pronunciata sulla questione se l'articolo 7, lettera f), della direttiva 95/46/CE osti ad una disposizione di diritto nazionale in forza della quale il fornitore di servizi di media online può raccogliere e impiegare i dati personali di un utente senza il suo consenso solo nella misura in cui ciò sia necessario per consentire e fatturare l'effettiva fruizione del medium online da parte del rispettivo utente e secondo la quale il fine di assicurare il funzionamento in generale di detto medium non può giustificare l'impiego dei dati oltre il termine della rispettiva fruizione.

La Corte ha dichiarato che l'articolo 7, lettera f), della direttiva 95/46/CE osta alla normativa di cui trattasi. Infatti, in forza di tale disposizione, il trattamento di dati personali ai sensi di tale disposizione è lecito 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 fondamentali della persona interessata. Orbene, nel caso di specie, la normativa tedesca aveva escluso in modo categorico e generalizzato la possibilità che talune categorie di dati personali fossero oggetto di trattamento, senza consentire la ponderazione dei diritti e degli interessi contrapposti in gioco nel caso specifico. Così facendo, essa aveva illecitamente ridotto la portata di tale principio previsto all'articolo 7, lettera f), della direttiva 95/46/CE, escludendo che l'obiettivo di garantire il funzionamento generale dei siti del medium online potesse essere oggetto di ponderazione con l'interesse o i diritti e le libertà fondamentali degli utenti (punti 62-64, disp. 2).

Sentenza del 4 maggio 2017, Rīgas satiksme (C-13/16, EU:C:2017:336)

Tale causa si inscrive nell'ambito di una controversia tra la polizia nazionale lettone e la Rīgas satiksme, società di filobus della città di Riga, relativamente a una richiesta di comunicazione dei dati identificativi dell'autore di un incidente. Nel caso di specie, in occasione di un sinistro stradale, un tassista aveva parcheggiato il suo veicolo al bordo della strada. Mentre un filobus della Rīgas satiksme passava accanto al taxi, il passeggero che occupava il sedile posteriore del medesimo aveva aperto la portiera e questa aveva urtato il filobus, danneggiandolo. Ai fini della presentazione di un ricorso di diritto civile, la Rīgas satiksme aveva, tra l'altro, chiesto alla polizia nazionale la comunicazione dei dati identificativi dell'autore dell'incidente. La polizia aveva rifiutato di comunicare il numero del documento di identità e il domicilio del passeggero nonché i documenti relativi alle spiegazioni delle persone coinvolte nell'incidente per il motivo che i documenti relativi a un procedimento amministrativo sanzionatorio potevano essere trasmessi unicamente alle parti di tale procedimento, e, per quanto riguardava il numero del documento di identità e il domicilio, la legge sulla protezione dei dati personali vietava la divulgazione di simili informazioni concernenti soggetti privati.

In tali circostanze, l'Augstākās tiesas Administratīvo lietu departaments (Corte suprema, Sezione del contenzioso amministrativo, Lettonia) ha deciso di sottoporre alla Corte di giustizia la questione se l'articolo 7, lettera f), della direttiva 95/46/CE imponga l'obbligo di comunicare dati personali a un terzo, al fine di consentirgli di proporre un ricorso per risarcimento dinanzi a un giudice civile per un danno causato dalla persona interessata dalla tutela di tali dati, e se il fatto che detta persona sia minorenne possa essere rilevante ai fini dell'interpretazione di tale disposizione.

La Corte ha dichiarato che l'articolo 7, lettera f), della direttiva 95/46/CE deve essere interpretato nel senso che non impone l'obbligo di comunicare dati personali a un terzo al fine di consentirgli di proporre un ricorso per risarcimento dinanzi a un giudice civile per un danno causato dalla persona interessata dalla tutela di tali dati. Tuttavia, detta disposizione non osterebbe a una comunicazione siffatta, qualora quest'ultima fosse effettuata in base al diritto nazionale, nel rispetto delle condizioni previste da tale disposizione (punti 27, 34 e disp.).

In tale contesto, la Corte ha rilevato che, fatte salve le verifiche che devono essere effettuate a tale riguardo dal giudice nazionale, non appare giustificato, in una situazione come quella di cui al procedimento principale, rifiutare di comunicare a una parte lesa dati personali necessari per proporre un ricorso per risarcimento contro l'autore del danno o, se del caso, le persone che esercitano la potestà genitoriale, per il fatto che detto autore sarebbe minorenne (punto 33).

Sentenza del 27 settembre 2017, Puškár (C-73/16, EU:C:2017:725)

Nell'ambito del procedimento principale, il sig. Puškár aveva presentato un ricorso dinanzi al Najvyšší súd Slovenskej republiky (Corte suprema della Repubblica slovacca) volto ad ottenere che fosse ingiunto al Finančné riaditel'stvo (Direzione delle Finanze), a tutte le autorità fiscali a esso subordinate e al Kriminálny úrad finančnej správy (Ufficio Crimini dell'amministrazione finanziaria) di non iscrivere il suo nome nell'elenco di persone considerate dalla Direzione delle Finanze dei prestanome, quale stabilito da quest'ultima ai fini della riscossione delle imposte e aggiornato a cura della Direzione delle Finanze medesima, nonché dell'Ufficio Crimini dell'amministrazione finanziaria (in prosieguo: l'«elenco controverso»). Inoltre, egli aveva chiesto di cancellare qualsiasi indicazione che lo riguardasse da tali elenchi e dal sistema informatico dell'Amministrazione finanziaria.

In tali circostanze, il Najvyšší súd ha investito la Corte di giustizia, in particolare, della questione se sia possibile interpretare il diritto al rispetto della vita privata e familiare, del domicilio e delle comunicazioni, sancito all'articolo 7, e il diritto alla protezione dei dati di carattere personale, sancito all'articolo 8 della Carta, nel senso che uno Stato membro non può, senza il consenso della persona interessata, compilare elenchi di dati personali ai fini della riscossione delle imposte, tale che l'acquisizione di dati personali nella disponibilità di un'autorità pubblica ai fini della lotta contro la frode fiscale sarebbe di per sé rischiosa.

La Corte ha concluso che l'articolo 7, lettera e), della direttiva 95/46/CE non osta a un trattamento dei dati personali da parte delle autorità di uno Stato membro ai fini della riscossione delle imposte e della lotta alla frode fiscale, come quello a cui si procede con la redazione di un elenco di persone del tipo oggetto del procedimento principale, senza il consenso delle persone interessate, a condizione, da un lato, che a tali autorità siano stati affidati compiti di interesse pubblico dalla normativa nazionale ai sensi di detta disposizione, la redazione di tale elenco e l'iscrizione in quest'ultimo del nome delle persone interessate siano effettivamente idonee e necessarie al raggiungimento degli obiettivi perseguiti e sussistano elementi sufficienti per presumere che le persone interessate figurino a ragione in tale elenco e, dall'altro lato, che siano soddisfatte tutte le condizioni di liceità di tale trattamento dei dati personali imposte dalla direttiva 95/46/CE (punto 117, disp. 3).

In proposito, la Corte ha rilevato che incombe al giudice nazionale verificare se la redazione dell'elenco controverso sia necessaria all'espletamento dei compiti di interesse pubblico di cui al procedimento

principale, tenendo conto, in particolare, della finalità esatta della redazione dell'elenco controverso, degli effetti giuridici a cui sono sottoposte le persone che vi sono iscritte e del carattere pubblico o meno di tale elenco. Inoltre, con riferimento al principio di proporzionalità, spetta al giudice nazionale verificare se la redazione dell'elenco controverso e l'iscrizione in quest'ultimo del nome delle persone interessate siano atte a conseguire gli obiettivi perseguiti dalle stesse e se non sussistano altri mezzi meno restrittivi per raggiungere tali obiettivi (punti 111, 112, 113).

