CORTE DI GIUSTIZIA
DELL'UNIONE EUROPEA

IT

Scheda tematica
Protezione dei dati personali

Premessa

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 dal diritto primario, segnatamente dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta») e dall'articolo 16, paragrafo 1, del Trattato sul funzionamento dell'Unione europea (TFUE). Tale diritto fondamentale è inoltre strettamente connesso al diritto al rispetto della vita privata e della vita familiare sancito all'articolo 7 della Carta.

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], abrogata dal 2018, costituiva in proposito il principale atto giuridico dell'Unione in materia.

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, per tener conto delle nuove evoluzioni tecnologiche e commerciali, il legislatore dell'Unione ha avviato, a partire dal 2017, un riesame di tale direttiva [4], che è, ad oggi, ancora in corso [5].

Nel 2016 l'Unione europea ha riformato il contesto normativo globale in materia. A tal fine, ha adottato il regolamento (UE) 2016/679 [6] relativo alla protezione dei dati

---

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 2003, abrogata a decorrere dal 25 maggio 2018 (v. nota 6).

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 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.

5 Il 10 febbraio 2021 il Consiglio dell'Unione europea ha approvato un mandato negoziale ai fini della revisione delle norme in materia di tutela della vita privata e della riservatezza nell'uso dei servizi di comunicazione elettronica che consente di avviare i negoziati con il Parlamento europeo. Il testo della proposta di regolamento 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) è disponibile al seguente indirizzo: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN*.

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)

personali (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, le cui disposizioni sono applicabili dal 6 maggio 2018.

Per quanto riguarda il trattamento dei dati personali da parte delle istituzioni e degli organi dell'UE, la loro protezione è garantita, segnatamente, dall'11 dicembre 2018, dal regolamento (UE) 2018/1725 [8]. Nell'interesse di un approccio coerente alla protezione dei dati personali in tutta l'Unione, tale regolamento mira ad allineare, per quanto possibile, le norme in materia al regime istituito dal RGPD.

Infine, per affrontare le sfide poste dalle nuove tecnologie, il legislatore dell'Unione ha avviato, a partire dal 2020, l'adozione di nuove misure legislative [9] che vanno ad aggiungersi alle disposizioni del diritto dell'Unione in materia di protezione dei dati personali.

Tenuto conto della ricca giurisprudenza della Corte di giustizia in materia di protezione dei dati personali, la presente scheda tematica mira a presentare una selezione di sentenze fondamentali in materia e di sentenze che hanno avuto un impatto importante sullo sviluppo di detta giurisprudenza, con un'attenzione particolare alle pronunce della Grande Sezione della Corte. Più in particolare, questa scheda intende comprendere sia la giurisprudenza relativa alla normativa generale in materia di protezione dei dati personali, frutto dell'interpretazione della direttiva 95/46 e del RGPD, sia quella vertente sulla normativa settoriale riguardante, segnatamente, l'ambito delle comunicazioni elettroniche e il diritto penale. Essa intende, inoltre, presentare una selezione di sentenze vertenti su normative di applicazione trasversale, mettendo in risalto anzitutto il ruolo determinante della Carta nello sviluppo della giurisprudenza.

---

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 (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 (GU 2018, L 295, pag. 39).

9 In tale contesto, vanno menzionate segnatamente tre iniziative legislative: *i)* il regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (regolamento sulla governance dei dati) (GU 2022, L 152, pag. 1) e il regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati) (GU 2023, L 2854, pag. 1); *ii)* un pacchetto legislativo sui servizi e i mercati digitali, composto dal regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) (GU 2022, L 277, pag. 1) e dal regolamento 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali) (GU 2022, L 265, pag. 1), e *iii)* la prima proposta legislativa in assoluto volta alla creazione di un quadro normativo in materia di intelligenza artificiale, che si è concretizzata in un regolamento sull'intelligenza artificiale (GU 2024, L, 1689).

Indice

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*)

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 [10] e 259/2008 [11], 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.

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,

[10] 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).

