CORTE DI GIUSTIZIA
DELL'UNIONE EUROPEA

DIREZIONE DELLA RICERCA
E DOCUMENTAZIONE

Scheda tematica

PROTEZIONE 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 a tal 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, costituiva a tal proposito il principale atto giuridico dell'Unione in materia. Essa stabiliva condizioni generali di liceità del

[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 1995, L 281, pag. 31), versione consolidata al 20 novembre, abrogata a decorrere dal 25 maggio 2018 (v. nota 5).

trattamento di tali dati nonché i diritti delle persone interessate e prevedeva, in particolare, l'istituzione negli Stati membri di autorità di controllo indipendenti.

La direttiva 2002/58/CE [2] è poi intervenuta a completare la direttiva 95/46, 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]. Occorre osservare che il legislatore dell'Unione prevede un riesame di tale direttiva. A tal riguardo, la Commissione ha presentato, il 10 gennaio 2017, una proposta volta a sostituire tale direttiva con un regolamento relativo alla vita privata e alle comunicazioni elettroniche [4].

Inoltre, nell'ambito dello spazio di libertà, sicurezza e giustizia (ex articoli 30 e 31 TUE), la decisione quadro 2008/977/GAI [5] ha disciplinato, fino al mese di maggio del 2018, la protezione dei dati personali nei settori della cooperazione giudiziaria e di polizia in materia penale.

Nel 2016 l'Unione europea ha riformato il contesto normativo globale in materia. A tal fine, essa ha adottato il regolamento (UE) 2016/679 [6] relativo alla protezione dei dati (in prosieguo: il «RGPD»), che abroga la direttiva 95/46 ed è applicabile a decorrere dal 25 maggio 2018, nonché la direttiva (UE) 2016/680 [7] 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 protezione dei dati personali era, in un primo tempo, garantita dal regolamento (CE) n. 45/2001 [8]. Tale regolamento ha consentito in particolare l'istituzione, nel 2004, del Garante europeo della protezione dei dati. Nel 2018 l'Unione europea si è dotata di un nuovo quadro giuridico in materia, in particolare mediante l'adozione del regolamento (UE) 2018/1725 [9], che

---

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 relativa alla vita privata e alle comunicazioni elettroniche) (GU 2002, L 201, pag. 37), versione consolidata al 19 dicembre 2009.

3 La direttiva 2002/58 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 2006, L 105, 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), con la motivazione che essa costituiva una grave violazione dei 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 protezione dei dati personali» della presente scheda).

4 Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM/2017/010 final - 2017/03 (COD).

5 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 2008, L 350, pag. 60), abrogata a decorrere dal 6 maggio 2018 (v. nota 6).

6 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 2016, L 119, pag. 1).

7 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 2016, L 119, pag. 89).

8 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 2001, L 8, pag. 1).

9 Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

abroga il regolamento n. 45/2001 e la decisione n. 1247/2002/CE [10] ed è applicabile dall'11 dicembre 2018. Nell'interesse di un approccio coerente nella protezione dei dati personali in tutta l'Unione, tale nuovo regolamento mira ad allineare, per quanto possibile, le norme in materia al regime istituito dal RGPD.

[10] Decisione n. 1247/2002/CE del Parlamento europeo, del Consiglio e della Commissione, del 1° luglio 2002, relativa allo statuto e alle condizioni generali d'esercizio delle funzioni di garante europeo della protezione dei dati (GU 2002, L 183, pag. 1).

INDICE

I. DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI RICONOSCIUTO DALLA CARTA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA 5

1. Conformità del diritto derivato dell'Unione al diritto alla protezione dei dati personali 5

2. Rispetto del diritto alla protezione dei dati personali nell'attuazione del diritto dell'Unione 9

II. TRATTAMENTO DEI DATI PERSONALI AI SENSI DELLA NORMATIVA GENERALE IN MATERIA 10

1. Trattamenti di dati personali esclusi dall'ambito di applicazione della direttiva 95/46 10

2. Nozione di «dati personali» 13

3. Nozione di «trattamento di dati personali» 15

4. Nozione di «archivio di dati personali» 20

5. Nozione di «responsabile del trattamento di dati personali» 20

6. Condizioni di liceità di un trattamento di dati personali 23

III. TRATTAMENTO DEI DATI PERSONALI AI SENSI DELLA DIRETTIVA 2002/58 32

IV. TRASFERIMENTO DEI DATI PERSONALI VERSO PAESI TERZI 38

V. LA PROTEZIONE DEI DATI PERSONALI SU INTERNET 45

1. Diritto di opposizione al trattamento dei dati personali («diritto all'oblio») 46

2. Trattamento dei dati personali e diritti di proprietà intellettuale 47

3. Deindicizzazione di dati personali 51

4. Consenso dell'utente di un sito Internet all'archiviazione di informazioni 55

VI. AUTORITÀ NAZIONALI DI CONTROLLO 56

1. Portata del requisito dell'indipendenza 56

2. Determinazione del diritto applicabile e dell'autorità di controllo competente 59

3. Poteri delle autorità nazionali di controllo 60

VII. APPLICAZIONE TERRITORIALE DELLA LEGISLAZIONE EUROPEA 64

VIII. DIRITTO DI ACCESSO DEL PUBBLICO AI DOCUMENTI DELLE ISTITUZIONI DELL'UNIONE EUROPEA E PROTEZIONE DEI DATI PERSONALI 65

I. Diritto alla protezione dei dati personali riconosciuto dalla Carta dei diritti fondamentali dell'Unione europea

1. Conformità del diritto derivato dell'Unione al diritto alla protezione 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) [11]

In tale causa i procedimenti principali avevano ad oggetto controversie tra alcuni agricoltori e il 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 [12] e 259/2008 [13], che disciplinano il finanziamento della politica agricola comune e impongono la 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 varie questioni vertenti sulla validità di talune disposizioni del regolamento n. 1290/2005 e sulla validità del regolamento 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 da 56 a 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). In tale contesto, la Corte ha considerato che, sebbene in una

---

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

12 Regolamento (CE) n. 1290/2005 del Consiglio, del 21 giugno 2005, relativo al finanziamento della politica agricola comune (GU 2005, L 209, 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 2013, L 347, pag. 549).

13 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 di finanziamenti provenienti dal FEAGA e dal FEASR (GU 2008, L 76, 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 2014, L 255, pag. 59).

società democratica i contribuenti abbiano diritto ad essere informati sull'impiego delle finanze pubbliche, nondimeno il Consiglio e la Commissione erano tenuti ad effettuare un contemperamento equilibrato dei differenti interessi in causa, il che avrebbe richiesto che, prima dell'adozione delle disposizioni contestate, si verificasse se la 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 e 86).

Pertanto, la Corte ha dichiarato invalide talune disposizioni del regolamento n. 1290/2005, nonché il regolamento 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 e disp. 1). Tuttavia, la Corte non ha rimesso 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 e 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), pur rifiutando, in tale occasione, che 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 comune di rilasciargli il passaporto senza rilevare le sue impronte digitali. Dinanzi a tale giudice, il sig. Schwarz contestava la validità del regolamento (CE) n. 2252/2004 [14] 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 tale contesto, il Verwaltungsgericht Gelsenkirchen ha adito la Corte 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 in senso affermativo, dichiarando che, sebbene il prelievo e la conservazione di impronte digitali da parte delle autorità nazionali, disciplinati dall'articolo 1, paragrafo 2, del regolamento n. 2252/2004, costituiscano una violazione dei diritti al rispetto della vita privata e alla tutela dei dati personali, tale violazione è giustificata dallo scopo di preservare i passaporti da qualsiasi uso fraudolento.

Anzitutto, 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 da 35 a 38). Inoltre, il prelievo e la conservazione delle

[14] 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 2004, L 385, pag. 1), come modificato dal regolamento (CE) n. 444/2009 del Parlamento europeo e del Consiglio, del 6 maggio 2009 (GU 2009, L 142, pag. 1).

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 da 42 a 45).

Infine, riguardo alla necessità di tale trattamento, 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 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 da 54 a 57, 60 e 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) [15]

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 nel diritto austriaco.

Con le loro domande di pronuncia pregiudiziale, i giudici irlandese e austriaco hanno interpellato la Corte sulla validità della direttiva 2006/24 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,

[15] Detta sentenza è stata presentata nella Relazione annuale 2014, pag. 60.

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. Tali 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, 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, in quanto non permetteva di venire a conoscenza del contenuto delle comunicazioni elettroniche in quanto tale e prevedeva che i fornitori di servizi o di reti siano 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 da 38 a 44).

Tuttavia, la Corte ha considerato che, adottando la direttiva riguardante la conservazione dei dati, il legislatore dell'Unione aveva 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 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 da 57 a 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 da 60 a 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 e 64).

Peraltro, per quanto concerne i requisiti derivanti dall'articolo 8, paragrafo 3, della Carta, la Corte ha constatato che la direttiva 2006/24 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 nel 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 da 66 a 68).

2. Rispetto del diritto alla protezione dei dati personali 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) [16]

In seguito alla sentenza Digital Rights Ireland e Seitlinger e a. che ha dichiarato invalida la direttiva 2006/24 (v. supra), sono state sottoposte alla Corte due cause vertenti sull'obbligo generale 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 annullata.

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 utenti iscritti, per quanto riguarda 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, sebbene la conservazione del contenuto di tali comunicazioni fosse 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, 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, 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, per quanto riguarda tutti i mezzi di comunicazione elettronica. Secondo la Corte, siffatta normativa travalica i limiti dello stretto necessario e non può essere considerata giustificata, in una società

[16] Detta sentenza è stata presentata nella Relazione annuale 2016, pag. 62.

democratica, così come richiede detto articolo 15, paragrafo 1, letto alla luce dei summenzionati articoli della Carta (punti da 99 a 105, 107, 112 e 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 da 118 a 122, 125 e disp. 2).

La Corte ha considerato, per contro, che l'articolo 15, paragrafo 1, della direttiva 2002/58 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, tali da 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 siano 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 da 108 a 111).

II. Trattamento dei dati personali ai sensi della normativa generale in materia

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

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 protezione dei dati, la Commissione aveva avviato negoziati con le autorità statunitensi. Al termine di tali negoziati, il 14 maggio 2004 la Commissione aveva adottato la decisione 2004/535/CE [17], 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») garantisce 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 [18] che approva la conclusione di un accordo tra la Comunità europea e gli Stati Uniti sul trattamento e 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 annullare le due decisioni menzionate sostenendo, in particolare, che la decisione sull'adeguatezza era stata adottata ultra vires, che l'articolo 95 CE (divenuto articolo 114 TFUE) non costituiva una base giuridica corretta per la decisione che approva la conclusione dell'accordo e, in entrambi i casi, che sussisteva una violazione dei diritti fondamentali.

Per quanto riguarda la decisione sull'adeguatezza, la Corte ha verificato, anzitutto, se la Commissione potesse validamente adottare la propria decisione sulla base della direttiva 95/46. 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, sebbene 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 possedeva, tuttavia, 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 e 57).

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, tale 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

[17] 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 2004, L 235, pag. 11).

[18] 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 2004, L 183, pag. 83, e rettifica in GU 2005, L 255, pag. 168).

riguardava un trattamento di dati personali che ne è escluso. La Corte, di conseguenza, ha annullato la decisione sull'adeguatezza (punti 58 e 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, 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 da 67 a 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'impugnazione proposta dal sig. Ryneš avverso una decisione del Městský soud v Praze (Tribunale municipale di Praga, Repubblica ceca) che aveva confermato la decisione dell'Ufficio, il Nejvyšší správní soud (Corte suprema amministrativa) ha chiesto alla Corte se la registrazione effettuata dal sig. Ryneš al fine di tutelare la sua vita, la sua salute e i suoi beni costituisse un trattamento di dati non rientrante nell'ambito di applicazione della direttiva 95/46, 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, della medesima 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, in quanto disciplinano il trattamento di dati personali suscettibile di ledere le libertà fondamentali e, in particolare, il diritto alla vita privata, devono essere necessariamente 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 da 27 a 29). Inoltre, il dettato stesso di tale disposizione sottrae all'applicazione della direttiva 95/46 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 e 33).

2. Nozione di «dati personali»

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

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. Per contro, il fornitore di accesso a Internet disponeva, quanto a lui, di informazioni aggiuntive che, se combinate con tale 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, 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 (punti 43 e 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, 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 e disp. 1).

[19] Detta sentenza è stata presentata nella Relazione annuale 2016, pag. 61.

Sentenza del 20 dicembre 2017, Nowak (C-434/16, EU:C:2017:994)

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.

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 la questione se l'articolo 2, lettera a), della direttiva 95/46 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, 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 (punti 31 e da 36 a 40).

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 (punti 42 e 43).

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 quindi 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, 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, non si estendono alle domande poste in sede di esame, le quali non costituiscono in quanto tali dati personali del candidato (punti 56 e 58).

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 (punto 62 e disp.).

3. Nozione di «trattamento di dati personali»

Sentenza del 6 novembre 2003 (Grande Sezione), 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.

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 e 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, in quanto 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, da 43 a 48 e 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 che fosse ordinato 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 ha quindi avuto l'occasione di precisare la nozione di «trattamento di dati personali» in Internet con riferimento alla direttiva 95/46.

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 e 30).

Sentenza del 10 luglio 2018 (Grande Sezione), Jehovan todistajat (C-25/17, EU:C:2018:551) [20]

L'autorità finlandese per la protezione dei dati aveva adottato una decisione che vietava alla

[20] Detta sentenza è stata presentata nella Relazione annuale 2018, pagg. 87 e 88.

comunità dei testimoni di Geova di raccogliere o di trattare dati personali nell'ambito dell'attività di predicazione porta a porta effettuata dai suoi membri senza che fossero rispettati i requisiti previsti dalla normativa finlandese relativa al trattamento di tali dati. I membri di tale comunità, infatti, nell'ambito della loro attività di predicazione porta a porta, prendono appunti sulle visite effettuate a persone che essi stessi o detta comunità non conoscono. Tali dati sono raccolti a titolo di promemoria, per poter essere consultati per un'eventuale visita successiva, senza che le persone interessate vi abbiano acconsentito o ne siano state informate. A tal riguardo, la comunità dei testimoni di Geova ha fornito ai suoi membri istruzioni in ordine alla redazione di tali appunti, che figurano in almeno una delle sue pubblicazioni riguardanti l'attività di predicazione.

La Corte ha dichiarato che la raccolta di dati personali effettuata da membri di una comunità religiosa nell'ambito di un'attività di predicazione porta a porta e i successivi trattamenti di tali dati non rientrano nelle eccezioni all'ambito di applicazione della direttiva 95/46, dato che non costituiscono né trattamenti di dati personali effettuati per l'esercizio di attività di cui all'articolo 3, paragrafo 2, primo trattino, di tale direttiva, né trattamenti di dati personali effettuati da persone fisiche per l'esercizio di un'attività a carattere esclusivamente personale o domestico, ai sensi dell'articolo 3, paragrafo 2, secondo trattino, di detta direttiva (punto 51 e disp. 1).

Sentenza del 14 febbraio 2019, Buivids (C-345/17, EU:C:2019:122)

In tale causa la Corte ha preso in esame l'interpretazione, da un lato, dell'ambito di applicazione della direttiva 95/46 e, dall'altro, della nozione di «trattamento di dati personali effettuato esclusivamente a scopi giornalistici», di cui all'articolo 9 di tale direttiva.