Inoltre, la Corte ha constatato che il fatto di essere iscritta nell'elenco controverso può pregiudicare i diritti di una persona. L'inclusione in tale elenco potrebbe, per esempio, nuocere alla sua reputazione e incidere sui suoi rapporti con le autorità fiscali. Allo stesso tempo, tale menzione potrebbe ledere la presunzione di innocenza di tale persona, sancita dall'articolo 48, paragrafo 1, della Carta, nonché la libertà d'impresa – ai sensi dell'articolo 16 della Carta – delle persone giuridiche collegate alle persone fisiche iscritte nell'elenco controverso. Di conseguenza, una tale ingerenza potrebbe risultare proporzionata solo ove sussistano elementi sufficienti a fondamento del sospetto che l'interessato rivesta funzioni direttive fittizie all'interno delle persone giuridiche ad esso collegate e pregiudichi, così, la riscossione delle imposte e la lotta alla frode fiscale (punto 114).

Peraltro, la Corte ha ritenuto che se sussistessero motivi per limitare, in forza dell'articolo 13 della direttiva 95/46/CE, taluni dei diritti previsti agli articoli 6 e da 10 a 12 della medesima direttiva, quale il diritto all'informazione della persona interessata, una siffatta restrizione dovrebbe essere necessaria alla tutela di un interesse previsto al paragrafo 1 di detto articolo 13, come lo è, in particolare, un rilevante interesse economico e finanziario in materia tributaria, e basarsi su disposizioni legislative (punto 116).

III. Trasferimento di dati personali verso paesi terzi

Sentenza del 6 novembre 2003 (Seduta plenaria), Lindqvist (C-101/01, EU:C:2003:596)[19]

In tale causa (v. altresì la rubrica II.3., intitolata «Nozione di "trattamento di dati personali"»), il giudice del rinvio intendeva sapere, in particolare, se la sig.ra Lindqvist avesse realizzato un trasferimento di dati verso un paese terzo ai sensi di detta direttiva.

La Corte ha dichiarato che non si configura un «trasferimento verso un paese terzo di dati», ai sensi dell'articolo 25 della direttiva 95/46/CE, allorché una persona che si trova in uno Stato membro inserisce in una pagina Internet – caricata presso una persona fisica o giuridica che ospita («web hosting» provider) il sito Internet nel quale la pagina può essere consultata e che è stabilita nello Stato stesso o in un altro Stato membro – dati personali, rendendoli così accessibili a chiunque si colleghi ad Internet, compresi coloro che si trovano in paesi terzi (punto 71, disp. 4).

Infatti, tenuto conto, da una parte, dello stato dello sviluppo di Internet all'epoca dell'elaborazione della direttiva 95/46/CE e, dall'altra, della mancanza di criteri applicabili all'uso di Internet nel suo capo IV, il quale include detto articolo 25, che mira a garantire un controllo da parte degli Stati membri sui trasferimenti di dati personali verso i paesi terzi e a vietare tali trasferimenti quando essi non offrono un livello di protezione adeguato, non si può presumere che il legislatore comunitario avesse l'intenzione di includere prospettivamente nella nozione di «trasferimento verso un paese terzo di dati» un siffatto inserimento di dati in una pagina Internet, anche se questi sono così resi accessibili alle persone di paesi terzi in possesso dei mezzi tecnici per consultarli (punti 63, 64, 68).

19 Tale sentenza è stata presentata nella Relazione annuale 2003, pag. 67.

Sentenza del 6 ottobre 2015 (Grande Sezione), Schrems (C-362/14, EU:C:2015:650)[20]

Il sig. Schrems, cittadino austriaco e iscritto alla rete sociale Facebook, aveva depositato una denuncia dinanzi al Data Protection Commissioner (commissario per la protezione dei dati, Irlanda) per il fatto che Facebook Ireland trasferiva negli Stati Uniti i dati personali dei propri utenti e li conservava su server ubicati in tale paese, ove erano oggetto di un trattamento. Secondo il sig. Schrems, il diritto e la prassi degli Stati Uniti non offrivano una protezione sufficiente contro il controllo, da parte delle autorità pubbliche, dei dati trasferiti verso tale paese. Il Data Protection Commissioner aveva rifiutato di istruire tale denuncia, per il motivo, in particolare, che nella sua decisione 2000/520/CE[21], la Commissione aveva considerato che, nel contesto del cosiddetto regime dell'«approdo sicuro» (in inglese, «safe harbour»)[22], gli Stati Uniti garantivano un livello adeguato di protezione dei dati personali trasferiti.

In tale contesto la Corte di giustizia è stata investita dalla High Court (Alta Corte, Irlanda) di una domanda di interpretazione dell'articolo 25, paragrafo 6, della direttiva 95/46/CE, in forza del quale la Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato per i dati trasferiti, nonché, in sostanza, di una domanda volta a stabilire la validità della decisione 2000/520/CE adottata dalla Commissione sulla base di detto articolo 25, paragrafo 6, della direttiva 95/46/CE.

La Corte ha dichiarato invalida la decisione della Commissione nel suo complesso, sottolineando, anzitutto, che la sua adozione richiedeva la constatazione, debitamente motivata, da parte della Commissione, che il paese terzo di cui trattasi garantisse effettivamente un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell'ordinamento giuridico dell'Unione. Orbene, nella misura in cui la Commissione, nella sua decisione 2000/520/CE, non ha affermato ciò, l'articolo 1 di tale decisione viola i requisiti fissati all'articolo 25, paragrafo 6, della direttiva 95/46/CE, letto alla luce della Carta, ed esso è, per tale motivo, invalido. Infatti, i principi dell'«approdo sicuro» sono applicabili soltanto alle organizzazioni americane autocertificate che ricevono dati personali dall'Unione, mentre dalle autorità pubbliche americane non si esige il rispetto di detti principi. Inoltre, la decisione 2000/520/CE rende possibili ingerenze nei diritti fondamentali delle persone i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti, senza contenere dichiarazioni quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze in tali diritti e senza menzionare l'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di tale natura (punti 82, 87-89, 96-98, disp. 2).

Inoltre, la Corte ha dichiarato invalido l'articolo 3 della decisione 2000/520/CE, nella parte in cui priva le autorità nazionali di controllo dei poteri che esse traggono dall'articolo 28 della direttiva 95/46/CE, nel caso in cui una persona adduca elementi idonei a rimettere in discussione il fatto che una decisione della Commissione che ha constatato che un paese terzo garantisce un livello di protezione adeguato sia compatibile con la protezione della vita privata, delle libertà e dei diritti fondamentali della persona. (punti 102-104). La Corte ha concluso che l'invalidità degli articoli 1 e 3 della decisione 2000/520/CE inficiava la validità di tale decisione nel suo complesso (punti 105, 106).

Riguardo all'impossibilità di giustificare una siffatta ingerenza, la Corte ha osservato, anzitutto, che una normativa dell'Unione che comporta un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati contro il rischio di abusi, nonché contro eventuali accessi e usi illeciti dei suddetti dati. La necessità di disporre di siffatte

20 Tale sentenza è stata presentata nella Relazione annuale 2015, pag. 53.

21 Decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti (GU L 215 del 25.8.2000, pag. 7).

22 Il regime dell'approdo sicuro include una serie di principi relativi alla tutela dei dati personali ai quali le imprese americane possono aderire volontariamente.

garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi (punto 91).

Inoltre, e soprattutto, la protezione del diritto fondamentale al rispetto della vita privata a livello dell'Unione richiede che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario (punto 92). In tal senso, non è limitata allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione senza operare alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta (punto 93). In particolare, una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudica il contenuto essenziale del diritto fondamentale al rispetto della vita privata. Analogamente, una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati, non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta (punti 94, 95).

Parere 1/15 (Accordo PNR UE-Canada) del 26 luglio 2017 (Grande Sezione) (EU:C:2017:592)

Il 26 luglio 2017 la Corte di giustizia si è pronunciata per la prima volta sulla compatibilità di un progetto di accordo internazionale con la Carta dei diritti fondamentali dell'Unione europea e, in particolare, con le disposizioni relative al rispetto della vita privata nonché alla protezione dei dati di carattere personale.