[11] Regolamento (CE) n. 259/2008 della Commissione, del 18 marzo 2008, recante modalità di applicazione del regolamento (CE) n. 1290/2005 del Consiglio per quanto riguarda la pubblicazione di informazioni sui beneficiari dei finanziamenti provenienti dal FEAGA e dal FEASR (GU 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).

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. In tale contesto, la Corte ha considerato che, sebbene in una 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.

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. 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.

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)

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, 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.

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. 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. 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. 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.

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.

Sentenza del 21 giugno 2022 (Grande Sezione), Ligue des droits humains (C-817/19, EU:C:2022:491)

I dati PNR (Passenger Name Record) sono informazioni di prenotazione archiviate dai vettori aerei nei loro sistemi di prenotazione e di controllo delle partenze. La direttiva PNR [12] obbliga tali vettori a trasferire i dati di tutti i passeggeri che si imbarcano su un volo extra-UE, operato tra un paese terzo e l'Unione europea, all'unità d'informazione sui passeggeri (in prosieguo: l'«UIP») dello Stato membro di destinazione o di partenza del volo in questione, al fine di lottare contro il terrorismo e i reati gravi. Infatti, i dati PNR così trasferiti sono oggetto di una valutazione preliminare da parte dell'UIP [13] e sono poi conservati ai fini di un'eventuale valutazione successiva da parte delle autorità competenti dello Stato membro interessato o di quelle di un altro Stato membro. Gli Stati membri possono decidere di applicare la direttiva anche a voli intra-UE [14]
.

La Cour constitutionnelle (Corte costituzionale, Belgio) è stata investita dalla Ligue des droits humains di un ricorso di annullamento avverso la legge belga che traspone nel diritto nazionale sia la direttiva PNR sia la direttiva API [15]. Secondo la ricorrente, tale legge viola il diritto al rispetto della vita privata e alla protezione dei dati personali. Essa contesta, da un lato, l'ampiezza dei dati PNR e, dall'altro, il carattere generale della raccolta, del trasferimento e del trattamento di tali dati. La legge pregiudicherebbe anche la libera circolazione delle persone in quanto reintrodurrebbe indirettamente controlli alle frontiere, estendendo il sistema PNR ai voli intra-UE e a trasporti effettuati con altri mezzi all'interno dell'Unione.

---

12 Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi (GU 2016, L 119, pag. 132; in prosieguo: la «direttiva PNR»).

13 Tale valutazione preliminare mira a identificare i passeggeri da sottoporre a ulteriore verifica da parte delle autorità competenti, in considerazione del fatto che gli stessi potrebbero essere implicati in reati di terrorismo o in reati gravi. Essa è effettuata in maniera sistematica e con mezzi automatizzati, confrontando i dati PNR con banche dati «pertinenti» o trattandoli sulla base di criteri prestabiliti di cui all'articolo 6, paragrafo 2, lettera a), e paragrafo 3, della direttiva PNR.

14 Utilizzando la possibilità prevista dall'articolo 2 della direttiva PNR.

15 Direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate (GU 2004, L 261, pag. 24) (in prosieguo: la «direttiva API»). Tale direttiva disciplina la trasmissione, da parte dei vettori aerei, d'informazioni

In tale contesto, la Cour constitutionnelle (Corte costituzionale) belga ha adito la Corte in via pregiudiziale sottoponendole questioni vertenti, in particolare, sulla validità della direttiva PNR.

Con la sua sentenza, pronunciata in Grande Sezione, la Corte conferma la validità della direttiva PNR nei limiti in cui quest'ultima può essere interpretata conformemente alla Carta.

A questo proposito, la Corte giudica che, dal momento che l'interpretazione fornita dalla Corte delle disposizioni della direttiva PNR alla luce dei diritti fondamentali garantiti dagli articoli 7, 8 e 21 nonché dall'articolo 52, paragrafo 1, della Carta [16] garantisce la conformità di tale direttiva con tali articoli, l'esame delle questioni poste non ha rivelato alcun elemento tale da inficiare la validità di detta direttiva.