Tale sentenza si inserisce nell'ambito di una domanda di pronuncia pregiudiziale presentata dalla Corte suprema di Lettonia, investita di una controversia tra il sig. Buivids (in prosieguo: il «ricorrente») e l'autorità nazionale per la protezione dei dati, vertente su un ricorso teso ad ottenere la dichiarazione di illegittimità di una decisione della predetta autorità, secondo la quale tale persona, avendo pubblicato, su un sito Internet, un video, da lui stesso registrato, della raccolta della sua deposizione, da parte degli agenti di polizia, all'interno dei locali del commissariato della polizia nazionale nell'ambito di un procedimento per illecito amministrativo, avrebbe violato la legislazione nazionale in materia di protezione dei dati personali. Pertanto, in seguito al rigetto del suo ricorso da parte di due giudici di grado inferiore, il ricorrente ha investito la Corte suprema di un ricorso per cassazione. Dinanzi a tale giudice, egli ha invocato il suo diritto alla libertà di espressione, sostenendo che il video in questione mostrava funzionari della polizia nazionale, che hanno la qualità di persone pubbliche, in un luogo accessibile al pubblico e che, pertanto, tali persone non beneficerebbero dell'applicazione delle disposizioni della legge sulla protezione dei dati.

Per quanto riguarda, in primo luogo, l'ambito di applicazione della direttiva 95/46, la Corte ha osservato che, da un lato, le immagini degli agenti di polizia registrati nel video in questione costituiscono dati personali e che, dall'altro, la registrazione video di tali persone archiviata nella memoria della telecamera utilizzata dal ricorrente costituisce un trattamento di dati personali. Pertanto, la Corte ha aggiunto che il fatto di pubblicare una registrazione video sulla quale compaiano dati personali su un sito Internet di video che possono essere visionati e condivisi dagli utenti costituisce un trattamento interamente o parzialmente automatizzato di tali dati.

Peraltro, la Corte ha sottolineato che detta registrazione e la sua pubblicazione non rientrano tra le eccezioni previste all'ambito di applicazione della direttiva 95/46, concernenti in particolare i trattamenti dei dati personali realizzati nell'esercizio di attività che non rientrano nell'ambito di applicazione di tale direttiva e i trattamenti che rientrano nell'esercizio delle attività a carattere esclusivamente personale o domestico. Pertanto, la Corte ha concluso che rientrano nell'ambito di applicazione di tale direttiva la registrazione video di taluni agenti di polizia all'interno di un commissariato, durante la raccolta di una deposizione, e la pubblicazione del video così registrato su un sito Internet di video sul quale gli utenti possono inviare, visionare e condividere questi ultimi (punti 31, 32, 35, 39, 42, 43 e disp. 1).

Per quanto riguarda, in secondo luogo, la portata della nozione di «trattamento di dati personali effettuato esclusivamente a scopi giornalistici», la Corte ha anzitutto ricordato che, secondo un'interpretazione estensiva della nozione di «giornalismo», le esenzioni e le deroghe previste all'articolo 9 della direttiva 95/46 si applicano a chiunque eserciti attività giornalistiche. Pertanto, la Corte ha dichiarato che il fatto che il ricorrente non sia un giornalista professionista non esclude che la registrazione del video di cui trattasi e la sua trasmissione possano essere qualificate come «trattamento di dati personali effettuato esclusivamente a scopi giornalistici». Inoltre, la Corte ha sottolineato che le esenzioni e le deroghe cui all'articolo 9 della direttiva 95/46 devono essere applicate solo nella misura in cui siano necessarie per conciliare due diritti fondamentali, vale a dire il diritto alla protezione della vita privata e alla libertà di espressione. A tal riguardo, la Corte ha precisato che non si può escludere che la registrazione e la pubblicazione del video in questione, avvenute senza che gli agenti di polizia che appaiono in tale video venissero informate di tale registrazione e delle sue finalità, costituiscano un'ingerenza nel diritto fondamentale al rispetto della vita privata di tali persone. Pertanto, essa ha concluso che la registrazione e la pubblicazione su un sito Internet di video del video in questione possono costituire un trattamento di dati personali esclusivamente a scopi giornalistici, purché da tale video risulti che detta registrazione e detta pubblicazione hanno come unica finalità la divulgazione al pubblico di informazioni, opinioni o idee, circostanza che spetta al giudice del rinvio verificare (punti 51, 52, 55, 63, 67 e disp. 2).

Sentenza del 22 giugno 2021 (Grande Sezione), Latvijas Republikas Saeima (Punti di penalità) (C-439/19, EU:C:2021:504)

B è una persona fisica alla quale sono stati inflitti punti di penalità per una o più infrazioni stradali. La Ceļu satiksmes drošības direkcija (Direzione per la sicurezza stradale, Lettonia) (in prosieguo: la «CSDD») ha iscritto tali punti di penalità nel registro nazionale dei veicoli e dei conducenti.

In forza della normativa lettone sulla circolazione stradale [21], le informazioni riguardanti i punti di penalità inflitti ai conducenti di veicoli iscritti in tale registro sono accessibili al pubblico e sono comunicate dalla CSDD a chiunque ne faccia domanda, compresi operatori economici a fini di riutilizzo, senza che il richiedente debba dimostrare un interesse specifico ad ottenere tali informazioni. Nutrendo dubbi sulla legittimità di tale normativa, B ha proposto un ricorso

[21] Articolo 14 [1], paragrafo 2, del Ceļu satiksmes likums (legge sulla circolazione stradale), del 1° ottobre 1997 (Latvijas Vēstnesis, 1997, n. 274/276).

costituzionale dinanzi alla Latvijas Republikas Satversmes tiesa (Corte costituzionale, Lettonia), affinché esaminasse la conformità di tale normativa al diritto al rispetto della vita privata.

La Corte costituzionale ha considerato che, nell'ambito della sua valutazione di tale diritto costituzionale, essa deve tener conto del RGPD. Pertanto, essa ha chiesto alla Corte di giustizia di chiarire la portata di varie disposizioni del RGPD per accertare se la normativa lettone sulla circolazione stradale sia compatibile con tale regolamento.

Con la sua sentenza, pronunciata in Grande Sezione, la Corte dichiara che il trattamento dei dati personali riguardanti i punti di penalità costituisce un «trattamento dei dati personali relativi a condanne penali e a reati» [22], per il quale il RGPD prevede una protezione maggiore in virtù del carattere particolarmente sensibile dei dati in questione (punti 10, 46, 74, 94 e disp. 1).

In tale contesto, essa osserva, in via preliminare, che le informazioni relative ai punti di penalità costituiscono dati personali e che la loro comunicazione a terzi da parte della CSDD costituisce un trattamento rientrante nell'ambito di applicazione materiale del RGPD. Tale ambito di applicazione, infatti, è alquanto ampio e detto trattamento non si annovera tra le eccezioni all'applicabilità di tale regolamento (punti 60, 61 e 72).

Infatti, da un lato, detto trattamento non è coperto dall'eccezione relativa all'inapplicabilità del RGPD a un trattamento effettuato per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione [23]. Occorre considerare che tale eccezione ha come unico obiettivo di escludere dall'ambito di applicazione di detto regolamento i trattamenti di dati personali effettuati dalle autorità statali nell'ambito di un'attività volta a salvaguardare la sicurezza nazionale o di un'attività che possa essere ascritta alla medesima categoria. Tali attività comprendono, in particolare, quelle volte a tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società. Orbene, le attività riguardanti la sicurezza stradale non perseguono un tale obiettivo e non possono essere quindi ascritte alla categoria delle attività che hanno lo scopo di salvaguardare la sicurezza nazionale (punti 62 e da 66 a 68).

Dall'altro lato, la comunicazione dei dati personali relativi ai punti di penalità non costituisce neppure un trattamento contemplato dall'eccezione che comporta l'inapplicabilità del RGPD ai trattamenti di dati personali effettuati dalle autorità competenti in materia penale [24]. La Corte dichiara infatti che la CSDD, quando effettua detta comunicazione, non può essere considerata una siffatta «autorità competente» [25] (punti da 69 a 71).

Per accertare se l'accesso ai dati personali relativi alle infrazioni stradali, come i punti di penalità, costituisca un trattamento di dati personali relativi a «reati» [26], che godono di una maggiore protezione, la Corte constata, basandosi segnatamente sulla genesi del RGPD, che tale nozione rinvia esclusivamente agli illeciti penali. Tuttavia, la circostanza che nel sistema giuridico lettone

---

22 Articolo 10 del RGPD.

23 Articolo 2, paragrafo 2, lettera a), del RGPD.

24 Articolo 2, paragrafo 2, lettera d), del RGPD.

25 Articolo 3, paragrafo 7, della 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 2016, L 119, pag. 89).

26 Articolo 10 del RGPD.

le infrazioni stradali siano qualificate come illeciti amministrativi non è determinante per valutare se tali infrazioni rientrino nella nozione di «reato», in quanto si tratta di una nozione autonoma del diritto dell'Unione che richiede, in tutta l'Unione, un'interpretazione autonoma e uniforme. Pertanto, dopo aver ricordato i tre criteri rilevanti per valutare la natura penale di un illecito, ossia la qualificazione giuridica dell'illecito nel diritto nazionale, la natura dell'illecito e il grado di severità della sanzione inflitta, la Corte statuisce che le infrazioni stradali in questione rientrano della nozione di «reato» ai sensi del RGPD. Per quanto attiene ai primi due criteri, la Corte constata che, anche se gli illeciti non sono qualificati come «penali» dal diritto nazionale, una simile qualificazione può derivare della natura dell'illecito, e segnatamente dalla finalità repressiva perseguita dalla sanzione che l'illecito può comportare. Orbene, nel caso di specie, l'attribuzione di punti di penalità per infrazioni stradali, al pari delle altre sanzioni che la commissione di queste ultime può comportare, perseguono, tra l'altro una siffatta finalità repressiva. Quanto al terzo criterio, la Corte osserva che solo le infrazioni stradali di una certa gravità comportano l'irrogazione di punti di penalità e che, di conseguenza, esse possono comportare sanzioni di una certa gravità. Peraltro, l'irrogazione di tali punti si aggiunge generalmente alla sanzione inflitta e il cumulo di detti punti comporta conseguenze giuridiche che possono spingersi addirittura fino al divieto di guidare (punti 77, 80, 85, da 87 a 90 e 93).

4. Nozione di «archivio di dati personali»

Sentenza del 10 luglio 2018 (Grande Sezione), Jehovan todistajat (C-25/17, EU:C:2018:551)

In tale sentenza (v. altresì la rubrica II.3., intitolata «Nozione di "trattamento di dati personali"»), la Corte ha precisato la nozione di «archivio» di cui all'articolo 2, lettera c), della direttiva 95/46.

Pertanto, dopo aver ricordato che la direttiva si applica ai trattamenti manuali di dati personali solo se i dati trattati sono contenuti o destinati a figurare in un archivio, la Corte ha rilevato che la nozione di «archivio» include l'insieme di dati personali raccolti nell'ambito di un'attività di predicazione porta a porta, contenente nomi, indirizzi e altre informazioni riguardanti le persone contattate, allorché tali dati sono strutturati secondo criteri specifici che consentono, in pratica, di recuperarli facilmente per un successivo impiego. Affinché il suddetto insieme rientri in tale nozione, non è necessario che esso comprenda schedari, elenchi specifici o altri sistemi di ricerca (punto 62 e disp. 2).

5. Nozione di «responsabile del trattamento di dati personali»

Sentenza del 10 luglio 2018 (Grande Sezione), Jehovan todistajat (C-25/17, EU:C:2018:551)

In tale causa (v. altresì le rubriche II.3. e II.4., intitolate «Nozione di "trattamento di dati personali"» e «Nozione di "archivio di dati personali"»), la Corte si è pronunciata sulla responsabilità di una comunità religiosa per quanto riguarda i trattamenti di dati personali effettuati nell'ambito di un'attività di predicazione porta a porta organizzata, coordinata e incoraggiata da tale comunità.

Infine, la Corte ha considerato che l'obbligo di ogni persona di conformarsi alle norme del diritto dell'Unione relative alla protezione dei dati personali non può essere ritenuto un'ingerenza nell'autonomia organizzativa delle comunità religiose. A tal riguardo, essa ha concluso che

l'articolo 2, lettera d), della direttiva 95/46, letto alla luce dell'articolo 10, paragrafo 1, della Carta, dev'essere interpretato nel senso che esso consente di considerare una comunità religiosa, congiuntamente ai suoi membri predicatori, quale responsabile dei trattamenti di dati personali effettuati da questi ultimi nell'ambito di un'attività di predicazione porta a porta organizzata, coordinata e incoraggiata da tale comunità, senza che sia necessario che detta comunità abbia accesso a tali dati o che si debba dimostrare che essa ha fornito ai propri membri istruzioni scritte o incarichi relativamente a tali trattamenti (punti 74, 75 e disp. 3).

Sentenza del 5 giugno 2018 (Grande Sezione), Wirtschaftsakademie Schleswig Holstein (C-210/16, ECLI:EU:C:2018:388) [27]

L'autorità tedesca per la protezione dei dati, nella sua qualità di autorità di controllo, ai sensi dell'articolo 28 della direttiva 95/46, aveva ordinato ad una società tedesca, specializzata nel settore della formazione e che offre servizi di formazione attraverso una fanpage presente sul sito del social network Facebook, di disattivare la sua fanpage. Infatti, secondo detta autorità, né tale società né Facebook avevano informato i visitatori della fanpage del fatto che quest'ultima raccoglieva, mediante cookie, informazioni a carattere personale che li riguardavano e che detta società e Facebook elaboravano successivamente tali dati.

In tale contesto, la Corte ha precisato la nozione di «responsabile del trattamento» di dati personali. A tal riguardo, essa ha considerato che l'amministratore di una fanpage presente su Facebook, quale la società di cui al procedimento principale, partecipa, attraverso la propria azione d'impostazione dei parametri (in funzione, segnatamente, del suo pubblico destinatario nonché di obiettivi di gestione o promozione delle sue attività), alla determinazione delle finalità e degli strumenti del trattamento dei dati personali dei visitatori della sua fanpage. Pertanto, secondo la Corte, tale amministratore deve essere qualificato come responsabile di tale trattamento all'interno dell'Unione, assieme alla Facebook Ireland (la controllata, all'interno dell'Unione, della società statunitense Facebook), ai sensi dell'articolo 2, lettera d), della direttiva 95/46 (punto 39).

Sentenza del 29 luglio 2019, Fashion ID (C-40/17, EU:C:2019:629)

In tale causa, la Corte ha avuto occasione di sviluppare la nozione di «responsabile del trattamento» con riferimento all'inserimento di un «plug-in» in una pagina Internet.

Nel caso di specie, la Fashion ID, impresa tedesca di abbigliamento di moda online, aveva inserito nel proprio sito Internet il plug-in social «Mi piace» del social network Facebook. Tale inserimento sembra avere come conseguenza che, quando un visitatore consulta il sito Internet della Fashion ID, alcuni dati personali di tale visitatore sono trasmessi alla Facebook Ireland. Risulta che tale trasmissione avviene senza che il suddetto visitatore ne sia consapevole e indipendentemente dal fatto che egli sia iscritto al social network Facebook o che abbia cliccato sul pulsante «Mi piace» di Facebook.

La Verbraucherzentrale NRW, associazione tedesca di pubblica utilità per la tutela degli interessi dei consumatori, contesta alla Fashion ID di aver trasmesso alla Facebook Ireland dati personali

[27] Detta sentenza è stata presentata nella Relazione annuale 2018, pagg. 86 e 87.

appartenenti ai visitatori del suo sito Internet, da un lato, senza il consenso di questi ultimi e, dall'altro, in violazione degli obblighi di informazione previsti dalle disposizioni relative alla protezione dei dati personali. Investito della controversia, l'Oberlandesgericht Düsseldorf (Tribunale superiore del Land di Düsseldorf, Germania) ha chiesto alla Corte di interpretare diverse disposizioni della direttiva 95/46.

La Corte ha constatato, anzitutto, che il gestore di un sito Internet, quale la Fashion ID, può essere considerato responsabile del trattamento, ai sensi dell'articolo 2, lettera d), della direttiva 95/46. Tale responsabilità è tuttavia limitata all'operazione o all'insieme delle operazioni di trattamento dei dati personali di cui determina effettivamente le finalità e gli strumenti, vale a dire la raccolta e la comunicazione mediante trasmissione dei dati di cui trattasi. Per contro, secondo la Corte, risulta escluso, a prima vista, che la Fashion ID determini le finalità e gli strumenti delle successive operazioni di trattamento di dati personali, effettuate dalla Facebook Ireland dopo la loro trasmissione a quest'ultima, cosicché la Fashion ID non può essere considerata responsabile di tali operazioni, ai sensi del summenzionato articolo 2, lettera d) (punti 76, 85 e disp. 2).