L'Unione europea e il Canada hanno negoziato un accordo sul trasferimento e sul trattamento dei dati del codice di prenotazione (Passenger Name Record – PNR) (accordo PNR) che è stato firmato nel 2014. Poiché il Consiglio dell'Unione europea ne ha chiesto la ratifica al Parlamento europeo, quest'ultimo ha deciso di adire la Corte di giustizia al fine di sapere se l'accordo previsto fosse conforme al diritto dell'Unione.

L'accordo previsto consente il trasferimento sistematico e continuo dei dati PNR di tutti i passeggeri aerei a un'autorità canadese in vista del loro uso e della loro conservazione, nonché del loro eventuale trasferimento successivo ad altre autorità e ad altri paesi terzi, a fini di contrasto del terrorismo e di gravi forme di criminalità transnazionale. A tale scopo, l'accordo previsto prevede, tra l'altro, una durata di archiviazione dei dati di cinque anni e stabilisce particolari condizioni in materia di sicurezza e di integrità dei PNR, come un mascheramento immediato dei dati sensibili, così come prevede diritti di accesso ai dati, di rettifica e di cancellazione degli stessi e la possibilità di presentare ricorsi amministrativi o giudiziari.

I dati PNR presi in considerazione dall'accordo previsto includono, in particolare, oltre al nome e alle informazioni di contatto del o dei passeggeri aerei, informazioni necessarie alla prenotazione, come le date previste del viaggio e l'itinerario di viaggio, informazioni relative ai biglietti, i gruppi di persone registrate sotto lo stesso numero di prenotazione, informazioni relative ai mezzi di pagamento o alla fatturazione, informazioni concernenti i bagagli nonché osservazioni generali riguardo ai passeggeri.

Nel proprio parere, la Corte ha dichiarato che l'accordo PNR non può essere concluso nella sua forma attuale a causa dell'incompatibilità di diverse sue disposizioni con i diritti fondamentali riconosciuti dall'Unione.

La Corte ha constatato, in primo luogo, che sia il trasferimento dei dati PNR dall'Unione all'autorità canadese competente sia la disciplina negoziata dall'Unione con il Canada delle condizioni attinenti alla conservazione di detti dati, al loro uso nonché ai loro eventuali trasferimenti ulteriori ad altre autorità

canadesi, a Europol, a Eurojust, alle autorità giudiziarie o di polizia degli Stati membri o ancora ad autorità di altri paesi terzi, costituiscono ingerenze nel diritto garantito all'articolo 7 della Carta. Tali operazioni integrano altresì un'ingerenza nel diritto fondamentale alla protezione dei dati personali garantito all'articolo 8 della Carta poiché esse costituiscono trattamenti di dati personali (punti 125, 126).

Inoltre, essa ha sottolineato che anche se taluni dati PNR, considerati isolatamente, non sembrano poter rivelare informazioni importanti sulla vita privata degli interessati, tuttavia, considerati complessivamente, detti dati possono, tra l'altro, rivelare un itinerario di viaggio completo, abitudini di viaggio, relazioni esistenti tra due o più persone nonché informazioni sulla situazione finanziaria dei passeggeri aerei, sulle loro abitudini alimentari o sul loro stato di salute, e potrebbero persino fornire informazioni sensibili su tali passeggeri, come definite all'articolo 2, lettera e), dell'accordo previsto (informazioni che rivelano l'origine etnica o razziale, le opinioni politiche, le convinzioni religiose, ecc.) (punto 128).

A tal proposito, la Corte ha considerato che, benché le ingerenze in esame possano essere giustificate dal perseguimento di una finalità d'interesse generale (garanzia della sicurezza pubblica nel contesto del contrasto dei reati di terrorismo e della criminalità transnazionale grave), varie disposizioni dell'accordo non sono limitate allo stretto necessario e non prevedono norme chiare e precise.

In particolare, la Corte ha rilevato che, in considerazione del rischio di un trattamento contrario al principio di non discriminazione, un trasferimento dei dati sensibili verso il Canada richiederebbe una giustificazione precisa e particolarmente solida, vertente su motivi diversi dalla protezione della sicurezza pubblica contro il terrorismo e i reati gravi di natura transnazionale. Orbene, nella fattispecie, una siffatta giustificazione manca. La Corte ne ha tratto la conclusione che le disposizioni dell'accordo sul trasferimento dei dati sensibili verso il Canada nonché sul trattamento e sulla conservazione di tali dati sono incompatibili con i diritti fondamentali (punti 165, 232).

In secondo luogo, la Corte ha ritenuto che, dopo la partenza dei passeggeri aerei dal Canada, l'archiviazione continua dei dati PNR di tutti i passeggeri aerei consentita dall'accordo previsto non sia limitata allo stretto necessario. Infatti, per quanto riguarda i passeggeri aerei per i quali un rischio in materia di terrorismo o di reati gravi di natura transnazionale non è stato individuato al loro arrivo in Canada e fino alla loro partenza da tale paese, non sembra che esista, una volta ripartiti, alcun rapporto, sia pure indiretto, tra i loro dati PNR e l'obiettivo perseguito dall'accordo previsto, che giustifichi la conservazione di tali dati. Invece, un'archiviazione dei dati PNR dei passeggeri aerei rispetto ai quali sono identificati elementi obiettivi che consentano di ritenere che possano, anche dopo la loro partenza dal Canada, presentare un rischio in termini di lotta al terrorismo e ai reati gravi di natura transnazionale è ammissibile al di là del loro soggiorno in tale paese, anche per una durata di cinque anni (punti 205-207, 209).

In terzo luogo, la Corte ha constatato che il diritto fondamentale al rispetto della vita privata, sancito dall'articolo 7 della Carta dei diritti fondamentali dell'Unione europea, implica che l'interessato possa assicurarsi che i suoi dati personali siano trattati in modo corretto e lecito. Al fine di poter effettuare le necessarie verifiche, tale persona deve disporre del diritto d'accesso ai dati che la riguardano che sono oggetto di trattamento.

In proposito, essa ha sottolineato che, nell'accordo previsto, occorre che i passeggeri aerei siano informati del trasferimento dei loro dati del codice di prenotazione verso il paese terzo interessato e dell'uso di tali dati, a partire dal momento in cui tale comunicazione non è suscettibile di compromettere le indagini condotte dalle autorità pubbliche contemplate dall'accordo previsto. Infatti, una siffatta informazione è, de facto, necessaria per consentire ai passeggeri aerei di esercitare i loro diritti di richiedere l'accesso ai dati che li riguardano e, se del caso, la rettifica degli stessi nonché di proporre, conformemente all'articolo 47, primo comma, della Carta, un ricorso effettivo dinanzi a un giudice.

Pertanto, risulta necessario informare individualmente i passeggeri aerei nelle ipotesi nelle quali si presentino elementi obiettivi che giustificano l'uso dei dati del codice di prenotazione a fini di contrasto del terrorismo e di reati gravi di natura transnazionale e che richiedono una previa autorizzazione di un'autorità giudiziaria o di un ente amministrativo indipendente. Lo stesso vale nei casi in cui i dati del codice di prenotazione dei passeggeri aerei siano comunicati ad altre autorità pubbliche o a privati. Tuttavia, una siffatta informazione deve avvenire soltanto a partire dal momento in cui essa non può compromettere le indagini condotte dalle autorità pubbliche contemplate dall'accordo previsto (punti 219, 220, 223, 224).

IV. La tutela dei dati personali in Internet

1. Diritto di opposizione al trattamento dei dati personali («diritto all'oblio»)

Sentenza del 13 maggio 2014 (Grande Sezione), Google Spain e Google (C-131/12, EU:C:2014:317)

In tale sentenza (v. altresì la rubrica II.3., intitolata «Nozione di "trattamento di dati personali"»), la Corte di giustizia ha precisato la portata dei diritti di accesso e di opposizione al trattamento dei dati personali in Internet, previsti dalla direttiva 95/46/CE.