In via preliminare, essa rammenta che un atto dell'Unione deve essere interpretato, per quanto possibile, in un modo che non pregiudichi la sua validità e in conformità con l'insieme del diritto primario e, segnatamente, con le disposizioni della Carta; gli Stati membri devono pertanto fare in modo di non basarsi su un'interpretazione della stessa che entri in conflitto con i diritti fondamentali tutelati dall'ordinamento giuridico dell'Unione o con gli altri principi generali riconosciuti in detto ordinamento giuridico. Per quanto riguarda la direttiva PNR, la Corte precisa che molti considerando e molte disposizioni di quest'ultima richiedono una siffatta interpretazione conforme, ponendo l'accento sull'importanza che il legislatore dell'Unione attribuisce, facendo riferimento a un livello elevato di protezione dei dati, al pieno rispetto dei diritti fondamentali sanciti dalla Carta.

La Corte constata che la direttiva PNR comporta ingerenze di una gravità certa nei diritti garantiti dagli articoli 7 e 8 della Carta, nella misura in cui, in particolare, essa mira a istituire un sistema di sorveglianza continua, indiscriminata e sistematica, che include la valutazione automatizzata di dati personali di tutte le persone che utilizzano servizi di trasporto aereo. Essa rammenta che la possibilità per gli Stati membri di giustificare una siffatta ingerenza deve essere valutata misurandone la gravità e verificando che l'importanza dell'obiettivo di interesse generale perseguito sia adeguata a detta gravità.

La Corte conclude che il trasferimento, il trattamento e la conservazione dei dati PNR previsti da tale direttiva possono essere considerati come limitati allo stretto necessario ai fini della lotta contro i reati di terrorismo e i reati gravi, a condizione che i poteri previsti da detta direttiva siano oggetto di un'interpretazione restrittiva. A tal riguardo, la sentenza pronunciata in data odierna precisa, segnatamente, che:

- Il sistema istituito dalla direttiva PNR deve includere solo le informazioni chiaramente identificabili e circoscritte nelle rubriche contenute nell'allegato I di

anticipate sui passeggeri (quali il numero e il tipo di documento di viaggio utilizzato nonché la cittadinanza) alle competenti autorità nazionali al fine di migliorare i controlli alle frontiere e combattere l'immigrazione irregolare.

[16] Ai sensi di tale disposizione, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Inoltre, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

quest'ultima, le quali sono connesse al volo effettuato e al passeggero interessato, il che implica, per talune rubriche contenute in tale allegato, che sono comprese soltanto le informazioni espressamente contemplate [17].

- L'applicazione del sistema istituito dalla direttiva PNR deve essere limitata ai reati di terrorismo e ai soli reati gravi che presentino un collegamento oggettivo, quantomeno indiretto, con il trasporto aereo di passeggeri. Per quanto attiene a detti reati gravi, l'applicazione di tale sistema non può essere estesa a reati che, sebbene soddisfino il criterio previsto da questa direttiva, relativo alla soglia di gravità, e siano in particolare contemplati nell'allegato II a quest'ultima, rientrano nei reati comuni tenuto conto delle specificità del sistema penale nazionale.
- L'eventuale estensione dell'applicazione della direttiva PNR a tutti i voli intra-UE o a una parte di essi, che può essere decisa da uno Stato membro avvalendosi della facoltà prevista da tale direttiva, deve essere limitata allo stretto necessario. A tal fine, essa deve poter essere oggetto di un controllo effettivo da parte di un organo giurisdizionale o di un organo amministrativo indipendente, la cui decisione sia dotata di effetto vincolante. A tal riguardo, la Corte precisa che:
  - Nel solo caso in cui detto Stato membro accerti l'esistenza di circostanze sufficientemente concrete per ritenere che sia confrontato a una minaccia terroristica che si riveli reale e attuale o prevedibile, l'applicazione di tale direttiva a tutti i voli intra-UE provenienti da o diretti verso detto Stato membro, per una durata limitata allo stretto necessario, ma rinnovabile, non deve eccedere i limiti dello stretto necessario [18].
  - In assenza di una siffatta minaccia terroristica, l'applicazione di detta direttiva non può estendersi a tutti i voli intra-UE, ma deve essere limitata ai voli intra-UE relativi, in particolare, a determinati collegamenti o modalità di viaggio o ancora a determinati aeroporti per i quali esistano, secondo la valutazione dello Stato membro interessato, indicazioni che giustifichino tale applicazione. Il carattere strettamente necessario di tale applicazione ai voli intra-UE così selezionati deve essere periodicamente rivisto, in funzione dell'evoluzione delle condizioni che ne hanno giustificato la selezione.
- Ai fini della valutazione preliminare dei dati PNR, che ha lo scopo d'identificare i passeggeri da sottoporre a ulteriore verifica prima del loro arrivo o della loro partenza e che è, in una prima fase, effettuata mediante trattamenti automatizzati, l'UIP non può, da un lato, confrontare tali dati alle sole banche dati