Inoltre, la Corte ha sottolineato che è necessario che il gestore di un sito Internet e il fornitore di un plug-in social, come Facebook Ireland, perseguano ciascuno, con le operazioni di trattamento succitate, un interesse legittimo, ai sensi dell'articolo 7, lettera f), della direttiva 95/46, al fine di poter addurre una giustificazione per dette operazioni (punto 97 e disp. 3).

Infine, la Corte ha precisato che il consenso della persona interessata, di cui all'articolo 2, lettera h), e all'articolo 7, lettera a), della direttiva 95/46, deve essere ottenuto dal gestore di un sito Internet unicamente per quanto riguarda le operazioni di trattamento dei dati personali di cui tale gestore determina le finalità e gli strumenti. In tale situazione, l'obbligo di informazione previsto dall'articolo 10 di tale direttiva incombe anche a detto gestore; l'informazione che quest'ultimo deve fornire alla persona interessata deve tuttavia riguardare soltanto l'operazione o l'insieme delle operazioni di trattamento dei dati personali di cui esso determina le finalità e gli strumenti (punto 106 e disp. 4).

Sentenza del 9 luglio 2020, Land Hessen, C-272/19, EU:C:2020:535

Un cittadino, dopo aver presentato una petizione alla commissione per le petizioni del Parlamento del Land Assia (Germania), ha chiesto a tale commissione l'accesso ai dati personali che lo riguardavano, conservati da quest'ultima nell'ambito del trattamento della sua petizione. Esso si basa, per tale domanda, sul RGPD che prevede il diritto di una persona interessata di ottenere, dal responsabile del trattamento, l'accesso ai dati personali che la riguardano.

Il presidente del Parlamento del Land Assia ha respinto tale domanda, adducendo la motivazione che la procedura di petizione costituisce un compito parlamentare e che il parlamento non ricade nell'ambito di applicazione del RGDP.

Il Verwaltungsgericht Wiesbaden (Tribunale amministrativo di Wiesbaden, Germania), adito dal cittadino, considera che il diritto tedesco non riconosce alcun diritto di accesso ai dati personali nel contesto di una petizione come quella di cui trattasi. Ritenendo, tuttavia, che siffatto diritto di accesso possa derivare dal RGPD, il Verwaltungsgericht Wiesbaden (Tribunale amministrativo di Wiesbaden) ha interpellato la Corte di giustizia su tale punto. Inoltre, nutrendo dubbi riguardo

alla propria indipendenza e quindi alla sua qualità di giudice, autorizzato a sottoporre questioni pregiudiziali alla Corte, il Verwaltungsgericht Wiesbaden (Tribunale amministrativo di Wiesbaden) ha interpellato la Corte anche su tale aspetto.

Con la sua sentenza, la Corte risponde che, nei limiti in cui una commissione per le petizioni del parlamento di uno Stato federato di uno Stato membro determina, singolarmente o insieme ad altri, le finalità e i mezzi del trattamento dei dati personali, tale commissione deve essere qualificata come «titolare del trattamento» ai sensi del RGPD [28]. Il trattamento di dati personali effettuato da siffatta commissione è quindi soggetto a tale regolamento, in particolare alla disposizione che conferisce alle persone interessate un diritto di accesso ai dati personali che li riguardano [29].

La Corte constata, in particolare, che le attività della commissione per le petizioni del Parlamento del Land Assia non rientrano in un'eccezione prevista dal RGPD. Essa ammette che tali attività sono di natura pubblica e proprie di tale Land, giacché detta commissione contribuisce indirettamente all'attività parlamentare, ma rileva che tali attività sono parimenti di natura tanto politica quanto amministrativa. Inoltre, dagli elementi di cui dispone la Corte non risulta in alcun modo che tali attività corrispondano, nel caso di specie, a una delle eccezioni previste dal RGPD (punti da 71 a 74 e disp.).

6. Condizioni di liceità di un trattamento di dati personali

Sentenza del 16 dicembre 2008 (Grande Sezione), Huber (C-524/06, EU:C:2008:724) [30]

L'Ufficio federale per l'immigrazione e i rifugiati (Bundesamt für Migration und Flüchtlinge, Germania), provvedeva alla gestione di un registro centrale 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 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

[28] Articolo 4, punto 7, del RGPD.
[29] Articolo 15 del RGPD.
[30] Detta sentenza è stata presentata nella Relazione annuale 2008, pag. 45.

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 e, considerata la sua natura, compatibile con il divieto di discriminazioni fondate sulla nazionalità contenuto nell'articolo 12, primo comma, CE (divenuto articolo 18, primo comma, TFUE). Tuttavia, siffatto registro non può contenere informazioni diverse da quelle a tal fine necessarie ai sensi della direttiva sulla protezione dei dati personali (punti 54, 58 e 59).

Riguardo alla nozione di «necessità» del trattamento ai sensi dell'articolo 7, lettera e), della direttiva 95/46, 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 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 tale registro non possono essere considerati necessari ai sensi dell'articolo 7, lettera e), della direttiva 95/46 (punti 52, 66 e 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, primo comma, CE (punti da 78 a 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 (Corte suprema, 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.

In particolare, l'ASNEF e la FECEMD osservavano che il diritto spagnolo, per permettere il trattamento dei dati personali, in assenza del consenso della persona interessata, aggiungeva una condizione che non esiste nella direttiva 95/46, 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 restringevano la portata dell'articolo 7, lettera f), della direttiva 95/46, 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 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 e 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 anche 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. Di conseguenza, la Corte ha concluso che l'articolo 7, lettera f), della direttiva 95/46 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 e 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 si è anche pronunciata sulla questione se l'articolo 7, lettera f), della direttiva 95/46 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 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 ridotto in maniera illegittima la portata di tale principio previsto all'articolo 7, lettera f), della direttiva 95/46, escludendo che l'obiettivo di garantire il funzionamento generale dei siti del medium online possa essere oggetto di ponderazione con l'interesse o i diritti e le libertà fondamentali degli utenti (punti da 62 a 64 e disp. 2).

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

Tale causa si inseriva 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 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 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 Slovenskej republiky (Corte suprema della Repubblica slovacca) ha investito la Corte di giustizia, in particolare, della questione se 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 potessero essere interpretati 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 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 è proceduto 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 (punto 117 e 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 e 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, taluni dei diritti previsti dagli 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).

Sentenza dell'11 novembre 2020, Orange Romania (C-61/19, EU:C:2020:901)

L'Orange România SA è un fornitore di servizi di telecomunicazione mobile nel mercato rumeno. Il 28 marzo 2018 l'Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (Autorità nazionale di sorveglianza del trattamento dei dati personali, Romania) le ha inflitto un'ammenda per aver raccolto e conservato le copie dei documenti d'identità dei suoi clienti senza il consenso espresso di questi ultimi.

Secondo l'ANSPDCP, nel periodo compreso tra il 1° e il 26 marzo 2018, l'Orange România ha concluso contratti per la fornitura di servizi di telecomunicazione mobile contenenti una clausola secondo la quale i clienti sono stati informati e hanno acconsentito alla raccolta e alla conservazione di una copia del loro documento di identità a fini di identificazione. La casella relativa a tale clausola è stata selezionata dal responsabile del trattamento prima della sottoscrizione di tale contratto.

È in tale contesto che il Tribunalul București (Tribunale superiore di Bucarest, Romania) ha chiesto alla Corte di precisare le condizioni alle quali il consenso dei clienti al trattamento di dati personali può essere considerato valido.

La Corte ricorda, anzitutto, che il diritto dell'Unione [31] prevede un elenco dei casi in cui il trattamento di dati personali può essere considerato lecito. In particolare, il consenso dell'interessato dev'essere libero, specifico, informato e inequivocabile [32]. A tal riguardo, il consenso non è validamente espresso in caso di silenzio, di preselezione di caselle o di inattività (punti 34, 36, 37 e 39).

Inoltre, qualora il consenso dell'interessato sia prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, tale dichiarazione deve essere presentata in forma comprensibile e facilmente accessibile, ed essere formulata in un linguaggio semplice e chiaro. Per garantire all'interessato un'effettiva libertà di scelta, le clausole contrattuali non devono indurlo in errore circa la possibilità di stipulare il contratto anche qualora egli rifiuti di acconsentire al trattamento dei suoi dati (punti 34, 36, 37, 39 e 41).

La Corte precisa che, poiché l'Orange România è il responsabile del trattamento dei dati personali, essa deve essere in grado di dimostrare la liceità del trattamento di tali dati e,

[31] Articolo 7, della direttiva 95/46 e articolo 6 del RGPD.
[32] Articolo 2, lettera h), della direttiva 95/46 e articolo 4, punto 11, del RGPD.

pertanto, nel caso di specie, l'esistenza di un valido consenso dei suoi clienti. A tal riguardo, dato che i clienti interessati non sembrano avere essi stessi selezionato la casella relativa alla raccolta e alla conservazione delle copie del loro documento di identità, il mero fatto che tale casella sia stata spuntata non è idoneo a dimostrare una manifestazione positiva del loro consenso. Spetta al giudice nazionale effettuare le necessarie verifiche a tal riguardo (punti 42 e 46).

Spetta parimenti al giudice nazionale, secondo la Corte, valutare se le clausole contrattuali di cui trattasi potessero indurre o meno i clienti interessati in errore circa la possibilità di concludere il contratto nonostante il rifiuto di acconsentire al trattamento dei loro dati, in assenza di precisazioni su tale possibilità. Inoltre, in caso di rifiuto da parte di un cliente di acconsentire al trattamento dei suoi dati, la Corte osserva che l'Orange România esigeva che quest'ultimo dichiarasse per iscritto di non acconsentire né alla raccolta né alla conservazione della copia del suo documento di identità. Secondo la Corte, un siffatto requisito supplementare è tale da incidere indebitamente sulla libera scelta di opporsi a tale raccolta e a tale conservazione. In ogni caso, poiché detta società è tenuta a dimostrare che i suoi clienti, con un comportamento attivo, hanno manifestato il loro consenso al trattamento dei loro dati personali, tale società non può pretendere che essi manifestino attivamente il loro rifiuto (punti da 49 a 51).

La Corte conclude quindi che un contratto relativo alla fornitura di servizi di telecomunicazione che contiene una clausola secondo cui l'interessato è stato informato e ha acconsentito alla raccolta e alla conservazione di una copia del suo documento di identità a fini di identificazione non è tale da dimostrare che tale persona abbia validamente manifestato il proprio consenso a tale raccolta e conservazione, qualora la casella relativa a tale clausola sia stata selezionata dal responsabile del trattamento dei dati prima della sottoscrizione di tale contratto, qualora le clausole contrattuali di tale contratto possano indurre in errore la persona interessata circa la possibilità di stipulare il contratto in questione anche se essa rifiuta di acconsentire al trattamento dei suoi dati, o qualora la libera scelta di opporsi a tale raccolta e a tale conservazione sia indebitamente pregiudicata da detto responsabile, in quanto esso esige che la persona interessata, per rifiutare il proprio consenso a tali trattamenti, compili un modulo supplementare che attesti tale rifiuto (punto 52 e disp.).

Sentenza del 12 maggio 2021 (Grande Sezione), Bundesrepublik Deutschland (Avviso rosso dell'Interpol) (C-505/19, EU:C:2021:376)

Nel 2012 l'Organizzazione internazionale della polizia criminale (in prosieguo: l'«Interpol») ha pubblicato, su richiesta degli Stati Uniti e sulla base di un mandato d'arresto emesso dalle autorità di tale paese, un avviso rosso riguardante WS, cittadino tedesco, ai fini della sua eventuale estradizione. Se una persona oggetto di un simile avviso viene localizzata in uno Stato membro dell'Interpol, tale Stato deve, in linea di principio, procedere al suo arresto provvisorio oppure controllarne o limitarne gli spostamenti.

Tuttavia, ancor prima della pubblicazione di tale avviso rosso, un procedimento di indagine avente ad oggetto, secondo il giudice del rinvio, gli stessi fatti all'origine di tale avviso era stato avviato a carico di WS in Germania. Tale procedimento è stato definitivamente archiviato nel 2010, dopo il pagamento di una somma di denaro da parte di WS, conformemente a un procedimento specifico di transazione previsto nel diritto penale tedesco. Successivamente, il Bundeskriminalamt (Ufficio federale anticrimine, Germania) ha informato l'Interpol che, a suo parere, a causa di tale precedente procedimento, il principio del ne bis in idem era applicabile al

caso di specie. Tale principio, sancito sia all'articolo 54 della Convenzione di applicazione dell'accordo di Schengen [33] sia all'articolo 50 della Carta, vieta segnatamente che una persona che sia già stata giudicata con sentenza definitiva sia nuovamente sottoposta a procedimento penale per il medesimo reato.

Nel 2017 WS ha proposto un ricorso contro la Repubblica federale di Germania dinanzi al Verwaltungsgericht Wiesbaden (Tribunale amministrativo di Wiesbaden, Germania), affinché le fosse ordinato di adottare le misure necessarie per il ritiro del suddetto avviso rosso. A tal riguardo, WS deduce, oltre a una violazione del principio del ne bis in idem, una violazione del suo diritto alla libera circolazione, garantito dall'articolo 21 TFUE, in quanto egli non può recarsi in uno Stato parte dell'accordo di Schengen o in uno Stato membro senza rischiare di essere arrestato. Egli ritiene altresì che, a causa di tali violazioni, il trattamento dei suoi dati personali, contenuti nell'avviso rosso, sia contrario alla direttiva 2016/680, relativa alla protezione dei dati personali in materia penale [34].

È in tale contesto che il Tribunale amministrativo di Wiesbaden ha deciso di interpellare la Corte sull'applicazione del principio del ne bis in idem e, più precisamente, sulla possibilità di procedere all'arresto provvisorio di una persona oggetto di un avviso rosso in una situazione come quella di cui trattasi. Inoltre, in caso di applicabilità di tale principio, detto giudice chiede quali siano le conseguenze sul trattamento, da parte degli Stati membri, dei dati personali contenuti in siffatto avviso.

Nella sua sentenza, pronunciata in Grande Sezione, la Corte dichiara, in particolare, che le disposizioni della direttiva 2016/680, lette alla luce dell'articolo 54 della CAAS e dell'articolo 50 della Carta, devono essere interpretate nel senso che esse non ostano al trattamento dei dati personali contenuti in un avviso rosso emesso dall'Interpol, fintanto che non sia stato accertato, con siffatta decisione giudiziaria, che con riferimento ai fatti su cui detto avviso si basa si applica il principio del ne bis in idem, purché un simile trattamento soddisfi le condizioni previste da tale direttiva (punto 121 e disp. 2).

Quanto alla questione relativa ai dati personali contenuti in un avviso rosso dell'Interpol, la Corte dichiara che ogni operazione applicata a tali dati, come la loro registrazione nei sistemi di ricerca di uno Stato membro, costituisce un «trattamento» rientrante nella direttiva 2016/680 [35]. Essa considera inoltre, da un lato, che tale trattamento persegue una finalità legittima e, dall'altro, che esso non può essere considerato illecito per la sola ragione che il principio del ne bis in idem potrebbe applicarsi ai fatti su cui si basa l'avviso rosso [36]. Tale trattamento, da parte delle autorità degli Stati membri, può del resto risultare indispensabile proprio al fine di verificare l'applicabilità di detto principio (punti 111, 114, 116, 117 e 119).

---

[33] Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 tra i governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni (GU 2000, L 239, pag. 19; in prosieguo: la «CAAS»).

[34] 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 2016, L 119, pag. 89).