Così, allorché si è pronunciata sulla questione dell'estensione della responsabilità del gestore di un motore di ricerca in Internet, la Corte, in sostanza, ha dichiarato che al fine di rispettare i diritti di accesso e di opposizione garantiti dagli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46/CE, e sempre che le condizioni fissate in tali articoli siano soddisfatte, tale gestore, in talune circostanze, è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, i link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona. La Corte ha precisato che un siffatto obbligo può sussistere anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita (punto 88, disp. 3).

Peraltro, interrogata sulla questione se la direttiva consenta alla persona interessata di chiedere che i link verso pagine web siano soppressi da un tale elenco di risultati a motivo del fatto che la medesima desidererebbe l'«oblio» dopo un certo tempo delle informazioni in esse contenute relative alla sua persona, la Corte rileva, anzitutto, che anche un trattamento inizialmente lecito di dati esatti può divenire, con il tempo, incompatibile con la direttiva suddetta qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati, in particolare nel caso in cui i dati risultino inadeguati, non siano pertinenti o non lo siano più, o ancora appaiano eccessivi in rapporto alle finalità suddette e al tempo trascorso (punto 93). Pertanto, nell'ipotesi in cui si constati, in seguito a una domanda della persona interessata, che l'inclusione nell'elenco di tali link è, allo stato attuale, incompatibile con la direttiva, le informazioni e i link che compaiono nel suddetto elenco devono essere cancellati (punto 94). In tale contesto, la constatazione di un diritto della persona interessata a che l'informazione riguardante la sua persona non venga più collegata al suo nome da un elenco di risultati non presuppone che l'inclusione dell'informazione in questione nell'elenco di risultati arrechi un pregiudizio all'interessato (punto 96, disp. 4).

Infine, la Corte ha precisato che, dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico mediante la sua inclusione in un siffatto elenco di risultati, tali diritti prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, mediante l'inclusione summenzionata, all'informazione di cui trattasi (punto 97, disp. 4).

2. Trattamento dei dati personali e diritti di proprietà intellettuale

Sentenza del 29 gennaio 2008 (Grande Sezione), Promusicae (C-275/06, EU:C:2008:54)[23]

La Promusicae, un'associazione spagnola senza scopo di lucro di cui fanno parte produttori ed editori di registrazioni musicali e di registrazioni audiovisive, aveva adito i tribunali spagnoli al fine di ingiungere alla Telefónica de España SAU (società commerciale la cui attività consiste, in particolare, nella fornitura di servizi di accesso a Internet) di rivelare l'identità e l'indirizzo fisico di talune persone alle quali quest'ultima forniva un servizio di accesso ad Internet e il cui indirizzo IP, nonché la data e l'ora di connessione, erano noti. Secondo la Promusicae, tali persone utilizzavano il programma di scambio di archivi cosiddetto «peer-to-peer» o «P2P» (mezzo trasparente di condivisione di contenuti, indipendente, decentralizzato e munito di funzioni di ricerca e di download avanzate) e consentivano l'accesso, nelle cartelle condivise del loro computer, a fonogrammi i cui diritti patrimoniali di utilizzo spettavano ai soci della Promusicae. Essa aveva pertanto richiesto che le fossero comunicate le suddette informazioni per poter esercitare azioni civili contro le persone coinvolte.

In tali circostanze, lo Juzgado de lo Mercantil n. 5 di Madrid (Tribunale commerciale n. 5 di Madrid, Spagna) ha sottoposto alla Corte di giustizia la questione se la legislazione europea imponga agli Stati membri di istituire, al fine di garantire l'effettiva tutela del diritto d'autore, l'obbligo di comunicare taluni dati personali nel contesto di un procedimento civile.

Secondo la Corte, detta domanda di pronuncia pregiudiziale ha sollevato la questione della necessaria conciliazione degli obblighi connessi alla tutela di diversi interessi fondamentali: da una parte, il diritto al rispetto della vita privata e, dall'altra, i diritti alla tutela della proprietà e ad un ricorso effettivo.

In proposito, la Corte ha concluso che le direttive 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»)[24], 2001/29/CE, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione[25], 2004/48/CE, sul rispetto dei diritti di proprietà intellettuale[26], e 2002/58/CE non impongono agli Stati membri, in una situazione come quella oggetto della causa principale, di istituire un obbligo di comunicare dati personali per garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento civile. Tuttavia, il diritto dell'Unione richiede che i detti Stati, in occasione della trasposizione di tali direttive, abbiano cura di fondarsi su un'interpretazione delle medesime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati

23 Tale sentenza è stata presentata nella Relazione annuale 2008, pag. 46.

24 Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («direttiva sul commercio elettronico») (GU L 178 del 17.7.2000, pag. 1).

25 Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione (GU L 167 del 22.6.2001, pag. 10).

26 Direttiva 2004/48/CE del Parlamento europeo e del Consiglio, del 29 aprile 2004, sul rispetto dei diritti di proprietà intellettuale (GU L 157 del 30.4.2004, pag. 45, e rettifica GU L 195 del 2.6.2004, pag. 16).

dall'ordinamento giuridico comunitario. Inoltre, in sede di attuazione delle misure di recepimento di dette direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali direttive, ma anche evitare di fondarsi su un'interpretazione delle medesime che entri in conflitto con detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come, ad esempio, il principio di proporzionalità (punto 70 e disp.).

Sentenza del 24 novembre 2011, Scarlet Extended (C-70/10, EU:C:2011:771)[27]

La société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) aveva constatato che alcuni utenti di Internet, che si avvalevano dei servizi della Scarlet Extended SA, fornitore di accesso ad Internet (in prosieguo: la «Scarlet»), scaricavano da Internet, senza autorizzazione e senza pagarne i diritti, opere contenute nel suo catalogo utilizzando reti «peer-to-peer». La SABAM aveva adito il giudice nazionale e ottenuto, in primo grado, la pronuncia, nei confronti della Scarlet, di un'ingiunzione a far cessare tali violazioni del diritto d'autore rendendo impossibile qualsiasi forma, realizzata mediante un programma «peer-to-peer», di invio o di ricezione, da parte dei suoi clienti, di file che contenessero un'opera musicale appartenente al repertorio della SABAM.

Adita dalla Scarlet, la cour d'appel de Bruxelles (Corte d'appello di Bruxelles, Belgio) ha sospeso il procedimento al fine di chiedere alla Corte di giustizia, in via pregiudiziale, se una simile ingiunzione fosse compatibile con il diritto europeo.

La Corte ha dichiarato che le direttive 95/46/CE, 2000/31/CE, 2001/29/CE, 2002/58/CE e 2004/48/CE, 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 alla Scarlet 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 applichi indistintamente a tutta la sua clientela, a titolo preventivo, a sue spese esclusive, senza limiti nel tempo e che sia idoneo ad identificare nella rete di tale fornitore la circolazione di file contenenti un'opera musicale, cinematografica o audiovisiva rispetto alla quale il richiedente affermi di vantare diritti di proprietà intellettuale, onde bloccare il trasferimento di file il cui scambio pregiudichi il diritto d'autore (punto 54 e disp.).

Infatti, secondo la Corte, una simile ingiunzione non rispetta il divieto, sancito dall'articolo 15, paragrafo 1, della direttiva 2000/31/CE, di imporre a un tale prestatore un obbligo generale di sorveglianza, né l'esigenza di garantire un giusto equilibrio tra, da un lato, la tutela del diritto di proprietà intellettuale e, dall'altro, la libertà d'impresa e il diritto alla tutela dei dati personali e la libertà di ricevere o di comunicare informazioni (punti 40, 49).

In tale contesto, la Corte ha rilevato che, da un lato, 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 (punto 51). Dall'altro, detta ingiunzione rischierebbe di ledere la libertà di informazione, poiché tale sistema potrebbe non essere in grado di distinguere adeguatamente tra un contenuto lecito ed un contenuto illecito, sicché il suo impiego potrebbe produrre il risultato di bloccare comunicazioni aventi un contenuto lecito. Infatti, è indiscusso che la questione della liceità di una trasmissione dipende anche dall'applicazione di eccezioni di legge al diritto di autore che variano da uno Stato membro all'altro. Inoltre, in certi Stati membri talune opere possono rientrare nel pubblico dominio o possono essere state messe in linea gratuitamente da parte dei relativi autori (punto 52).