[35] V. articolo 2, paragrafo 1, e articolo 3, punto 2, della direttiva 2016/680.

[36] V. articolo 4, paragrafo 1, lettera b), e articolo 8, paragrafo 1, della direttiva 2016/680.

In tali circostanze, la Corte dichiara, parimenti, che la direttiva 2016/680, letta alla luce dell'articolo 54 della CAAS e dell'articolo 50 della Carta, non osta al trattamento dei dati personali contenuti in un avviso rosso, fintanto che una decisione giudiziaria definitiva non abbia accertato che, nella fattispecie, si applica il principio del ne bis in idem. Tuttavia, un simile trattamento deve rispettare le condizioni previste da tale direttiva. In questa ottica, esso deve essere necessario, in particolare, per l'esecuzione di un compito di un'autorità nazionale competente, a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali [37] (punto 121 e disp. 2).

Per contro, quando si applica il principio del ne bis in idem, la registrazione, nei sistemi di ricerca degli Stati membri, dei dati personali contenuti in un avviso rosso dell'Interpol non è più necessaria, dato che la persona di cui trattasi non può più essere sottoposta a procedimento penale per i fatti oggetto di detto avviso né, di conseguenza, essere arrestata per i medesimi fatti. Ne consegue che la persona interessata deve poter chiedere la cancellazione dei suoi dati. Se, tuttavia, tale registrazione è mantenuta, essa deve essere accompagnata dall'indicazione che la persona di cui trattasi non può più essere sottoposta a procedimento penale in uno Stato membro o in uno Stato contraente per i medesimi fatti, a causa del principio del ne bis in idem (punto 120).

Sentenza del 22 giugno 2021 (Grande Sezione), Latvijas Republikas Saeima (Punti di penalità) (C-439/19, EU:C:2021:504)

In tale sentenza (v. altresì la rubrica II.3., intitolata «Nozione di "trattamento dei dati personali"»), la Corte dichiara che il RGPD osta alla normativa che obbliga la Ceļu satiksmes drošības direkcija (Direzione per la sicurezza stradale, Lettonia; in prosieguo: la «CSDD») a rendere accessibili al pubblico i dati relativi ai punti di penalità inflitti ai conducenti di veicoli per infrazioni stradali, senza che la persona richiedente l'accesso debba dimostrare di avere un interesse specifico a ottenerli. Essa constata che la necessità, segnatamente alla luce dell'obiettivo di migliorare la sicurezza stradale addotto dal governo lettone, di comunicare dati personali relativi ai punti di penalità inflitti per infrazioni stradali, non è dimostrata. Inoltre, secondo la Corte, né il diritto del pubblico ad accedere ai documenti ufficiali, né il diritto alla libertà di informazione giustificano una normativa del genere (punti 113, da 120 a 122 e disp. 2).

In tale contesto, la Corte sottolinea che il miglioramento della sicurezza stradale, cui mira la normativa lettone, costituisce un obiettivo di interesse generale riconosciuto dall'Unione e che gli Stati membri sono quindi legittimati a qualificare la sicurezza stradale come «compito di interesse pubblico» [38]. Tuttavia, la necessità del regime lettone di comunicazione dei dati personali relativi ai punti di penalità per garantire il conseguimento dell'obiettivo considerato non è dimostrata. Infatti, da un lato, il legislatore lettone dispone di diverse linee d'azione, che gli avrebbero consentito di conseguire tale obiettivo con altri mezzi meno pregiudizievoli per i diritti fondamentali degli interessati. Dall'altro lato, occorre tener conto della sensibilità dei dati relativi ai punti di penalità e della circostanza che la loro comunicazione al pubblico può costituire una grave ingerenza nei diritti al rispetto della vita privata e alla protezione dei dati personali poiché

[37] V. articolo 1, paragrafo 1, e articolo 8, paragrafo 1, della direttiva 2016/680.

[38] In forza dell'articolo 6, paragrafo 1, lettera e), del RGPD, un trattamento di dati personali è lecito quando è «necessario per l'esecuzione di un compito di interesse pubblico **(...)**».

essa può suscitare la disapprovazione sociale e comportare la stigmatizzazione della persona interessata (punti da 109 a 113).

Inoltre, la Corte considera che, tenuto conto della sensibilità di tali dati e della gravità di detta ingerenza in questi due diritti fondamentali, tali diritti prevalgono sia sull'interesse del pubblico ad avere accesso a documenti ufficiali, come il registro nazionale dei veicoli e dei conducenti, sia sul diritto alla libertà d'informazione (punti 120 e 121).

Peraltro, per le medesime ragioni, la Corte dichiara che il RGPD osta anche alla normativa lettone nella parte in cui essa autorizza la CSDD a comunicare i dati relativi ai punti di penalità inflitti ai conducenti di veicoli per infrazioni stradali a operatori economici affinché questi ultimi possano riutilizzarli e comunicarli al pubblico (punto 126 e disp. 3).

Infine, la Corte precisa che il principio del primato del diritto dell'Unione osta a che il giudice del rinvio, investito di un ricorso avverso la normativa lettone, che la Corte ha qualificato incompatibile con il diritto dell'Unione, decida di mantenere gli effetti giuridici di tale normativa fino alla data di pronuncia della sua sentenza definitiva (punto 137 e disp. 4).

III. Trattamento dei dati personali ai sensi della direttiva 2002/58

Sentenza del 2 ottobre 2018 (Grande Sezione), Ministerio Fiscal (C-207/16, EU:C:2018:788) [39]

La presente causa verteva sul rigetto, da parte di un giudice istruttore spagnolo, di una domanda presentata nel contesto delle indagini su una rapina con sottrazione di un portafoglio e di un telefono cellulare. Più in particolare, la polizia giudiziaria aveva chiesto a detto giudice di accordarle l'accesso ai dati identificativi degli utenti dei numeri di telefono attivati dal telefono rubato per un periodo di dodici giorni a decorrere dalla data del furto. Il rigetto era basato sulla motivazione secondo cui i fatti all'origine dell'indagine penale non integravano gli estremi di un reato «grave» – vale a dire, secondo il diritto spagnolo, un reato punibile con pena detentiva superiore a cinque anni – e l'accesso ai dati di identificazione era in effetti possibile solamente per tale tipo di reati.

Dopo aver ricordato che l'accesso di autorità pubbliche a dati personali conservati dai fornitori di servizi di comunicazione elettronica, nell'ambito di un procedimento istruttorio penale, rientra nell'ambito di applicazione della direttiva 2002/58, la Corte ha dichiarato che l'accesso ai dati che mirano all'identificazione dei titolari delle carte SIM attivate con un telefono cellulare rubato, quali i nomi, i cognomi e, se del caso, gli indirizzi di tali titolari, costituisce un'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati, sanciti dalla Carta, persino in mancanza di circostanze che permettano di qualificare tale ingerenza come «grave», e senza che rilevi il fatto che le informazioni in questione relative alla vita privata siano o meno delicate o che gli interessati abbiano subito o meno eventuali inconvenienti a seguito di tale ingerenza. Tuttavia, la Corte ha sottolineato che tale ingerenza non presenta una gravità tale da dover limitare il suddetto accesso, in materia di prevenzione, ricerca, accertamento e perseguimento

[39] Detta sentenza è stata presentata nella Relazione annuale 2018, pagg. 88 e 89.

dei reati, alla lotta contro la criminalità grave. Infatti, se la direttiva 2002/58 elenca in maniera tassativa gli obiettivi idonei a giustificare una normativa nazionale che disciplina l'accesso delle autorità pubbliche ai dati interessati e che deroga pertanto al principio della riservatezza delle comunicazioni elettroniche, e tale accesso deve rispondere in modo effettivo e rigoroso a uno di tali obiettivi, la Corte osserva che, per quanto riguarda l'obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati, la formulazione della direttiva 2002/58 non limita tale obiettivo alla lotta contro i soli reati gravi, ma si riferisce ai «reati» in generale (punti 38, 42, da 59 a 63 e disp.).

In tale contesto, la Corte ha precisato che, se è vero che nella sua sentenza Tele2 Sverige e Watson e a. [40], essa aveva affermato che soltanto la lotta contro la criminalità grave è idonea a giustificare un accesso delle autorità pubbliche a dati personali conservati dai fornitori di servizi di comunicazione che, considerati nel loro insieme, consentono di trarre conclusioni precise sulla vita privata delle persone i cui dati sono oggetto di attenzione, una siffatta interpretazione era motivata dal fatto che l'obiettivo perseguito da una normativa che disciplina tale accesso deve essere adeguato alla gravità dell'ingerenza nei diritti fondamentali in questione che tale operazione determina. Pertanto, in conformità al principio di proporzionalità, una grave ingerenza può essere giustificata in tale settore solo da un obiettivo di lotta contro la criminalità che deve essere parimenti qualificata come «grave». Al contrario, qualora l'ingerenza non sia grave, detto accesso può essere giustificato da un obiettivo di prevenzione, ricerca, accertamento e perseguimento di un «reato» in generale.

Per quanto attiene al caso di specie, la Corte ha considerato che l'accesso ai soli dati oggetto della domanda in questione non può essere qualificato come un'ingerenza «grave» nei diritti fondamentali delle persone i cui dati sono oggetto di attenzione, poiché tali dati non consentono di trarre conclusioni precise sulla loro vita privata. La Corte ne ha tratto la conclusione che l'ingerenza che un accesso a tali dati comporterebbe può essere quindi giustificata dall'obiettivo di prevenzione, ricerca, accertamento e perseguimento di «reati» in generale, senza che sia necessario che tali reati siano qualificati come «gravi» (punti 61 e 62).

Sentenze del 6 ottobre 2020 (Grande Sezione), Privacy International (C-623/17, EU:C:2020:790) e La Quadrature du Net e a.(C-511/18, C-512/18 e C-520/18, EU:C:2020:791) [41]

La giurisprudenza relativa alla conservazione e all'accesso ai dati personali nel settore delle comunicazioni elettroniche, in particolare la sentenza Tele2 Sverige e Watson e a., nella quale la Corte ha in particolare considerato che gli Stati membri non potevano imporre ai fornitori di servizi di comunicazione elettronica un obbligo di conservazione generalizzato e indifferenziato dei dati relativi al traffico e all'ubicazione, ha suscitato le preoccupazioni di taluni Stati, che temevano di essere stati privati di uno strumento che essi ritengono necessario per la salvaguardia della sicurezza nazionale e per la lotta alla criminalità.

In tale contesto l'Investigatory Powers Tribunal (Tribunale incaricato dei poteri di indagine, Regno Unito) (Privacy International, C-623/17), il Conseil d'État (Consiglio di Stato, Francia) (La Quadrature du Net e a., cause riunite C-511/18 e C-512/18), nonché la Cour constitutionnelle

[40] Sentenza della Corte del 21 dicembre 2016, *Tele2 Sverige e Watson e a.* (C-293/15 e C-594/15, EU:C:2016:970).
[41] Dette sentenze sono state presentate nella Relazione annuale 2020, pagg. da 29 a 32.

(Corte costituzionale, Belgio) (Ordre des barreaux francophones et germanophone e a., C-520/18) sono stati chiamati a pronunciarsi su controversie relative alla legittimità delle normative adottate da taluni Stati membri in tali settori, che prevedono, in particolare, l'obbligo per i fornitori di servizi di comunicazione elettronica di trasmettere a un'autorità pubblica o di conservare in maniera generalizzata o indifferenziata i dati degli utenti relativi al traffico e all'ubicazione.

Con due sentenze pronunciate in Grande Sezione, il 6 ottobre 2020, la Corte dichiara, anzitutto, che normative nazionali che impongono ai fornitori di servizi di comunicazione elettronica di conservare dati relativi al traffico e all'ubicazione oppure di trasmettere tali dati alle autorità nazionali di sicurezza e di intelligence a tal fine rientrano nell'ambito di applicazione della direttiva 2002/58 (punto 49, disp. 1 della sentenza Privacy International e punto 104 della sentenza La Quadrature du Net e a.).

La Corte ricorda poi che la direttiva 2002/58 [42] non consente che la deroga all'obbligo di principio di garantire la riservatezza delle comunicazioni elettroniche e dei dati a queste correlati e al divieto di memorizzare tali dati divenga la regola. Ciò implica che tale direttiva autorizza gli Stati membri ad adottare, tra l'altro a fini di sicurezza nazionale, misure legislative volte a limitare la portata dei diritti e degli obblighi previsti da tale direttiva, in particolare l'obbligo di garantire la riservatezza delle comunicazioni e dei dati relativi al traffico [43], solo nel rispetto dei principi generali del diritto dell'Unione, tra i quali figura il principio di proporzionalità, e dei diritti fondamentali garantiti dalla Carta [44] (punti 59 e 60 della sentenza Privacy International e punti 111 e 113 della sentenza La Quadrature du Net e a.).

In tale contesto, la Corte considera, da un lato, nella causa Privacy International, che la direttiva 2002/58, letta alla luce della Carta, osta a una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica, al fine di salvaguardare la sicurezza nazionale, la trasmissione generalizzata e indifferenziata ai servizi di sicurezza e di intelligence dei dati relativi al traffico e all'ubicazione. Dall'altro lato, nelle cause riunite La Quadrature du Net e a. nonché nella causa Ordre des barreaux francophones et germanophone e a., la Corte considera che la stessa direttiva osta a misure legislative che impongono ai fornitori di servizi di comunicazione elettronica, a titolo preventivo, una conservazione generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione.

Infatti, tali obblighi di trasmissione e di conservazione generalizzata e indifferenziata di tali dati costituiscono ingerenze particolarmente gravi nei diritti fondamentali garantiti dalla Carta, senza che il comportamento delle persone i cui dati sono interessati presenti un nesso con l'obiettivo perseguito dalla normativa di cui trattasi. Analogamente, la Corte interpreta l'articolo 23, paragrafo 1, del RGPD, letto alla luce della Carta, nel senso che osta a una normativa nazionale che impone ai fornitori di accesso a servizi di comunicazione al pubblico online e ai fornitori di servizi di hosting la conservazione generalizzata e indifferenziata, in particolare, dei dati personali relativi a tali servizi (punti 71, 82 e disp. 2 della sentenza Privacy International e punti 146, 168, 174, 177, 212, disp. 1 e 3 della sentenza La Quadrature du Net e a.).

---

42 Articolo 15, paragrafi 1 e 3, della direttiva 2002/58.

43 Articolo 5, paragrafo1, della direttiva 2002/58.

44 In particolare, articoli 7, 8 e 11 nonché articolo 52, paragrafo 1, della Carta.

Per contro, la Corte considera che, in situazioni in cui lo Stato membro interessato affronta una minaccia grave per la sicurezza nazionale che risulta reale e attuale o prevedibile, la direttiva 2002/58, letta alla luce della Carta, non osta al fatto di ingiungere ai fornitori di servizi di comunicazione elettronica di conservare in maniera generalizzata e indifferenziata dati relativi al traffico e all'ubicazione. In tale contesto, la Corte precisa che la decisione che prevede tale ingiunzione, per un periodo temporalmente limitato allo stretto necessario, deve essere oggetto di un controllo effettivo, da parte di un giudice o di un organo amministrativo indipendente, la cui decisione sia dotata di effetto vincolante, al fine di verificare l'esistenza di una di tali situazioni nonché il rispetto delle condizioni e delle garanzie previste. Nelle stesse circostanze, detta direttiva non osta neppure all'analisi automatizzata dei dati, in particolare quelli relativi al traffico e all'ubicazione, di tutti gli utenti di mezzi di comunicazione elettronica (punti da 137 a 139, da 177 a 179, disp. 1 e 2 della sentenza La Quadrature du Net e a.).

La Corte aggiunge che la direttiva 2002/58, letta alla luce della Carta, non osta a misure legislative che consentono il ricorso a una conservazione mirata, temporalmente limitata allo stretto necessario, dei dati relativi al traffico e all'ubicazione, che sia delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico. Analogamente, tale direttiva non osta a siffatte misure che prevedono una conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una comunicazione, purché la durata della conservazione sia limitata allo stretto necessario, né a quelle che prevedono una siffatta conservazione dei dati relativi all'identità civile degli utenti dei mezzi di comunicazione elettronica, e gli Stati membri non sono tenuti, in quest'ultimo caso, a limitare nel tempo la conservazione. Inoltre, detta direttiva non osta a una misura legislativa che consente il ricorso a una conservazione rapida dei dati di cui dispongono i fornitori di servizi qualora si presentino situazioni nelle quali si pone l'esigenza di conservare detti dati oltre i termini legali di conservazione dei dati al fine di indagare su reati gravi o attentati alla sicurezza nazionale, qualora tali reati o attentati siano già stati accertati o la loro esistenza possa essere ragionevolmente sospettata (punti 161, 163, 168 e disp. 1 della sentenza La Quadrature du Net e a.).

Inoltre, la Corte dichiara che la direttiva 2002/58, letta alla luce della Carta, non osta a una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica il ricorso a una raccolta in tempo reale, in particolare, dei dati relativi al traffico e all'ubicazione, quando tale raccolta è limitata alle persone nei confronti delle quali esiste un valido motivo per sospettare che esse siano implicate, in un modo o nell'altro, in attività di terrorismo ed è soggetta a un controllo preventivo, effettuato da un giudice o da un organo amministrativo indipendente, la cui decisione ha effetto vincolante, al fine di accertarsi che tale raccolta in tempo reale sia autorizzata soltanto nei limiti di quanto strettamente necessario. In caso di emergenza, il controllo deve avvenire tempestivamente (punto 192 e disp. 2 della sentenza La Quadrature du Net e a.).

Infine, la Corte affronta la questione del mantenimento degli effetti nel tempo di una normativa nazionale giudicata incompatibile con il diritto dell'Unione. A tal riguardo, essa dichiara che un giudice nazionale non può applicare una disposizione del suo diritto nazionale che lo autorizzi a limitare nel tempo gli effetti di una dichiarazione di illegittimità ad esso incombente, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica una conservazione generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione, giudicata incompatibile con la direttiva 2002/58, letta alla luce della Carta.

Ciò premesso, al fine di fornire una risposta utile al giudice nazionale, la Corte ricorda che l'ammissibilità e la valutazione di elementi di prova ottenuti mediante una conservazione di dati contraria al diritto dell'Unione, nell'ambito di un procedimento penale avviato nei confronti di persone sospettate di avere commesso reati gravi, rientra, allo stato attuale del diritto dell'Unione, unicamente nel diritto nazionale. Tuttavia, la Corte precisa che la direttiva 2002/58 58, interpretata alla luce del principio di effettività, impone al giudice penale nazionale di non tener conto degli elementi di prova ottenuti mediante una conservazione generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione incompatibile con il diritto dell'Unione, nell'ambito di siffatto procedimento penale, qualora le persone sospettate di avere commesso reati non siano in grado di prendere efficacemente posizione su tali elementi di prova (punti 222, 228 e disp. 4 della sentenza La Quadrature du Net e a.).

Sentenza del 2 marzo 2021 (Grande Sezione), Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) (C-746/18, EU:C:2021:152)

In Estonia è stato instaurato un procedimento penale a carico di H. K. per le imputazioni di furto, di uso della carta bancaria di un terzo e di violenza nei confronti di persone partecipanti a un procedimento giudiziario. H. K. è stata condannata per tali reati da un tribunale di primo grado a una pena detentiva di due anni. Tale decisione è stata successivamente confermata in appello. I verbali sui quali si fonda la constatazione dei reati suddetti sono stati redatti, in particolare, sulla base di dati personali generati nel quadro della fornitura di servizi di comunicazione elettronica. La Riigikohus (Corte suprema, Estonia), dinanzi alla quale H. K. ha proposto un ricorso per cassazione, ha sollevato dubbi riguardo alla compatibilità con il diritto dell'Unione [45] dei presupposti in presenza dei quali gli organi inquirenti hanno avuto accesso ai dati suddetti.

Tali dubbi riguardano, in primo luogo, la questione se la durata del periodo per il quale gli organi inquirenti hanno avuto accesso ai dati costituisca un criterio che consente di valutare la gravità dell'ingerenza che tale accesso determina nei diritti fondamentali delle persone interessate. Così, nel caso in cui tale periodo sia particolarmente breve o la quantità di dati raccolti sia assai limitata, il giudice del rinvio si è interrogato sulla questione se l'obiettivo della lotta contro la criminalità in generale, e non soltanto della lotta contro le forme gravi di criminalità, sia idoneo a giustificare siffatta ingerenza. In secondo luogo, il giudice del rinvio ha nutrito dubbi quanto alla possibilità di considerare il pubblico ministero estone, alla luce dei diversi compiti che gli sono affidati dalla normativa nazionale, come un'autorità amministrativa «indipendente» ai sensi della sentenza Tele2 Sverige e Watson e a. [46], che può autorizzare l'accesso dell'autorità incaricata dell'indagine ai dati in questione.

Con la sua sentenza, pronunciata in Grande Sezione, la Corte dichiara che la direttiva 2002/58, letta alla luce della Carta, osta a una normativa nazionale, la quale consenta l'accesso di autorità pubbliche a dati relativi al traffico o di dati relativi all'ubicazione, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da costui utilizzate e a permettere di trarre

[45] Più precisamente, con l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta.

[46] Sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970, punto 120).

precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica. Secondo la Corte, la durata del periodo per il quale l'accesso a tali dati viene richiesto nonché la quantità o la natura dei dati disponibili per tale periodo non hanno alcuna incidenza al riguardo. Inoltre, la Corte considera che la medesima direttiva, letta alla luce della Carta, osta a una normativa nazionale, la quale renda il pubblico ministero competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione al fine di condurre un'istruttoria penale (punti 45, 59, disp. 1 e 2).

Per quanto riguarda l'obiettivo della prevenzione, della ricerca, dell'accertamento e del perseguimento di reati, perseguito dalla normativa in questione, conformemente al principio di proporzionalità, la Corte considera che soltanto gli obiettivi della lotta contro le forme gravi di criminalità o della prevenzione di gravi minacce per la sicurezza pubblica sono idonei a giustificare l'accesso delle autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi all'ubicazione, tali da permettere di trarre precise conclusioni sulla vita privata delle persone interessate, senza che altri fattori attinenti alla proporzionalità di una domanda di accesso, come la durata del periodo per il quale viene richiesto l'accesso a tali dati, possano avere come effetto che l'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale sia idoneo a giustificare tale accesso (punti 33 e 35).

Per quanto riguarda la competenza conferita al pubblico ministero ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione al fine di dirigere un'istruttoria penale, la Corte ricorda che spetta al diritto nazionale stabilire le condizioni alle quali i fornitori di servizi di comunicazioni elettroniche devono accordare alle autorità nazionali competenti l'accesso ai dati di cui essi dispongono. Tuttavia, per soddisfare il requisito di proporzionalità, tale normativa deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e fissino dei requisiti minimi, di modo che le persone i cui dati personali vengono in discussione dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati contro i rischi di abusi. Tale normativa deve essere legalmente vincolante nell'ordinamento interno e precisare in quali circostanze e a quali condizioni sostanziali e procedurali possa essere adottata una misura che prevede il trattamento di dati del genere, in modo da garantire che l'ingerenza sia limitata allo stretto necessario (punto 48).

Secondo la Corte, al fine di garantire, in pratica, il pieno rispetto di tali condizioni, è essenziale che l'accesso delle autorità nazionali competenti ai dati conservati sia subordinato ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente e che la decisione di tale giudice o di tale entità intervenga a seguito di una richiesta motivata delle autorità suddette presentata, in particolare, nell'ambito di procedure di prevenzione o di accertamento di reati ovvero nel contesto di azioni penali esercitate. In caso di urgenza debitamente giustificata, il controllo deve intervenire entro termini brevi (punto 51).

A tal proposito, la Corte precisa che il controllo preventivo richiede, tra l'altro, che il giudice o l'entità incaricata di effettuare tale controllo disponga di tutte le attribuzioni e presenti tutte le garanzie necessarie per garantire una conciliazione dei diversi interessi e diritti in gioco. Per quanto riguarda, più in particolare, un'indagine penale, tale controllo preventivo richiede che detto giudice o detta entità sia in grado di garantire un giusto equilibrio tra, da un lato, gli interessi connessi alle necessità dell'indagine nell'ambito della lotta contro la criminalità e,

dall'altro, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone i cui dati sono interessati dall'accesso. Qualora tale controllo venga effettuato non da un giudice bensì da un'entità amministrativa indipendente, quest'ultima deve godere di uno status che le permetta di agire, nell'assolvimento dei propri compiti, in modo obiettivo e imparziale, e deve essere, a tale scopo, al riparo da qualsiasi influenza esterna (punti 52 e 53).

A giudizio della Corte, ne consegue che il requisito di indipendenza che l'autorità incaricata di esercitare il controllo preventivo deve soddisfare impone che tale autorità abbia la qualità di terzo rispetto a quella che chiede l'accesso ai dati, di modo che la prima sia in grado di esercitare tale controllo in modo obiettivo e imparziale al riparo da qualsiasi influenza esterna. In particolare, in ambito penale, il requisito di indipendenza implica che l'autorità incaricata di tale controllo preventivo, da un lato, non sia coinvolta nella conduzione dell'indagine penale di cui trattasi e, dall'altro, abbia una posizione di neutralità nei confronti delle parti del procedimento penale. Orbene, ciò non si verifica nel caso di un pubblico ministero che, come nel caso del pubblico ministero estone, diriga il procedimento di indagine ed eserciti, se del caso, l'azione penale. Ne consegue che il pubblico ministero non è in grado di effettuare il suddetto controllo preventivo (punti 54, 55 e 57).

IV. Trasferimento dei dati personali verso paesi terzi

Sentenza del 6 novembre 2003 (Grande Sezione), Lindqvist (C-101/01, EU:C:2003:596)[47]

In tale causa (v. altresì la rubrica II.3., intitolata «Nozione di "trattamento di dati personali"»), il giudice del rinvio chiedeva, 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, 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 e disp. 4).

Infatti, tenuto conto, da una parte, dello stato di sviluppo di Internet all'epoca dell'elaborazione della direttiva 95/46 e, dall'altra, della mancanza di criteri applicabili all'uso di Internet nel suo capo IV, che comprende detto articolo 25, volto a garantire un controllo da parte degli Stati membri sui trasferimenti di dati personali verso i paesi terzi e a vietare questi trasferimenti quando non offrono un livello di tutela adeguato, non si può presumere che il legislatore comunitario avesse l'intenzione di includere prospettivamente, nella nozione di «trasferimenti verso un paese terzo di dati personali», tale 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 e 68).

[47] Detta 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) [48]

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 Commissionner aveva rifiutato di istruire tale denuncia, per il motivo, in particolare, che nella sua decisione 2000/520/CE [49], la Commissione aveva considerato che, nel contesto del cosiddetto regime dell'«approdo sicuro» (in inglese, «safe harbour») [50], gli Stati Uniti garantivano un livello adeguato di protezione dei dati personali trasferiti.

In tale contesto la Corte è stata investita dalla High Court (Alta Corte, Irlanda) di una domanda di interpretazione dell'articolo 25, paragrafo 6, della direttiva 95/46, 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 adottata dalla Commissione sulla base di detto articolo 25, paragrafo 6, della direttiva 95/46.

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 garantisce effettivamente un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell'ordinamento giuridico dell'Unione. Orbene, poiché la Commissione, nella sua decisione 2000/520, non ha affermato ciò, l'articolo 1 di tale decisione viola i requisiti fissati all'articolo 25, paragrafo 6, della direttiva 95/46, 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 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, da 87 a 89, da 96 a 98 e disp. 2).

Inoltre, la Corte ha dichiarato invalido l'articolo 3 della decisione 2000/520, nella parte in cui priva le autorità nazionali di controllo dei poteri che esse traggono dall'articolo 28 della direttiva 95/46, 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

---

48 Detta sentenza è stata presentata nella Relazione annuale 2015, pag. 53.

49 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 2000, L 215, pag. 7).

50 Il regime dell'approdo sicuro comprende una serie di principi relativi alla protezione dei dati personali ai quali le imprese statunitensi possono aderire volontariamente.

fondamentali della persona (punti da 102 a 104). La Corte ha concluso che l'invalidità degli articoli 1 e 3 della decisione 2000/520 inficiava la validità di tale decisione nel suo complesso (punti 105 e 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 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 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 e 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 al fine di accertare 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 stabilisce, 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 e 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 dei reati gravi di natura transnazionale), 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 e 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. Per contro, 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 da 205 a 207 e 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, nelle ipotesi in cui si presentino elementi obiettivi che giustificano l'uso dei dati del codice di prenotazione al fine di combattere il terrorismo e i reati gravi di natura transnazionale e che richiedono una previa autorizzazione di un'autorità giudiziaria o di un ente amministrativo indipendente, un'informazione individuale ai passeggeri aerei risulta necessaria. 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 e 224).

Sentenza del 16 luglio 2020 (Grande Sezione), Facebook Ireland e Schrems (C-311/18, EU:C:2020:559) [51]

Il RGPD dispone che il trasferimento di tali dati verso un paese terzo può avere luogo, in linea di principio, solo se il paese terzo in questione garantisce un livello di protezione adeguato a tali dati. Secondo tale regolamento, la Commissione può constatare che un paese terzo garantisce, in considerazione della sua legislazione nazionale o degli impegni internazionali, un livello di

[51] Detta sentenza è stata presentata nella Relazione annuale 2020, pagg. da 26 a 29.

protezione adeguato [52]. In mancanza di una decisione di adeguatezza siffatta, un trasferimento del genere può essere effettuato solo se l'esportatore dei dati personali, stabilito nell'Unione, prevede garanzie adeguate, le quali possono risultare, in particolare, da clausole tipo di protezione dei dati adottate dalla Commissione, e se gli interessati dispongono di diritti azionabili e di mezzi di ricorso effettivi [53]. Il RGPD stabilisce precisamente, inoltre, a quali condizioni può avvenire un trasferimento siffatto in mancanza di una decisione di adeguatezza o di garanzie adeguate [54].

Il sig. Maximillian Schrems, cittadino austriaco residente in Austria, è iscritto a Facebook dal 2008. Al pari di quanto avviene per gli altri utenti residenti dell'Unione, i dati personali del sig. Schrems vengono trasferiti, in tutto o in parte, da Facebook Ireland verso server di Facebook Inc., ubicati nel territorio degli Stati Uniti, ove sono oggetto di trattamento. Il sig. Schrems ha depositato una denuncia presso l'autorità irlandese di controllo, volta, in sostanza, a far vietare tali trasferimenti. Egli ha sostenuto che il diritto e la prassi degli Stati Uniti non offrono una protezione sufficiente contro l'accesso, da parte delle autorità pubbliche, ai dati trasferiti verso tale paese. Tale denuncia è stata respinta segnatamente sulla base del rilievo che la Commissione aveva constatato, nella sua decisione 2000/520 [55], che gli Stati Uniti garantivano un livello adeguato di protezione. Con sentenza pronunciata il 6 ottobre 2015, la Corte, investita di una questione pregiudiziale sottopostale dalla High Court (Alta Corte, Irlanda), ha dichiarato invalida tale decisione (in prosieguo la «sentenza Schrems I») [56] (punti 52 e 53).