27 Tale sentenza è stata presentata nella Relazione annuale 2011, pag. 37.

Pertanto, la Corte ha dichiarato che, adottando l'ingiunzione che costringe la Scarlet a predisporre il sistema di filtraggio controverso, il giudice nazionale in questione non rispetterebbe l'obbligo di garantire un giusto equilibrio tra, da un lato, il diritto di proprietà intellettuale e, dall'altro, la libertà di impresa, il diritto alla tutela dei dati personali e la libertà di ricevere o di comunicare informazioni (punto 53).

Sentenza del 19 aprile 2012, Bonnier Audio e a. (C-461/10, EU:C:2012:219)

L'Högsta domstolen (Corte suprema, Svezia) ha adito la Corte di giustizia in via pregiudiziale affinché interpretasse le direttive 2002/58/CE e 2004/48/CE, nell'ambito di una controversia tra la Bonnier Audio AB, l'Earbooks AB, la Norstedts Förlagsgrupp AB, la Piratförlaget AB e la Storyside AB (in prosieguo: la «Bonnier Audio e a.») e la Perfect Communication Sweden AB (in prosieguo: la «ePhone») in merito all'opposizione di quest'ultima ad una domanda di ingiunzione di comunicazione di dati proposta dalla Bonnier Audio e a.

Nel caso di specie, la Bonnier Audio e a. erano case editrici titolari, segnatamente, di diritti esclusivi di riproduzione, di edizione e di messa a disposizione del pubblico di ventisette opere presentate in forma di audiolibro. Esse ritenevano che i diritti esclusivi di cui erano titolari fossero stati violati, a causa della diffusione al pubblico di tali ventisette opere, senza il loro consenso, a mezzo di un server FTP («file transfer protocol»), che consentiva la condivisione di file e il trasferimento di dati tra computer connessi a Internet. Pertanto, avevano investito i giudici svedesi di una domanda di ingiunzione al fine di ottenere la comunicazione del nome e del recapito della persona facente uso dell'indirizzo IP dal quale si presumeva fossero stati trasmessi i file in questione.

In tali circostanze, l'Högsta domstolen, investito di un ricorso per cassazione, ha sottoposto alla Corte di giustizia la questione se il diritto dell'Unione osti all'applicazione di una disposizione nazionale, introdotta in forza dell'articolo 8 della direttiva 2004/48/CE, che, in un procedimento civile e allo scopo di identificare un abbonato, permetta di ingiungere ad un operatore Internet di fornire al titolare di diritti d'autore o al suo avente causa informazioni sull'identità dell'abbonato al quale sia stato assegnato l'indirizzo IP utilizzato ai fini della violazione di detti diritti. Si presume, da un lato, che il richiedente l'ingiunzione abbia raccolto indizi effettivi dell'avvenuta violazione del diritto d'autore e, dall'altro, che la misura richiesta risulti proporzionata.

La Corte ha anzitutto ricordato che l'articolo 8, paragrafo 3, della direttiva 2004/48/CE, in combinato disposto con l'articolo 15, paragrafo 1, della direttiva 2002/58/CE, non osta a che gli Stati membri prevedano l'obbligo di trasmissione a soggetti privati di dati di carattere personale per consentire l'avvio, dinanzi ai giudici civili, di procedimenti nei confronti delle violazioni del diritto d'autore, senza peraltro imporre agli Stati medesimi di disporre tale obbligo. Tuttavia, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a dette direttive, bensì anche provvedere a non fondarsi su un'interpretazione di esse che entri in conflitto con i summenzionati diritti fondamentali o con gli altri principi generali del diritto dell'Unione, quale il principio di proporzionalità (punti 55, 56).

In proposito, la Corte ha constatato che la normativa nazionale in esame esigeva, segnatamente, che, affinché potesse essere disposta l'ingiunzione di comunicazione dei dati in questione, sussistessero indizi reali di violazione di un diritto di proprietà intellettuale su un'opera, che le informazioni richieste fossero tali da facilitare le indagini sulla violazione o sulla minaccia di violazione del diritto d'autore e che i motivi alla base di tale ingiunzione si ricollegassero ad un interesse superiore agli inconvenienti o agli altri pregiudizi che ne potessero derivare per il destinatario o a qualsivoglia altro contrapposto interesse (punto 58).

Di conseguenza, la Corte ha concluso che le direttive 2002/58/CE e 2004/48/CE non ostano ad una normativa nazionale, come quella oggetto della causa principale, nella parte in cui tale normativa consente al giudice nazionale, dinanzi al quale sia stata proposta, da parte di un soggetto legittimato ad agire, domanda di ingiunzione di comunicare dati di carattere personale, di ponderare, in funzione delle circostanze della specie e tenuto debitamente conto delle esigenze risultanti dal principio di proporzionalità, i contrapposti interessi in gioco (punto 61 e disp).

V. Autorità nazionali di controllo

1. Portata del requisito dell'indipendenza

Sentenza del 9 marzo 2010 (Grande Sezione), Commissione/Germania (C-518/07, EU:C:2010:125)[28]

Con il proprio ricorso la Commissione aveva chiesto alla Corte di voler dichiarare che la Repubblica federale di Germania era venuta meno agli obblighi ad essa incombenti ai sensi dell'articolo 28, paragrafo 1, secondo comma, della direttiva 95/46/CE, sottoponendo alla vigilanza dello Stato le autorità di controllo competenti a vegliare sul trattamento dei dati personali nei settori diversi da quello pubblico nei vari Länder e trasponendo pertanto erroneamente il requisito che le autorità garanti della protezione di tali dati siano «pienamente indipendenti».

La Repubblica federale di Germania riteneva, per parte sua, che l'articolo 28, paragrafo 1, secondo comma, della direttiva 95/46/CE richiedesse un'indipendenza funzionale delle autorità di controllo, nel senso che dette autorità devono essere indipendenti dai settori diversi da quello pubblico soggetti al loro controllo e che non devono essere esposte a influenze esterne. Orbene, a suo parere, la vigilanza dello Stato esercitata nei Länder tedeschi non costituiva una siffatta influenza esterna, bensì un meccanismo di sorveglianza interno all'amministrazione, messo in atto da autorità appartenenti al medesimo apparato amministrativo delle autorità di controllo e tenute, proprio come queste ultime, a soddisfare le finalità della direttiva 95/46/CE.

La Corte ha dichiarato che la garanzia dell'indipendenza delle autorità nazionali di controllo prevista dalla direttiva 95/46/CE è diretta ad assicurare l'efficacia e l'affidabilità del controllo del rispetto delle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali e deve essere interpretata alla luce di tale finalità. Essa non è stata disposta al fine di attribuire uno status particolare a dette autorità e ai loro agenti, bensì per rafforzare la protezione delle persone e degli organismi interessati dalle loro decisioni, e le autorità di controllo devono di conseguenza agire, nello svolgimento delle loro funzioni, in modo obiettivo ed imparziale (punto 25).

La Corte ha considerato che tali autorità di controllo competenti a vegliare sul trattamento dei dati personali nei settori diversi da quello pubblico devono godere di un'indipendenza che consenta loro di svolgere le proprie funzioni senza influenze esterne. Tale indipendenza esclude non solamente qualsiasi influenza esercitata dagli organismi controllati, ma anche qualsivoglia imposizione e ogni altra influenza esterna, diretta o indiretta, che possa rimettere in discussione lo svolgimento, da parte delle menzionate autorità, del loro compito, consistente nello stabilire un giusto equilibrio fra la protezione del diritto alla vita privata e la libera circolazione dei dati personali. Il solo rischio che le autorità di vigilanza possano esercitare un'influenza politica sulle decisioni delle competenti autorità di controllo è sufficiente ad

28 Tale sentenza è stata presentata nella Relazione annuale 2010, pag. 34.

ostacolare lo svolgimento indipendente delle funzioni di queste ultime. Da un lato, vi potrebbe essere un'«obbedienza anticipata» di tali autorità, in considerazione della prassi decisionale dell'autorità di vigilanza. Dall'altro, il ruolo di custodi del diritto alla vita privata che assumono dette autorità di controllo impone che le loro decisioni, e, quindi, esse stesse, siano al di sopra di qualsivoglia sospetto di parzialità. Secondo la Corte, la vigilanza dello Stato esercitata sulle autorità nazionali di controllo non è dunque compatibile con il requisito dell'indipendenza (punti 30, 36, 37 e disp.).

Sentenza del 16 ottobre 2012 (Grande Sezione), Commissione/Austria (C-614/10, EU:C:2012:631)

Con il suo ricorso, la Commissione aveva chiesto alla Corte di dichiarare che, non avendo adottato tutte le disposizioni necessarie affinché la normativa vigente in Austria rispondesse al criterio di indipendenza per quanto riguarda la Datenschutzkommission (commissione per la protezione dei dati), istituita quale autorità di controllo per la protezione dei dati personali, l'Austria era venuta meno agli obblighi ad essa incombenti in forza dell'articolo 28, paragrafo 1, secondo comma, della direttiva 95/46/CE.

La Corte ha constatato un inadempimento da parte dell'Austria, considerando, in sostanza, che non soddisfa il criterio di indipendenza dell'autorità di controllo, sancito dalla direttiva 95/46/CE, lo Stato membro che istituisce un contesto normativo in forza del quale il membro amministratore di detta autorità è un funzionario statale soggetto a un controllo di servizio, il cui ufficio è inserito nei servizi del governo nazionale, e su cui il capo del governo nazionale gode di un diritto incondizionato all'informazione su ogni aspetto della gestione di detta autorità (punto 66 e disp.).

La Corte, anzitutto, ha ricordato che l'espressione «pienamente indipendenti», di cui all'articolo 28, paragrafo 1, secondo comma, della direttiva 95/46/CE, implica che le autorità di controllo devono godere di un'indipendenza che consenta loro di svolgere le proprie funzioni senza influenze esterne. In proposito, la circostanza che una tale autorità goda di un'indipendenza funzionale, in quanto i suoi membri sono indipendenti e non sono vincolati ad alcuna istruzione nell'esercizio delle loro funzioni, da sola non è sufficiente per preservare la suddetta autorità di controllo da qualsiasi influenza esterna. Orbene, l'indipendenza richiesta in tale contesto mira ad escludere non soltanto l'influenza diretta, sotto forma di istruzioni, ma anche qualsiasi forma di influenza indiretta che possa orientare le decisioni dell'autorità di controllo. Peraltro, in considerazione del ruolo di custodi del diritto alla vita privata che assumono le autorità di controllo, le loro decisioni, e quindi esse stesse, devono essere al di sopra di ogni sospetto di parzialità (punti 41-43, 52).

La Corte ha precisato che, per poter soddisfare il criterio di indipendenza sancito nella summenzionata disposizione della direttiva 95/46/CE, un'autorità nazionale di controllo non deve disporre di una linea di bilancio autonoma, alla stregua di quella prevista dall'articolo 43, paragrafo 3, del regolamento (CE) n. 45/2001. Gli Stati membri non sono infatti tenuti a riprendere nella loro legislazione nazionale disposizioni analoghe a quelle del capo V del regolamento (CE) n. 45/2001 al fine di garantire una totale indipendenza alla/e loro autorità di controllo e possono quindi prevedere che, dal punto di vista del diritto in materia di bilancio, l'autorità di controllo dipenda da un determinato dipartimento ministeriale. Tuttavia, l'attribuzione delle risorse umane e materiali occorrenti a una siffatta autorità non deve impedire a quest'ultima di essere «pienamente indipendent[e]» nell'esercizio delle sue funzioni, ai sensi dell'articolo 28, paragrafo 1, secondo comma, della direttiva 95/46/CE (punto 58).

Sentenza dell'8 aprile 2014 (Grande Sezione), Commissione/Ungheria (C-288/12, EU:C:2014:237)[29]

In tale causa, la Commissione aveva chiesto alla Corte di giustizia di constatare che l'Ungheria, ponendo anticipatamente fine al mandato dell'autorità di controllo per la protezione dei dati personali, era venuta meno agli obblighi ad essa incombenti in forza della direttiva 95/46/CE 95/46/CE.

La Corte ha dichiarato che viene meno agli obblighi ad esso incombenti in forza della direttiva 95/46/CE uno Stato membro che ponga anticipatamente fine al mandato dell'autorità di controllo per la protezione dei dati personali (punto 62, disp. 1).

Infatti, secondo la Corte, l'indipendenza di cui devono godere le autorità di controllo competenti per la vigilanza del trattamento di detti dati esclude in particolare qualsiasi imposizione e ogni altra influenza esterna di qualunque forma, sia diretta che indiretta, che possano orientare le loro decisioni e che potrebbero quindi rimettere in discussione lo svolgimento, da parte di dette autorità, del loro compito, consistente nello stabilire un giusto equilibrio tra la protezione del diritto alla vita privata e la libera circolazione dei dati personali (punto 51).

La Corte ha inoltre ricordato che, poiché l'indipendenza funzionale non è sufficiente, di per se stessa, per preservare le autorità di controllo da qualsiasi influenza esterna, il solo rischio che le autorità responsabili di uno Stato possano esercitare un'influenza politica sulle decisioni delle autorità di controllo è sufficiente ad ostacolare lo svolgimento indipendente delle funzioni di queste ultime. Orbene, se fosse consentito ad ogni Stato membro di porre fine al mandato di un'autorità di controllo prima del relativo termine inizialmente previsto senza rispettare le norme e le garanzie prestabilite a tal fine dalla legislazione applicabile, la minaccia di una tale cessazione anticipata incombente su detta autorità durante l'intero esercizio del suo mandato potrebbe condurre ad una forma di obbedienza al potere politico in capo alla stessa, incompatibile con detto requisito dell'indipendenza. Inoltre, in una tale situazione, non potrebbe ritenersi che l'autorità di controllo possa agire, in ogni circostanza, al di sopra di qualsivoglia sospetto di parzialità (punti 52-55).

2. Determinazione del diritto applicabile e dell'autorità di controllo competente

Sentenza del 1° ottobre 2015, Weltimmo (C-230/14, EU:C:2015:639)[30]

La Nemzeti Adatvédelmi és Információszabadság Hatóság (autorità nazionale incaricata della protezione dei dati e della libertà dell'informazione, Ungheria) aveva comminato un'ammenda alla società Weltimmo, registrata in Slovacchia e che gestiva siti Internet di annunci immobiliari riguardanti beni situati in Ungheria, per il motivo che essa non aveva proceduto alla cancellazione dei dati personali degli inserzionisti di tali siti, nonostante la loro richiesta in tal senso, e aveva trasmesso tali dati ad agenzie di recupero crediti al fine di ottenere il pagamento di fatture insolute. Secondo l'autorità di controllo ungherese, così facendo la società Weltimmo aveva violato la legge ungherese di recepimento della direttiva 95/46/CE.

Investita di un ricorso per cassazione, la Kúria (Corte suprema, Ungheria) ha espresso dubbi riguardo alla determinazione del diritto applicabile e ai poteri di cui dispone l'autorità di controllo ungherese alla luce degli articoli 4, paragrafo 1, e 28 della direttiva 95/46/CE. Conseguentemente, essa ha sottoposto alla Corte di giustizia varie questioni pregiudiziali.

29 Tale sentenza è stata presentata nella Relazione annuale 2014, pag. 62.
30 Tale sentenza è stata presentata nella Relazione annuale 2015, pag. 55.