A seguito della sentenza Schrems I e del successivo annullamento, ad opera del giudice irlandese, della decisione di rigetto della denuncia del sig. Schrems, l'autorità di controllo irlandese ha invitato quest'ultimo a riformulare la sua denuncia tenendo conto della dichiarazione di invalidità, da parte della Corte, della decisione 2000/520. Nella sua denuncia riformulata il sig. Schrems sostiene che gli Stati Uniti non offrono una protezione sufficiente per i dati trasferiti verso tale paese. Egli chiede di sospendere o di vietare, per il futuro, i trasferimenti dei suoi dati personali dall'Unione verso gli Stati Uniti, che Facebook Ireland effettua oramai sulla base delle clausole tipo di protezione contenute nell'allegato della decisione 2010/87/UE [57]. Considerando che il trattamento della denuncia del sig. Schrems dipendeva, in particolare, dalla validità della decisione 2010/87, l'autorità di controllo irlandese ha avviato un procedimento dinanzi alla High Court affinché quest'ultima presentasse alla Corte una domanda di pronuncia pregiudiziale. Dopo l'avvio di tale procedimento, la Commissione ha adottato la decisione (UE) 2016/1250 sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy [58] (punti 54, 55 e 57).

Con la sua domanda di pronuncia pregiudiziale, il giudice del rinvio interroga la Corte

---

52 Articolo 45 del RGPD.

53 Articolo 46, paragrafi 1 e 2, lettera c), del RGPD.

54 Articolo 49 del RGPD.

55 Decisione 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 2000, L 215, pag. 7).

56 Sentenza della Corte del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650 (v. altresì CS n. 117/15).

57 Decisione della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio (GU 2010, L 39, pag. 5), come modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione del 16 dicembre 2016 (GU 2016, L 344, pag. 100).

58 Decisione di esecuzione della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy (GU 2016, L 207, pag. 1).

sull'applicabilità del RGPD a trasferimenti di dati personali fondati su clausole tipo di protezione contenute nella decisione 2010/87, sul livello di protezione richiesto da tale regolamento nel quadro di un trasferimento siffatto e sugli obblighi che incombono alle autorità di controllo in tale contesto. La High Court ha sollevato inoltre la questione della validità tanto della decisione 2010/87 quanto della decisione 2016/1250.

La Corte constata che dall'esame della decisione 2010/87 alla luce della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta») non emerge alcun elemento idoneo ad inficiarne la validità. Essa dichiara invece invalida la decisione 2016/1250 (disp. 4 e 5).

La Corte considera, anzitutto, che il diritto dell'Unione, e segnatamente il RGPD, si applica ad un trasferimento di dati personali effettuato a fini commerciali da un operatore economico stabilito in uno Stato membro verso un operatore economico stabilito in un paese terzo anche se, durante o in seguito a tale trasferimento, i suddetti dati possono essere sottoposti a trattamento a fini di pubblica sicurezza, di difesa e di sicurezza dello Stato da parte delle autorità del paese terzo considerato. La Corte precisa che tale tipo di trattamento di dati da parte delle autorità di un paese terzo non può escludere un trasferimento siffatto dall'ambito di applicazione del RGPD (punti 86, 88, 89 e disp. 1).

Per quanto riguarda il livello di protezione richiesto nell'ambito di un trasferimento siffatto, la Corte dichiara che i requisiti previsti a tal fine dalle disposizioni del RGPD, attinenti a garanzie adeguate, diritti azionabili e mezzi di ricorso effettivi, devono essere interpretati nel senso che le persone i cui dati personali sono trasferiti verso un paese terzo sulla base di clausole tipo di protezione dei dati devono godere di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta. In tale contesto essa precisa che la valutazione del suddetto livello di protezione deve prendere in considerazione tanto le clausole contrattuali convenute tra l'esportatore dei dati stabilito nell'Unione e il destinatario del trasferimento stabilito nel paese terzo interessato quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati così trasferiti, gli elementi rilevanti del sistema giuridico di quest'ultimo (punto 105 e disp. 2).

Relativamente agli obblighi che incombono alle autorità di controllo nel contesto di un trasferimento siffatto, la Corte dichiara che, salvo che esista una decisione di adeguatezza validamente adottata dalla Commissione, tali autorità sono segnatamente tenute a sospendere o a vietare un trasferimento di dati personali verso un paese terzo qualora ritengano, alla luce delle circostanze proprie di tale trasferimento, che le clausole tipo di protezione dei dati non siano o non possano essere rispettate in tale paese e che la protezione dei dati trasferiti, richiesta dal diritto dell'Unione, non possa essere garantita con altri mezzi, ove l'esportatore stabilito nell'Unione non abbia esso stesso sospeso tale trasferimento o messo fine a quest'ultimo (punto 121 e disp. 3).

La Corte esamina poi la validità della decisione 2010/87. Secondo la Corte, la validità di tale decisione non è rimessa in discussione dal solo fatto che le clausole tipo di protezione dei dati contenute in quest'ultima, per il loro carattere contrattuale, non vincolano le autorità del paese terzo verso il quale potrebbe essere effettuato un trasferimento di dati. Per contro, la Corte precisa che tale validità dipende dalla questione se la suddetta decisione contenga meccanismi efficaci che consentano, in pratica, di garantire che sia rispettato il livello di protezione richiesto dal diritto dell'Unione e che i trasferimenti di dati personali, fondati su tali clausole, siano

sospesi o vietati in caso di violazione di tali clausole o di impossibilità di rispettarle. La Corte constata che la decisione 2010/87 instaura meccanismi di questo tipo. A tal riguardo, essa sottolinea, in particolare, che la decisione in parola stabilisce un obbligo per l'esportatore dei dati e per il destinatario del trasferimento di verificare, preliminarmente, che tale livello di protezione sia rispettato nel paese terzo considerato, e inoltre che la decisione impone al suddetto destinatario di informare l'esportatore dei dati della sua eventuale impossibilità di conformarsi alle clausole tipo di protezione, con l'onere, in tal caso, per quest'ultimo di sospendere il trasferimento di dati e/o di risolvere il contratto concluso con il primo (punti 132, 136, 137, 142, 148 e disp. 4).

La Corte procede infine all'esame della validità della decisione 2016/1250 con riferimento ai requisiti derivanti dal RGPD, letto alla luce delle disposizioni della Carta che garantiscono il rispetto della vita privata e familiare, la protezione dei dati personali e il diritto ad una tutela giurisdizionale effettiva. A tal proposito, la Corte rileva che la suddetta decisione, al pari della decisione 2000/520, sancisce il primato delle esigenze attinenti alla sicurezza nazionale, all'interesse pubblico e al rispetto della normativa statunitense, rendendo così possibili ingerenze nei diritti fondamentali delle persone i cui dati sono trasferiti verso tale paese terzo. Secondo la Corte, le limitazioni della protezione dei dati personali che derivano dalla normativa interna degli Stati Uniti in materia di accesso e di utilizzo, da parte delle autorità pubbliche statunitensi, di tali dati trasferiti dall'Unione verso tale paese terzo, e che la Commissione ha valutato nella decisione 2016/1250, non sono inquadrate in modo da rispondere a requisiti sostanzialmente equivalenti a quelli richiesti, nel diritto dell'Unione, dal principio di proporzionalità, giacché i programmi di sorveglianza basati sulla suddetta normativa non sono limitati allo stretto necessario. Basandosi sulle constatazioni contenute in tale decisione, la Corte rileva che, per taluni programmi di sorveglianza, detta normativa non fa emergere in alcun modo l'esistenza di limitazioni all'autorizzazione, che essa comporta, per l'attuazione di tali programmi né l'esistenza di garanzie per i cittadini stranieri che ne sono potenzialmente oggetto. La Corte aggiunge che la stessa normativa, pur se prevede requisiti che devono essere rispettati dalle autorità statunitensi nell'attuare i programmi di sorveglianza considerati, non conferisce agli interessati diritti nei confronti delle autorità statunitensi azionabili dinanzi ai giudici (punti 164, 165, da 180 a 182, 184 e 185).

Quanto al requisito della tutela giurisdizionale, la Corte dichiara che, contrariamente a quanto considerato dalla Commissione nella decisione 2016/1250, il meccanismo di mediazione previsto da tale decisione non fornisce a tali persone un mezzo di ricorso dinanzi ad un organo che offra garanzie sostanzialmente equivalenti a quelle richieste nel diritto dell'Unione, tali da assicurare tanto l'indipendenza del Mediatore previsto da tale meccanismo quanto l'esistenza di norme che autorizzino il suddetto Mediatore di adottare decisioni vincolanti nei confronti dei servizi di intelligence statunitensi. Per tutte queste ragioni, la Corte dichiara invalida la decisione 2016/1250 (punti da 195 a 197, 201 e disp. 5).

V. La protezione dei dati personali su 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 ha precisato la portata dei diritti di accesso e di opposizione al trattamento dei dati personali in Internet, previsti dalla direttiva 95/46.

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, 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 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 e 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 o non siano più pertinenti, 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 dell'interessato 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 e 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 e 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) [59]

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 de 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») [60], 2001/29/CE, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione [61], 2004/48/CE, sul rispetto dei diritti di proprietà intellettuale [62], e 2002/58 non impongono agli Stati membri, in una situazione come quella oggetto del procedimento principale, di istituire l'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 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 dall'ordinamento giuridico comunitario. Inoltre, in sede di attuazione delle misure di trasposizione 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

---

59 Detta sentenza è stata presentata nella Relazione annuale 2008, pag. 46.

60 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 2000, L 178, pag. 1).

61 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 2001, L 167, pag. 10).

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

delle medesime che entri in conflitto con detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come il principio di proporzionalità (punto 70 e disp.).

Sentenza del 24 novembre 2011, Scarlet Extended (C-70/10, EU:C:2011:771)[63]

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, in via pregiudiziale, se una simile ingiunzione fosse compatibile con il diritto europeo.

La Corte ha dichiarato che le direttive 95/46, 2000/31, 2001/29, 2002/58 e 2004/48, lette in combinato disposto e interpretate alla luce delle condizioni derivanti dalla tutela dei diritti fondamentali applicabili, devono essere interpretate nel senso che ostano all'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 applica indistintamente a tutta la sua clientela, a titolo preventivo, a sue spese esclusive, e 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, tale ingiunzione non rispetta il divieto, sancito dall'articolo 15, paragrafo 1, della direttiva 2000/31, di imporre a siffatto 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 e 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 e 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

[63] Detta sentenza è stata presentata nella Relazione annuale 2011, pag. 37.

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).

Pertanto, la Corte ha constatato 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)

Lo Högsta domstolen (Corte suprema, Svezia) ha adito la Corte in via pregiudiziale per interpretare le direttive 2002/58 e 2004/48 nell'ambito di una controversia tra la Bonnier Audio AB, la 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 a una domanda di ingiunzione di comunicazione di dati formulata 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 delle 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 tale contesto, lo Högsta domstolen, investito di un ricorso per cassazione, ha sottoposto alla Corte la questione se il diritto dell'Unione osti all'applicazione di una disposizione nazionale, introdotta in forza dell'articolo 8 della direttiva 2004/48, che, in un procedimento civile e allo scopo di identificare un abbonato, permettesse di ingiungere ad un operatore Internet di comunicare al titolare di un diritto d'autore o al suo avente causa l'identità dell'abbonato al quale fosse stato attribuito un indirizzo IP utilizzato ai fini della violazione di detto diritto. Si presumeva, da un lato, che il richiedente l'ingiunzione avesse raccolto indizi effettivi dell'avvenuta violazione del diritto d'autore e, dall'altro, che la misura richiesta fosse proporzionata.

La Corte ha anzitutto ricordato che l'articolo 8, paragrafo 3, della direttiva 2004/48, in combinato disposto con l'articolo 15, paragrafo 1, della direttiva 2002/58, 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 obbligare gli Stati medesimi a 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 e 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 e 2004/48 non ostano ad una normativa nazionale, come quella oggetto del procedimento 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.).

Sentenza del 17 giugno 2021, M.I.C.M. (C-597/19, EU:C:2021:492)

L'impresa Mircom International Content Management & Consulting (M.I.C.M.) Limited (in prosieguo: la «Mircom») ha presentato una richiesta di informazioni diretta contro la Telenet BVBA, un fornitore di accesso a Internet, presso l'Ondernemingsrechtbank Antwerpen (Tribunale delle imprese di Anversa, Belgio; in prosieguo: il «giudice del rinvio»). Tale domanda è volta a ottenere una decisione che ingiunga alla Telenet di produrre i dati identificativi dei suoi clienti sulla base degli indirizzi IP raccolti, da una società specializzata, per conto della Mircom. Le connessioni Internet di clienti della Telenet sono state utilizzate per condividere film facenti parte del catalogo della Mircom su una rete tra utenti (peer-to-peer) con l'ausilio del protocollo BitTorrent. La Telenet si oppone alla domanda della Microm.

È in tale contesto che il giudice del rinvio ha anzitutto chiesto alla Corte se la condivisione di segmenti di un file multimediale contenente un'opera protetta su detta rete costituisca una comunicazione al pubblico ai sensi del diritto dell'Unione. Esso ha poi chiesto se il titolare di diritti di proprietà intellettuale, come la Mircom, che non li sfrutta, ma chiede il risarcimento del danno a presunti autori di violazioni, possa beneficiare delle misure, delle procedure e dei mezzi di ricorso previsti dal diritto dell'Unione al fine di garantire il rispetto di tali diritti, ad esempio richiedendo informazioni. Infine, il giudice del rinvio ha invitato la Corte a chiarire la questione della liceità, da un lato, del modo in cui gli indirizzi IP dei clienti sono stati raccolti dalla Mircom e, dall'altro, della comunicazione dei dati richiesta dalla Mircom alla Telenet.

La Corte dichiara che il diritto dell'Unione [64] non osta, in linea di principio, né alla registrazione sistematica, da parte del titolare di diritti di proprietà intellettuale o da parte di un terzo per suo conto, di indirizzi IP di utenti di reti tra pari (peer-to-peer) le cui connessioni Internet sono state asseritamente utilizzate in attività di violazione (trattamento dei dati a monte), né alla comunicazione dei nomi e degli indirizzi postali degli utenti a tale titolare o a un terzo ai fini di un ricorso per risarcimento danni (trattamento dei dati a valle). Tuttavia, le iniziative e le richieste in tal senso devono essere giustificate, proporzionate, non abusive e previste da una misura

[64] Articolo 6, paragrafo 1, lettera f), del RGPD e articolo 15, paragrafo 1, della direttiva 2002/58.

legislativa nazionale che limita la portata dei diritti e degli obblighi derivanti dal diritto dell'Unione. La Corte precisa che quest'ultimo non prevede l'obbligo per una società come la Telenet di comunicare a privati i dati personali al fine di poter avviare, dinanzi ai giudici civili, procedimenti nei confronti delle violazioni del diritto d'autore. Il diritto dell'Unione consente tuttavia agli Stati membri di imporre un siffatto obbligo (punti 97, da 125 a 127 e disp. 3).

3. Deindicizzazione di dati personali

Sentenza del 24 settembre 2019 (Grande Sezione), GC e a. (Deindicizzazione di dati sensibili) (C-136/17, EU:C:2019:773) [65]

In tale sentenza, la Corte, riunita in Grande Sezione, ha precisato gli obblighi del gestore di un motore di ricerca nell'ambito di una richiesta di deindicizzazione vertente su dati sensibili.

Google aveva rifiutato di accogliere le richieste di quattro persone di deindicizzare, dall'elenco dei risultati visualizzato dal motore di ricerca in esito a una ricerca effettuata a partire dai rispettivi nomi, vari link che rinviavano a pagine web pubblicate da terzi, in particolare articoli di stampa. A seguito delle denunce delle quattro persone di cui trattasi, la Commission nationale de l'informatique et des libertés (CNIL) (Commissione nazionale per l'informatica e le libertà, Francia) si è rifiutata di ingiungere a Google di procedere alle deindicizzazioni richieste. Il Conseil d'État (Consiglio di Stato, Francia), chiamato a pronunciarsi sulla causa, ha chiesto alla Corte di precisare gli obblighi gravanti sul gestore di un motore di ricerca in sede di trattamento di una richiesta di deindicizzazione ai sensi della direttiva 95/46.