Riguardo al diritto nazionale applicabile, la Corte ha dichiarato che l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46/CE consente l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile del trattamento di tali dati è registrato, purché il medesimo svolga, tramite un'organizzazione stabile nel territorio di tale Stato membro, un'attività effettiva e reale, anche minima, nel contesto della quale si svolge tale trattamento. Per determinare se ciò si verifichi, il giudice del rinvio può tener conto, in particolare, del fatto, da un lato, che l'attività del responsabile di detto trattamento, nell'ambito della quale il medesimo ha luogo, consiste nella gestione di siti Internet di annunci immobiliari riguardanti beni immobili situati nel territorio di tale Stato membro e redatti nella lingua di quest'ultimo e che essa, di conseguenza, è principalmente, ovvero interamente, rivolta verso detto Stato membro. Il giudice del rinvio può, dall'altro lato, tenere conto anche del fatto che tale responsabile ha un rappresentante in detto Stato membro, il quale è incaricato di recuperare i crediti risultanti da tale attività nonché di rappresentarlo nei procedimenti amministrativo e giudiziario relativi al trattamento dei dati interessati. La Corte ha, invece, precisato che è inconferente la questione della cittadinanza delle persone interessate da tale trattamento (punto 41, disp. 1).

Riguardo alla competenza e ai poteri dell'autorità di controllo cui sia proposto un reclamo, ai sensi dell'articolo 28, paragrafo 4, della direttiva 95/46/CE, la Corte ha considerato che tale autorità può esaminare detto ricorso a prescindere dal diritto applicabile e ancor prima di sapere quale sia il diritto nazionale che si applica al trattamento controverso (punto 54). Tuttavia, essa, qualora giunga alla conclusione che si applica il diritto di un altro Stato membro, non può imporre sanzioni al di fuori del territorio del suo Stato membro. In una situazione del genere è tenuta, in virtù dell'obbligo di collaborazione di cui all'articolo 28, paragrafo 6, di tale direttiva, a chiedere all'autorità di controllo di tale altro Stato membro di accertare un'eventuale violazione di tale diritto e di imporre sanzioni se questo lo consente, appoggiandosi, se del caso, sulle informazioni che essa le avrà comunicato (punti 57, 60, disp. 2).

3. Poteri delle autorità nazionali di controllo

Sentenza del 6 ottobre 2015 (Grande Sezione), Schrems (C-362/14, EU:C:2015:650)

In tale causa (v. altresì la rubrica III, intitolata «Trasferimento di dati personali verso paesi terzi»), la Corte di giustizia ha dichiarato, in particolare, che le autorità nazionali di controllo sono competenti a controllare i trasferimenti di dati personali verso paesi terzi.

In proposito, la Corte ha rilevato anzitutto che le autorità nazionali di controllo dispongono di un'ampia gamma di poteri e questi, elencati in maniera non esaustiva all'articolo 28, paragrafo 3, della direttiva 95/46/CE, costituiscono altrettanti mezzi necessari all'adempimento dei loro compiti. In tal senso, dette autorità godono, segnatamente, di poteri investigativi, come quello di raccogliere qualsiasi informazione necessaria all'esercizio della loro funzione di controllo, di poteri effettivi d'intervento, come quello di vietare a titolo provvisorio o definitivo un trattamento di dati o, ancora, del potere di promuovere azioni giudiziarie (punto 43).

Riguardo al potere di controllo dei trasferimenti di dati personali verso i paesi terzi, la Corte ha dichiarato che è vero che si evince dall'articolo 28, paragrafi 1 e 6, della direttiva 95/46/CE che i poteri delle autorità nazionali di controllo riguardano i trattamenti di dati personali effettuati nel territorio del loro Stato membro, cosicché esse non dispongono di poteri, sulla base di tale articolo 28, con riguardo ai trattamenti di siffatti dati effettuati nel territorio di un paese terzo (punto 44).

Tuttavia, l'operazione consistente nel far trasferire dati personali da uno Stato membro verso un paese terzo costituisce, di per sé, un trattamento di dati personali effettuato nel territorio di uno Stato membro. Di conseguenza, poiché le autorità nazionali di controllo sono incaricate, ai sensi dell'articolo 8,

paragrafo 3, della Carta e dell'articolo 28 della direttiva 95/46/CE, di sorvegliare il rispetto delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, ciascuna di esse è investita della competenza a verificare se un trasferimento di tali dati dal proprio Stato membro verso un paese terzo rispetti i requisiti fissati dalla direttiva in parola (punti 45, 47).

VI. Applicazione territoriale della normativa europea

Sentenza del 13 maggio 2014 (Grande Sezione), Google Spain e Google (C-131/12, EU:C:2014:317)

In tale sentenza [v. altresì le rubriche II.3., intitolata «Nozione di "trattamento di dati personali"», e IV.1., intitolata «Diritto di opposizione al trattamento dei dati personali ("diritto all'oblio")»], la Corte di giustizia si è, altresì, pronunciata sull'ambito di applicazione territoriale della direttiva 95/46/CE.

Così, la Corte ha dichiarato che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai sensi della direttiva 95/46/CE, qualora il gestore di un motore di ricerca, pur avendo la propria sede in un paese terzo, apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro (punti 55, 60, disp. 2).

Infatti, in circostanze del genere, le attività del gestore del motore di ricerca e quelle del suo stabilimento situato in uno Stato membro, benché distinte, sono inscindibilmente connesse, dal momento che le attività relative agli spazi pubblicitari costituiscono il mezzo per rendere il motore di ricerca in questione economicamente redditizio e che tale motore è, al tempo stesso, lo strumento che consente lo svolgimento di dette attività (punto 56).

VII. Diritto di accesso del pubblico ai documenti delle istituzioni dell'Unione europea e tutela dei dati personali

Sentenza del 29 giugno 2010 (Grande Sezione), Commissione/Bavarian Lager (C-28/08 P, EU:C:2010:378)

La Bavarian Lager, una società creata con lo scopo d'importare birra tedesca destinata agli spacci di bevande del Regno Unito, non aveva potuto vendere il suo prodotto in quanto nel Regno Unito un gran numero di esercenti di spacci di bevande erano vincolati da contratti di acquisto esclusivo che li obbligavano a rifornirsi di birra presso determinati birrifici.

In virtù della normativa del Regno Unito relativa alla fornitura di birra (in prosieguo: la «GBP»), i birrifici britannici erano tenuti a concedere ai gestori di locali pubblici la possibilità di acquistare birra di un altro fabbricante purché fosse stata confezionata in barile. Orbene, la maggior parte delle birre prodotte al di fuori del Regno Unito non poteva essere considerata come «birra confezionata in barile» ai sensi della GBP e non rientrava quindi nel campo di applicazione di quest'ultima. Ritenendo che detta normativa costituisse una misura di effetto equivalente ad una restrizione quantitativa alle importazioni, la Bavarian Lager aveva presentato una denuncia alla Commissione.

Nel corso del procedimento per inadempimento avviato dalla Commissione nei confronti del Regno Unito, rappresentanti delle amministrazioni comunitaria e britannica, nonché rappresentanti della Confederazione delle industrie della birra del mercato comune (CBMC) avevano partecipato a una riunione tenutasi l'11 ottobre 1996. Dopo essere stata avvertita dalle autorità britanniche della modifica della normativa in esame volta a consentire la vendita di birra imbottigliata come birra di diversa provenienza allo stesso modo della birra confezionata in barile, la Commissione aveva informato la Bavarian Lager della sospensione del procedimento per inadempimento.

Poiché la Bavarian Lager aveva presentato una domanda volta ad ottenere il verbale completo della riunione tenutasi nell'ottobre del 1996, con l'indicazione del nome di tutti i partecipanti, la Commissione aveva, successivamente, respinto tale domanda, con decisione del 18 marzo 2004, adducendo in particolare la tutela della vita privata di tali persone, come garantita dal regolamento sulla tutela dei dati personali.

La Bavarian Lager ha quindi presentato un ricorso dinanzi al Tribunale chiedendo l'annullamento di tale decisione della Commissione. Con sentenza dell'8 novembre 2007, il Tribunale ha annullato la decisione della Commissione, ritenendo in particolare che la mera iscrizione del nome degli interessati nell'elenco delle persone che avevano partecipato a una riunione in nome dell'ente che rappresentavano non costituisse un pregiudizio e non mettesse in pericolo la vita privata di tali persone. La Commissione, sostenuta dal Regno Unito e dal Consiglio, ha allora investito la Corte di giustizia di un'impugnazione avverso tale sentenza del Tribunale.