In primo luogo la Corte ha ricordato che il trattamento dei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale è vietato [66], fatte salve alcune eccezioni e deroghe. Quanto al trattamento di dati relativi alle infrazioni, alle condanne penali o alle misure di sicurezza, esso può essere effettuato, in linea di principio, solo sotto controllo dell'autorità pubblica, o se vengono fornite opportune garanzie specifiche, sulla base del diritto nazionale [67] (punti 39 e 40).

La Corte ha dichiarato che il divieto e le restrizioni relative al trattamento di tali categorie particolari di dati si applicano al gestore di un motore di ricerca, al pari di qualsiasi altro responsabile del trattamento di dati personali. Infatti, la finalità di detti divieti e restrizioni consiste nel garantire una maggiore protezione contro trattamenti del genere, i quali, a causa della natura particolarmente sensibile di tali dati, possono costituire un'ingerenza particolarmente grave nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali (punti da 42 a 44).

Tuttavia, il gestore di un motore di ricerca è responsabile non del fatto che i dati personali compaiono su una pagina web pubblicata da terzi, ma dell'indicizzazione di tale pagina. Pertanto, il divieto e le restrizioni relativi al trattamento di dati sensibili si applicano a tale gestore solo a

[65] Detta sentenza è stata presentata nella Relazione annuale 2019, pagg. 117 e 118.
[66] Articolo 8, paragrafo 1, della direttiva 95/46 e articolo 9, paragrafo 1, del regolamento 2016/679.
[67] Articolo 8, paragrafo 5, della direttiva 95/46 e articolo 10 del regolamento 2016/679.

causa di tale indicizzazione e, quindi, mediante una verifica da effettuare, sotto il controllo delle autorità nazionali competenti, sulla base di una richiesta presentata dalla persona interessata (punti 46 e 47).

In secondo luogo la Corte ha dichiarato che, quando al gestore viene sottoposta una richiesta di deindicizzazione relativa a dati sensibili, esso è in linea di principio obbligato ad accoglierla, fatte salve determinate eccezioni. Quanto a tali eccezioni, il gestore può segnatamente rifiutarsi di accogliere una simile richiesta ove constati che i link rinviano a dati manifestamente resi pubblici dalla persona interessata [68], purché l'indicizzazione di tali link rispetti le altre condizioni di liceità di un trattamento di dati personali e a meno che detta persona non abbia il diritto di opporsi a detta indicizzazione per motivi derivanti dalla sua situazione specifica [69] (punti 65 e 69).

In ogni caso, il gestore di un motore di ricerca, quando riceve una richiesta di deindicizzazione, deve verificare se l'inserimento, nell'elenco dei risultati, del link verso una pagina web in cui sono pubblicati dati sensibili, visualizzato in esito ad una ricerca effettuata a partire dal nome della persona in questione, si riveli strettamente necessario per proteggere la libertà di informazione degli utenti di Internet potenzialmente interessati ad avere accesso a tale pagina web mediante una ricerca siffatta. A tal proposito, la Corte ha sottolineato che, sebbene i diritti al rispetto della vita privata e alla protezione dei dati personali prevalgano, di norma, sulla libertà di informazione degli utenti di Internet, tale equilibrio può nondimeno dipendere, in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona interessata, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, in base al ruolo che tale persona riveste nella vita pubblica (punti 66 e 68).

In terzo luogo, la Corte ha dichiarato che, nell'ambito di una richiesta di deindicizzazione riguardante dati relativi a un procedimento penale a carico della persona interessata, che si riferiscono a una fase precedente di tale procedimento e non corrispondono più alla situazione attuale, incombe al gestore del motore di ricerca valutare se, tenuto conto di tutte le circostanze del caso di specie, detta persona abbia diritto a che le informazioni di cui trattasi non siano più, allo stato attuale, collegate al suo nome mediante un elenco dei risultati, visualizzato in esito ad una ricerca effettuata a partire da tale nome. Tuttavia, anche se tale ipotesi non ricorre per il fatto che l'inserimento di tale link si rivela strettamente necessario per conciliare i diritti della persona interessata al rispetto della vita privata e alla protezione dei dati con la libertà di informazione degli utenti di Internet potenzialmente interessati, il gestore è tenuto, al più tardi al momento della richiesta di deindicizzazione, a sistemare l'elenco dei risultati in modo tale che l'immagine globale che ne risulta per l'utente di Internet rifletta la situazione giudiziaria attuale, il che necessita, in particolare, che compaiano per primi, nel suddetto elenco, i link verso pagine web contenenti informazioni a tal proposito (punti 77 e 78).

[68] Articolo 8, paragrafo 2, lettera e), della direttiva 95/46 e articolo 9, paragrafo 2, lettera e), del regolamento 2016/679.
[69] Articolo 14, primo comma, lettera a), della direttiva 95/46 e articolo 21, paragrafo 1, del regolamento 2016/679.

Sentenza del 24 settembre 2019 (Grande Sezione), Google (Portata territoriale della deindicizzazione) C-507/17, EU:C:2019:772) [70]

La Commission nationale de l'informatique et des libertés (CNIL) (Commissione nazionale per l'informatica e le libertà; in prosieguo: la «CNIL», Francia) ha ingiunto a Google di procedere, quando accoglie una richiesta di deindicizzazione, alla cancellazione dall'elenco di risultati visualizzato a seguito di una ricerca effettuata a partire dal nome della persona interessata, dei link che rinviano a pagine web contenenti dati personali relativi a quest'ultima, su tutte le estensioni del nome di dominio del suo motore di ricerca. A seguito del rifiuto di Google di ottemperare a tale ingiunzione, la CNIL ha inflitto a tale società una sanzione di EUR 100 000. Il Conseil d'État (Consiglio di Stato, Francia), adito da Google, ha chiesto alla Corte di precisare la portata territoriale dell'obbligo, per il gestore di un motore di ricerca, di attuare il diritto alla deindicizzazione in applicazione della direttiva 95/46.

Anzitutto, la Corte ha ricordato la possibilità per le persone fisiche di far valere, sulla base del diritto dell'Unione, il loro diritto alla deindicizzazione nei confronti del gestore di un motore di ricerca che dispone di uno o più stabilimenti nel territorio dell'Unione, indipendentemente dal fatto che il trattamento di dati personali (nella fattispecie, l'indicizzazione di link verso pagine web contenenti dati personali relativi alla persona che si avvale di tale diritto) avvenga o meno nell'Unione [71].

Quanto alla portata del diritto alla deindicizzazione, la Corte ha dichiarato che il gestore di un motore di ricerca è tenuto ad effettuare la deindicizzazione non su tutte le versioni del suo motore di ricerca, bensì sulle versioni di tale motore corrispondenti a tutti gli Stati membri. A tal proposito essa ha rilevato che anche se, tenuto conto delle caratteristiche di Internet e dei motori di ricerca, una deindicizzazione mondiale sarebbe idonea a conseguire pienamente l'obiettivo del legislatore dell'Unione consistente nel garantire un elevato livello di protezione dei dati personali in tutta l'Unione, non risulta affatto dal diritto dell'Unione [72] che, ai fini della realizzazione di un simile obiettivo, il legislatore abbia scelto di attribuire al diritto alla deindicizzazione una portata che vada oltre il territorio degli Stati membri. In particolare, mentre il diritto dell'Unione istituisce meccanismi di cooperazione tra autorità di controllo degli Stati membri per raggiungere una decisione comune, basata su un bilanciamento tra il diritto alla tutela della vita privata e dei dati personali, da un lato, e l'interesse del pubblico dei diversi Stati membri ad avere accesso alle informazioni, dall'altro, meccanismi del genere non sono attualmente previsti per quanto riguarda la portata di una deindicizzazione al di fuori dell'Unione (punti 62 e 63).

Allo stato attuale del diritto dell'Unione, il gestore di un motore di ricerca è tenuto a effettuare la deindicizzazione richiesta non sulla sola versione del motore corrispondente allo Stato membro di residenza del beneficiario di tale deindicizzazione, bensì sulle versioni del motore di ricerca corrispondenti agli Stati membri, e ciò al fine, segnatamente, di garantire un livello coerente ed elevato di protezione in tutta l'Unione. È compito, inoltre, di tale gestore adottare, se necessario, misure sufficientemente efficaci per impedire o, quanto meno, per scoraggiare seriamente gli

[70] Detta sentenza è stata presentata nella Relazione annuale 2019, pagg. 118 e 119.
[71] Articolo 4, paragrafo 1, lettera a), della direttiva 95/46, e articolo 3, paragrafo 1, del regolamento 2016/679.
[72] Articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46, e articolo 17, paragrafo 1, del regolamento 2016/679.

utenti di Internet dell'Unione dall'accedere – eventualmente a partire da una versione del motore di ricerca corrispondente a uno Stato terzo – ai link oggetto della deindicizzazione, e spetta al giudice nazionale verificare se le misure adottate dal gestore soddisfino tale esigenza (punto 70).

Infine, la Corte ha sottolineato che il diritto dell'Unione, pur non imponendo al gestore di un motore di ricerca di effettuare la deindicizzazione su tutte le versioni del suo motore, neppure lo vieta. Pertanto, un'autorità di controllo o un'autorità giudiziaria di uno Stato membro resta competente a effettuare, conformemente agli standard nazionali di protezione dei diritti fondamentali, un bilanciamento tra il diritto della persona interessata alla tutela della sua vita privata e alla protezione dei suoi dati personali, da un lato, e il diritto alla libertà d'informazione, dall'altro, e, al termine di tale bilanciamento, a richiedere, se del caso, al gestore di tale motore di ricerca di effettuare una deindicizzazione su tutte le versioni del suddetto motore (punti 65 e 72).

4. Consenso dell'utente di un sito Internet all'archiviazione di informazioni

Sentenza del 1° ottobre 2019 (Grande Sezione), Planet49 (C-673/17, EU:C:2019:801) [73]

Con tale sentenza, la Corte ha dichiarato che il consenso all'archiviazione di informazioni o all'accesso a informazioni attraverso cookie installati sull'apparecchiatura terminale dell'utente di un sito Internet non è validamente concesso qualora l'autorizzazione risulti da una casella di spunta preselezionata, indipendentemente dal fatto che le informazioni di cui trattasi costituiscano o meno dati personali. La Corte ha inoltre precisato che il fornitore di servizi deve comunicare all'utente di un sito Internet il periodo di attività dei cookie, nonché la possibilità o meno per i terzi di avere accesso a tali cookie.

La controversia nel procedimento principale verteva sull'organizzazione di un gioco a premi da parte della Planet49 sul sito Internet www.dein-macbook.de. Per partecipare, gli utenti di internet dovevano comunicare il loro nome e indirizzo in una pagina web nella quale erano presenti caselle di spunta da selezionare. La casella che autorizzava l'installazione dei cookie era preselezionata. Adito con un ricorso dalla Federazione tedesca delle organizzazioni di consumatori, il Bundesgerichtshof (Corte federale di giustizia, Germania) nutriva dubbi sulla validità del consenso degli utenti ottenuto mediante una casella di spunta preselezionata, nonché sulla portata dell'obbligo di informazione gravante sul fornitore di servizi.

La domanda di pronuncia pregiudiziale verteva essenzialmente sull'interpretazione della nozione di «consenso» di cui alla direttiva 2002/58 [74], letta in combinato disposto con la direttiva 95/46 [75], nonché con il RGPD [76].

In primo luogo, la Corte ha osservato che l'articolo 2, lettera h), della direttiva 95/46, alla quale fa rinvio l'articolo 2, lettera f), della direttiva 2002/58, definisce il consenso come «qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento». Essa ha rilevato che il requisito della «manifestazione» di volontà della persona interessata evoca chiaramente un comportamento attivo e non uno passivo. Orbene, il consenso espresso mediante una casella di spunta preselezionata non implica un comportamento attivo da parte dell'utente di un sito Internet. Inoltre, la genesi dell'articolo 5, paragrafo 3, della direttiva 2002/58, il quale prevede, dopo la modifica per effetto della direttiva 2009/136, che l'utente debba aver «espresso preliminarmente il proprio consenso» all'installazione di cookie, tende a indicare che il consenso dell'utente oramai non può più essere presunto e deve risultare dal comportamento attivo di quest'ultimo. Infine, un consenso attivo è ora previsto dal RGPD [77], il cui articolo 4, punto 11, richiede una manifestazione di volontà nella forma, segnatamente, di un'«azione positiva inequivocabile» e il cui considerando 32 esclude espressamente che «il silenzio, l'inattività o la preselezione di caselle» configurino consenso (punti 49, 52, 56 e 62).

---

73 Detta sentenza è stata presentata nella Relazione annuale 2019, pagg. 120 e 121.

74 Articoli 2, lettera f), e 5, paragrafo 3, della direttiva 2002/58, come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 (GU 2009, L 337, pag. 11).

75 Articolo 2, lettera h), della direttiva 95/46.

76 Articolo 6, paragrafo 1, lettera a), del regolamento 2016/679.

77 IDEM.

La Corte ha pertanto dichiarato che il consenso non è validamente espresso quando l'archiviazione di informazioni o l'accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente di un sito Internet sono autorizzati mediante una casella di spunta preselezionata che l'utente deve deselezionare al fine di negare il proprio consenso. Essa ha aggiunto che il fatto che l'utente attivi il pulsante di partecipazione al gioco a premi in questione non può essere sufficiente per ritenere che l'utente abbia validamente espresso il suo consenso all'installazione di cookie (punto 63).

In secondo luogo, la Corte ha constatato che l'articolo 5, paragrafo 3, della direttiva 2002/58 mira a proteggere l'utente da qualsiasi ingerenza nella sua vita privata, indipendentemente dal fatto che detta ingerenza riguardi o meno dati personali. Ne consegue che la nozione di «consenso» non deve essere interpretata in modo diverso a seconda che le informazioni archiviate o consultate nell'apparecchiatura terminale dell'utente di un sito Internet costituiscano o meno dati personali (punti 69 e 71).

In terzo luogo, la Corte ha rilevato che l'articolo 5, paragrafo 3, della direttiva 2002/58 esige che l'utente abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento. Orbene, un'informazione chiara e completa implica che un utente sia in grado di determinare agevolmente le conseguenze di un eventuale consenso prestato e assicurare che questo sia espresso con piena conoscenza di causa. A tal proposito, la Corte ha considerato che il periodo di attività dei cookie, nonché la possibilità o meno per i terzi di avere accesso a tali cookie rientrano nell'informazione chiara e completa da fornire all'utente di un sito Internet (punti da 73 a 75 e 81).

VI. 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) [78]

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, 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 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

[78] Detta sentenza è stata presentata nella Relazione annuale 2010, pag. 34.

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.

La Corte ha dichiarato che la garanzia dell'indipendenza delle autorità nazionali di controllo prevista dalla direttiva 95/46 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 per la vigilanza del 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 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.

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, 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, implica che le autorità di controllo

devono godere di un'indipendenza che consenta loro di svolgere le proprie funzioni senza influenze esterne. A tal riguardo, la circostanza che una siffatta 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, non è di per sé sufficiente a preservare l'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 da 41 a 43 e 52).

La Corte ha precisato che, per poter soddisfare il criterio di indipendenza sancito nella summenzionata disposizione della direttiva 95/46, 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 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 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 (punto 58).

Sentenza dell'8 aprile 2014 (Grande Sezione), Commissione/Ungheria (C-288/12, EU:C:2014:237) [79]

In tale causa la Commissione aveva chiesto alla Corte 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.

La Corte ha dichiarato che viene meno agli obblighi ad esso incombenti in forza della direttiva 95/46 uno Stato membro che ponga anticipatamente fine al mandato dell'autorità di controllo per la protezione dei dati personali (punto 62 e 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 possano 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 l'indipendenza funzionale non è sufficiente, di per sé, a preservare le autorità di controllo da qualsiasi influenza esterna, il solo rischio che le autorità di vigilanza 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 porre fine al mandato di un'autorità di

[79] Detta sentenza è stata presentata nella Relazione annuale 2014, pag. 62.

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 di 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 da 52 a 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) [80]

La Nemzeti Adatvédelmi és Információszabadság Hatóság (autorità nazionale incaricata della protezione dei dati e della libertà dell'informazione, Ungheria) aveva inflitto 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.

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. Conseguentemente, essa ha sottoposto alla Corte di giustizia varie questioni pregiudiziali.

Riguardo al diritto nazionale applicabile, la Corte ha dichiarato che l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 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 e disp. 1).

[80] Detta sentenza è stata presentata nella Relazione annuale 2015, pag. 55.

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, la Corte ha considerato che tale autorità può esaminare tale reclamo indipendentemente 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, essa 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 e 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 IV, intitolata «Trasferimento di dati personali verso paesi terzi»), la Corte 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 constatato 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, 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 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, 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 e 47).

Sentenza del 5 giugno 2018 (Grande Sezione), Wirtschaftsakademie Schleswig-Holstein (C-210/16, ECLI:EU:C:2018:388)

In tale sentenza (v. altresì la rubrica II.5., intitolata «Nozione di "responsabile del trattamento dei dati personali"») vertente, tra l'altro, sull'interpretazione degli articoli 4 e 28 della direttiva 95/46, la Corte si è pronunciata sulla portata dei poteri di intervento di cui dispongono le autorità di controllo riguardo al trattamento di dati personali che implica la partecipazione di più attori.

In tal senso, la Corte ha dichiarato che, qualora un'impresa stabilita al di fuori dell'Unione europea (come la società statunitense Facebook) disponga di varie filiali in diversi Stati membri, l'autorità di controllo di uno Stato membro è autorizzata a esercitare i poteri che le conferisce l'articolo 28, paragrafo 3, di tale direttiva nei confronti di una filiale di detta impresa situata nel territorio di tale Stato membro (nel caso di specie, la Facebook Germany), anche se, in base alla ripartizione delle funzioni all'interno del gruppo, da un lato, tale filiale è competente solamente per la vendita di spazi pubblicitari e per altre attività di marketing sul territorio di detto Stato membro e, dall'altro, la responsabilità esclusiva per la raccolta e per il trattamento dei dati personali grava, per l'intero territorio dell'Unione europea, su una filiale situata in un altro Stato membro (nel caso di specie, la Facebook Ireland) (punto 64 e disp. 2).

Inoltre, la Corte ha precisato che qualora l'autorità di controllo di uno Stato membro intenda esercitare, nei confronti di un organismo stabilito sul territorio di tale Stato membro, i poteri d'intervento di cui all'articolo 28, paragrafo 3, della direttiva 95/46 a motivo di violazioni delle disposizioni relative alla protezione dei dati personali, commesse da un terzo responsabile del trattamento di tali dati che ha la propria sede in un altro Stato membro (nel caso di specie, la Facebook Ireland), tale autorità di controllo è competente a valutare, in modo autonomo rispetto all'autorità di controllo di quest'ultimo Stato membro (Irlanda), la liceità di un siffatto trattamento di dati e può esercitare i suoi poteri d'intervento nei confronti dell'organismo stabilito sul proprio territorio senza previamente richiedere l'intervento dell'autorità di controllo dell'altro Stato membro (punto 74 e disp. 3).

Sentenza del 15 giugno 2021 (Grande Sezione), Facebook Ireland e a. (C-645/19, EU:C:2021:483)

L'11 settembre 2015 il presidente della Commissione belga per la tutela della vita privata (in prosieguo: la «CPVP») ha intentato un'azione inibitoria nei confronti delle società Facebook Ireland, Facebook Inc. e Facebook Belgium dinanzi al Nederlandstalige rechtbank van eerste aanleg Brussel (Tribunale di primo grado di Bruxelles di lingua neerlandese, Belgio) volta a porre fine a violazioni, asseritamente commesse da Facebook, della normativa relativa alla protezione dei dati. Tali violazioni consistevano segnatamente nella raccolta e nell'uso di informazioni sul comportamento di navigazione degli internauti belgi, detentori o meno di un account Facebook, mediante varie tecnologie, quali i cookie, i social plugin [81] o i pixel.

Il 16 febbraio 2018 detto tribunale si è dichiarato competente a statuire su tale azione e, nel merito, ha dichiarato che il social network Facebook non aveva sufficientemente informato gli internauti belgi relativamente alla raccolta e all'uso delle informazioni di cui trattasi. Peraltro, non

[81] Ad esempio, i pulsanti «Mi piace» o «Condividi».

è stato ritenuto valido il consenso prestato dagli internauti alla raccolta e al trattamento di dette informazioni.

Il 2 marzo 2018 Facebook Ireland, Facebook Inc. e Facebook Belgium hanno interposto appello avverso tale sentenza dinanzi allo Hof van beroep te Brussel (Corte d'appello di Bruxelles, Belgio), giudice del rinvio nella presente causa. Dinanzi a tale giudice, l'Autorità belga per la protezione dei dati (in prosieguo: l'«APD») ha agito in qualità di successore legale del presidente della CPVP. Il giudice del rinvio si è dichiarato competente a statuire unicamente sull'appello interposto da Facebook Belgium.

Il giudice del rinvio ha nutrito dubbi in merito all'incidenza dell'applicazione del meccanismo dello «sportello unico» previsto dal RGPD [82] sulle competenze dell'APD e si è posto, più in particolare, la questione se, per i fatti successivi all'entrata in vigore del RGPD, ossia il 25 maggio 2018, l'APD possa agire nei confronti di Facebook Belgium, dal momento che è Facebook Ireland ad essere stata individuata come titolare del trattamento dei dati interessati. Infatti, a partire da tale data e segnatamente in applicazione del principio dello «sportello unico» previsto dal RGPD, solo il Commissario irlandese per la protezione dei dati sarebbe competente ad intentare un'azione inibitoria, sotto il controllo dei giudici irlandesi (punti 36 e 37).

Nella sua sentenza, pronunciata in Grande Sezione, la Corte precisa i poteri delle autorità nazionali di controllo nell'ambito del RGPD. In tal senso, essa dichiara in particolare che, in presenza di determinate condizioni, detto regolamento autorizza un'autorità di controllo di uno Stato membro ad esercitare il suo potere di intentare un'azione dinanzi ad un giudice di tale Stato e di agire in sede giudiziale in caso di presunta violazione del RGPD, con riguardo ad un trattamento transfrontaliero di dati [83], pur non essendo l'autorità di controllo capofila per tale trattamento (disp. 1).

In primo luogo, la Corte precisa le condizioni in presenza delle quali un'autorità nazionale di controllo, priva della qualità di autorità capofila con riguardo a un trattamento transfrontaliero, deve esercitare il proprio potere di intentare un'azione dinanzi ad un giudice di uno Stato membro e, se del caso, di agire in sede giudiziale in caso di presunta violazione del RGPD al fine di garantire il rispetto di tale regolamento. Pertanto, da un lato, il RGPD deve conferire a tale autorità di controllo la competenza ad adottare una decisione che accerti che tale trattamento viola le norme previste dal regolamento in parola e, dall'altro, tale potere deve essere esercitato nel rispetto delle procedure di cooperazione e di coerenza previste da tale regolamento [84] (punto 75 e disp. 1).

Infatti, per i trattamenti transfrontalieri, il RGPD prevede il meccanismo dello «sportello unico» [85], basato su una ripartizione delle competenze tra un'«autorità di controllo capofila» e le altre autorità nazionali di controllo interessate. Tale meccanismo richiede una cooperazione stretta, leale ed efficace tra dette autorità, al fine di garantire una protezione coerente ed omogenea

---

82 Ai sensi dell'articolo 56, paragrafo 1, del RGPD: «Fatto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento».

83 Ai sensi dell'articolo 4, punto 23, del RGPD.

84 Previste agli articoli 56 e 60 del RGPD.

85 Articolo 56, paragrafo 1, del RGPD.

delle norme relative alla protezione dei dati personali e di preservare così il suo effetto utile. Il RGPD stabilisce a tal riguardo la competenza di principio dell'autorità di controllo capofila ad adottare una decisione che accerti che un trattamento transfrontaliero viola le norme previste da detto regolamento [86], mentre la competenza delle altre autorità nazionali di controllo ad adottare una siffatta decisione, anche in via provvisoria, costituisce l'eccezione [87]. Tuttavia, nell'esercizio delle sue competenze, l'autorità di controllo capofila non può sottrarsi a un dialogo indispensabile nonché a una cooperazione leale ed efficace con le altre autorità di controllo interessate. Di conseguenza, nell'ambito di detta cooperazione, l'autorità di controllo capofila non può ignorare le opinioni delle altre autorità di controllo interessate e qualsiasi obiezione pertinente e motivata formulata da una di queste ultime autorità ha l'effetto di bloccare, almeno temporaneamente, l'adozione del progetto di decisione dell'autorità di controllo capofila (punti da 50 a 53, da 56 a 59 e da 63 a 65).

La Corte precisa inoltre che la circostanza che un'autorità di controllo di uno Stato membro, che non sia l'autorità di controllo capofila con riguardo ad un trattamento transfrontaliero di dati, possa esercitare il potere di intentare un'azione dinanzi ad un giudice di tale Stato e di agire in sede giudiziale in caso di presunta violazione del RGPD solo nel rispetto delle norme di ripartizione delle competenze decisionali tra l'autorità di controllo capofila e le altre autorità di controllo [88] è conforme agli articoli 7, 8 e 47 della Carta, che garantiscono all'interessato, rispettivamente, il diritto alla protezione dei dati personali e il diritto ad un ricorso effettivo (punto 67).

In secondo luogo, la Corte dichiara che, in caso di trattamento transfrontaliero di dati, l'esercizio del potere di un'autorità di controllo di uno Stato membro, diversa dall'autorità di controllo capofila, di intentare un'azione giudiziaria [89] non richiede che il titolare del trattamento o il responsabile del trattamento transfrontaliero di dati personali oggetto di tale azione disponga di uno stabilimento principale o di un altro stabilimento nel territorio di tale Stato membro. Tuttavia, l'esercizio di tale potere deve rientrare nell'ambito di applicazione territoriale del RGPD [90], il che presuppone che il titolare del trattamento o il responsabile del trattamento transfrontaliero disponga di uno stabilimento nel territorio dell'Unione (punti 80, 83, 84 e disp. 2).

In terzo luogo, la Corte dichiara che, in caso di trattamento transfrontaliero di dati, il potere di un'autorità di controllo di uno Stato membro, diversa dall'autorità di controllo capofila, di intentare un'azione dinanzi ad un giudice di tale Stato e, se del caso, di agire in sede giudiziale in caso di presunta violazione del RGPD, può essere esercitato tanto nei confronti dello stabilimento principale del titolare del trattamento che si trovi nello Stato membro di appartenenza di tale autorità quanto nei confronti di un altro stabilimento di tale titolare, purché

86 Articolo 60, paragrafo 7, del RGPD.

87 L'articolo 56, paragrafo 2, e l'articolo 66 del RGPD stabiliscono le eccezioni al principio della competenza decisionale dell'autorità di controllo capofila.

88 Previste agli articoli 55 e 56, letti in combinato disposto con l'articolo 60 del RGPD.

89 In forza dell'articolo 58, paragrafo 5, del RGPD.

90 L'articolo 3, paragrafo 1, del RGPD prevede che detto regolamento si applichi al trattamento dei dati personali effettuato «nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione».

l'azione giudiziaria riguardi un trattamento di dati effettuato nell'ambito delle attività di detto stabilimento e l'autorità di cui trattasi sia competente ad esercitare siffatto potere.

Tuttavia, la Corte precisa che l'esercizio di tale potere presuppone che il RGPD sia applicabile. Nel caso di specie, poiché le attività dello stabilimento del gruppo Facebook situato in Belgio sono inscindibilmente connesse al trattamento dei dati personali di cui trattasi nel procedimento principale, per il quale il titolare del trattamento è Facebook Ireland per quanto riguarda il territorio dell'Unione, tale trattamento è effettuato «nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento», e, pertanto, rientra effettivamente nell'ambito di applicazione del RGPD (punti da 94 a 96 e disp. 3).

In quarto luogo, la Corte dichiara che, qualora un'autorità di controllo di uno Stato membro che non sia l'«autorità di controllo capofila» abbia intentato, prima della data di entrata in vigore del RGPD, un'azione giudiziaria riguardante un trattamento transfrontaliero di dati personali, tale azione può essere mantenuta, in forza del diritto dell'Unione, in base alle disposizioni della direttiva 95/46, la quale rimane applicabile per quanto riguarda le violazioni delle norme in essa contenute fino alla data di abrogazione di tale direttiva. Inoltre, siffatta azione può essere intentata da tale autorità per violazioni commesse dopo la data di entrata in vigore del RGPD, purché ciò avvenga in una delle situazioni in cui, a titolo di eccezione, tale regolamento conferisce alla stessa autorità una competenza ad adottare una decisione che accerti che il trattamento di dati di cui trattasi viola le norme contenute in detto regolamento e nel rispetto delle procedure di cooperazione e di coerenza previste da quest'ultimo (punto 105 e disp. 4).

In quinto e ultimo luogo, la Corte riconosce l'effetto diretto della disposizione del RGPD in forza della quale ciascuno Stato membro dispone, per legge, che la sua autorità di controllo abbia il potere di intentare un'azione e, se del caso, di agire in sede giudiziale in caso di violazione del predetto regolamento. Di conseguenza, siffatta autorità può invocare tale disposizione per intentare o proseguire un'azione nei confronti di privati, anche qualora essa non sia stata specificamente attuata nella normativa dello Stato membro interessato (punto 113 e disp. 5).

VII. Applicazione territoriale della legislazione 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 V.1., intitolata «Diritto di opposizione al trattamento dei dati personali ("diritto all'oblio")»], la Corte si è, altresì, pronunciata sull'ambito di applicazione territoriale della direttiva 95/46.

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, 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 e 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, seppur 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).

VIII. Diritto di accesso del pubblico ai documenti delle istituzioni dell'Unione europea e protezione 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, invocando in particolare la tutela della vita privata di tali persone, come garantita dal regolamento n. 45/2001.

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 n. 1049/2001 [91], relativo all'accesso ai documenti, sia diretta a ottenere l'accesso a documenti che contengono dati personali, le disposizioni del regolamento 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).

Inoltre, 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 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 avevano 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 n. 1049/2001, non è fornita alcuna motivazione espressa e legittima né è fornito 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 possa arrecare pregiudizio agli interessi legittimi delle persone coinvolte, come richiesto dall'articolo 8, lettera b), del regolamento n. 45/2001 (punto 78) [92].

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 [93], 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

[91] 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 2001, L 145, pag. 43).

[92] Detta sentenza è stata presentata nella Relazione annuale 2010, pag. 14.

[93] 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 del Consiglio 79/117/CEE e 91/414/CEE (GU 2009, L 309, pag. 1).

proposito. In tale contesto, esse avevano presentato congiuntamente all'EFSA una domanda di accesso a vari documenti relativi alla preparazione del progetto di orientamento, comprese 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. La stessa ha tuttavia affermato di aver occultato i nomi di tali esperti, in conformità all'articolo 4, paragrafo 1, lettera b), del regolamento n. 1049/2001 nonché della normativa dell'Unione in materia di tutela dei dati personali, segnatamente il regolamento 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 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 presentato un'impugnazione avverso la sentenza [94] del Tribunale dinanzi alla Corte di giustizia.

In primo luogo, la Corte ha rilevato che, atteso che l'informazione richiesta avrebbe consentito 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 n. 45/2001. Dal momento che le nozioni di «dati personali», di cui all'articolo 2, lettera a), del regolamento 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 e 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 da 57 a 59).

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

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

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 e 73).

* * *

Le sentenze contenute nella presente scheda sono classificate nel Repertorio della giurisprudenza sotto le rubriche 1.04.03.07, 1.04.03.08, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07., 4.11.11.01.