La Corte ha anzitutto rilevato che, qualora una domanda fondata sul regolamento (CE) n. 1049/2001[31], relativo all'accesso ai documenti, sia diretta a ottenere l'accesso a documenti che contengono dati personali, le disposizioni del regolamento (CE) n. 45/2001 sono integralmente applicabili, inclusa la disposizione che impone al destinatario del trasferimento di dati personali l'obbligo di dimostrare la necessità della loro divulgazione nonché la disposizione che attribuisce all'interessato la facoltà di opporsi in qualsiasi momento, per motivi preminenti e legittimi connessi alla sua situazione particolare, al trattamento di dati che lo riguardano (punto 63).

Successivamente, la Corte ha rilevato che l'elenco dei partecipanti a una riunione tenutasi nel contesto di un procedimento per inadempimento che figurava nel verbale di detta riunione conteneva dati personali, ai sensi dell'articolo 2, lettera a), del regolamento (CE) n. 45/2001, poiché le persone che hanno partecipato a detta riunione potevano esservi identificate (punto 70).

Infine, essa ha concluso che esigendo che, per le persone che non hanno prestato il proprio consenso espresso alla diffusione dei dati personali che le riguardavano contenuti in tale verbale, fosse dimostrata la necessità del trasferimento di tali dati personali, la Commissione si era conformata alle disposizioni dell'articolo 8, lettera b), di detto regolamento (punto 77).

Infatti, allorché, nel quadro di una domanda di accesso a detto verbale ai sensi del regolamento (CE) n. 1049/2001, non è fornita alcuna motivazione espressa e legittima né alcun argomento convincente per dimostrare la necessità del trasferimento di tali dati personali, la Commissione non può soppesare i differenti interessi delle parti in causa. Essa non è neppure in grado di verificare se sussistano ragioni per presumere che tale trasferimento potrebbe arrecare pregiudizio agli interessi legittimi delle persone coinvolte, come richiesto dall'articolo 8, lettera b), del regolamento (CE) n. 45/2001 (punto 78)[32].

31 Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (GU L 145 del 31.5.2001, pag. 43).

32 Tale sentenza è stata presentata nella Relazione annuale 2010, pag. 14.

Sentenza del 16 luglio 2015, ClientEarth e PAN Europe/EFSA (C-615/13 P, EU:C:2015:489)

L'Autorità europea per la sicurezza alimentare (EFSA) aveva costituito un gruppo di lavoro al fine di elaborare l'orientamento per indicare le modalità di attuazione dell'articolo 8, paragrafo 5, del regolamento (CE) n. 1107/2009[33], ai sensi del quale, conformemente alle disposizioni dell'EFSA, il richiedente un'autorizzazione all'immissione sul mercato di un prodotto fitosanitario aggiunge al fascicolo la letteratura scientifica revisionata disponibile riguardante la sostanza attiva, i relativi metaboliti e i suoi effetti collaterali sulla salute, sull'ambiente e sulle specie non bersaglio.

Poiché il progetto di orientamento era stato sottoposto a consultazione pubblica, la ClientEarth e la Pesticide Action Network Europe (PAN Europe) avevano presentato osservazioni in proposito. In tale contesto, avevano presentato congiuntamente all'EFSA una domanda di accesso a vari documenti relativi alla preparazione del progetto di orientamento, incluse le osservazioni degli esperti esterni.

L'EFSA ha autorizzato la ClientEarth e la PAN Europe ad accedere, in particolare, alle osservazioni individuali degli esperti esterni sul progetto di orientamento. Tuttavia, essa ha affermato di aver occultato i nomi di tali esperti, in conformità dell'articolo 4, paragrafo 1, lettera b), del regolamento (CE) n. 1049/2001 nonché della normativa dell'Unione in materia di tutela dei dati personali, segnatamente il regolamento (CE) n. 45/2001. L'EFSA ha addotto, a tal proposito, che la divulgazione dei nomi di tali esperti corrispondeva a un trasferimento di dati personali, ai sensi dell'articolo 8 del regolamento (CE) n. 45/2001, e che nella fattispecie non ricorrevano le condizioni di un trasferimento siffatto previste da tale articolo.

Pertanto, la ClientEarth e la PAN Europe hanno proposto dinanzi al Tribunale un ricorso di annullamento della decisione dell'EFSA. Poiché il Tribunale ha respinto tale ricorso, la ClientEarth e la PAN Europe hanno allora presentato un'impugnazione avverso la sentenza[34] del Tribunale dinanzi alla Corte di giustizia.

In primo luogo, la Corte ha rilevato che, atteso che l'informazione richiesta consentirebbe di associare a ogni singolo esperto una determinata osservazione, essa riguardava persone fisiche identificate e, pertanto, costituiva un insieme di dati personali, ai sensi dell'articolo 2, lettera a), del regolamento (CE) n. 45/2001. Dal momento che le nozioni di «dati personali», di cui all'articolo 2, lettera a), del regolamento (CE) n. 45/2001, e di «dati relativi alla vita privata» non vanno confuse, la Corte ha considerato, inoltre, che l'affermazione della ClientEarth e della PAN Europe secondo la quale l'informazione controversa non rientrava nella sfera della vita privata degli esperti interessati era inconferente (punti 29, 32).

La Corte ha esaminato, in secondo luogo, l'argomento della ClientEarth e della PAN Europe basato sull'esistenza di un clima di sfiducia nei confronti dell'EFSA, spesso accusata di parzialità per via del suo ricorso a esperti che avevano interessi personali dettati dai loro legami con gli ambienti industriali, nonché sulla necessità di garantire la trasparenza del processo decisionale di tale autorità. Tale argomento era corroborato da uno studio sui legami intrattenuti dalla maggioranza degli esperti membri di un gruppo di lavoro dell'EFSA con lobby industriali. In proposito, la Corte ha dichiarato che ottenere l'informazione controversa risultava necessario per consentire di verificare in concreto l'imparzialità di ciascun esperto nell'adempimento della sua missione scientifica al servizio dell'EFSA. La Corte ha conseguentemente annullato la sentenza del Tribunale, constatando che esso aveva errato nel ritenere che il succitato argomento della ClientEarth e della PAN Europe non fosse sufficiente a dimostrare la necessità del trasferimento dell'informazione controversa (punti 57-59).

33 Regolamento (CE) n. 1107/2009 del Parlamento europeo e del Consiglio, del 21 ottobre 2009, relativo all'immissione sul mercato dei prodotti fitosanitari e che abroga le direttive 79/117/CEE e 91/414/CEE del Consiglio (GU L 309 del 24.11.2009, pag. 1).

34 Sentenza del Tribunale del 13 settembre 2013, ClientEarth e PAN Europe/EFSA (T-214/11, EU:T:2013:483).

In terzo luogo, al fine di valutare la legittimità della decisione controversa dell'EFSA, la Corte ha verificato se sussistessero o meno ragioni per presumere che tale trasferimento avrebbe potuto pregiudicare gli interessi legittimi degli interessati. In proposito, essa ha constatato che l'affermazione dell'EFSA secondo la quale la divulgazione dell'informazione controversa avrebbe comportato un potenziale pregiudizio per la vita privata e per l'integrità di detti esperti rappresentava una considerazione generale non supportata da altri elementi del caso di specie. La Corte ha considerato, al contrario, che tale divulgazione avrebbe consentito, di per sé, di dissipare i sospetti di parzialità in questione o avrebbe offerto agli esperti eventualmente interessati l'opportunità di contestare, eventualmente mediante i mezzi di ricorso disponibili, la fondatezza di tali accuse di parzialità. Alla luce di tali elementi, la Corte ha altresì annullato la decisione dell'EFSA (punti 69, 73).

* * *

Le sentenze contenute nella presente scheda sono classificate nel Repertorio della giurisprudenza sotto le rubriche 1.04.03.07, 1.04.03.08, 1.04.03.11, 2.04, 2.05.00, 4.11.01 e 4.11.07.