[17] Così, in particolare, le «informazioni sulle modalità di pagamento» (rubrica 6 dell'allegato) devono essere limitate alle modalità di pagamento e alla fatturazione del biglietto aereo, ad esclusione di qualsiasi altra informazione priva di rapporto diretto con il volo, e le «osservazioni generali» (rubrica 12) possono riguardare solo i dati espressamente elencati in tale rubrica, relativi ai passeggeri minorenni.

[18] Infatti, l'esistenza di una siffatta minaccia è idonea, di per se stessa, a stabilire una relazione tra il trasferimento e il trattamento dei dati interessati e la lotta contro il terrorismo. Pertanto, prevedere l'applicazione della direttiva PNR a tutti i voli intra-UE provenienti da o diretti verso lo Stato membro interessato, per una durata limitata, non eccede i limiti dello stretto necessario, poiché la decisione che prevede tale applicazione deve poter essere oggetto di un controllo da parte di un tribunale o di un organo amministrativo indipendente.

riguardanti persone o oggetti ricercati o segnalati [19]. Tali banche dati devono essere non discriminatorie e utilizzate, dalle autorità competenti, in relazione alla lotta contro reati di terrorismo e reati gravi che abbiano un collegamento oggettivo, quantomeno indiretto, con il trasporto aereo dei passeggeri. Per quanto riguarda, dall'altro lato, la valutazione preliminare sulla base dei criteri prestabiliti, l'UIP non può utilizzare tecnologie di intelligenza artificiale nell'ambito di sistemi di autoapprendimento (machine learning), che possono modificare, senza intervento e controllo umani, il processo di valutazione e, in particolare, i criteri di valutazione sui quali si fonda il risultato dell'applicazione di detto processo nonché la ponderazione di tali criteri. Detti criteri devono essere determinati in modo che la loro applicazione prenda di mira, specificamente, gli individui nei confronti dei quali potrebbe gravare un ragionevole sospetto di partecipazione a reati di terrorismo o a reati gravi e in modo da tener conto sia degli elementi «a carico» sia di quelli «a discarico», senza dar luogo a discriminazioni dirette o indirette [20].

- Tenuto conto del tasso di errore inerente a siffatti trattamenti automatizzati dei dati PNR e del numero piuttosto consistente di risultati «erroneamente positivi», che sono stati ottenuti a seguito della loro applicazione nel corso del 2018 e del 2019, l'idoneità del sistema istituito dalla direttiva PNR a raggiungere gli obiettivi perseguiti dipende essenzialmente dal buon funzionamento della verifica dei risultati positivi, ottenuti a titolo di tali trattamenti, che l'UIP effettua, in una seconda fase, con mezzi non automatizzati. A tal riguardo, gli Stati membri devono prevedere norme chiare e precise atte a orientare e a inquadrare l'analisi effettuata dai funzionari dell'UIP incaricati del riesame individuale, al fine di assicurare il pieno rispetto dei diritti fondamentali sanciti dagli articoli 7, 8 e 21 della Carta e, in particolare, al fine di garantire una prassi amministrativa coerente all'interno dell'UIP che rispetti il divieto di discriminazioni. In particolare, essi devono assicurarsi che l'UIP stabilisca criteri di riesame oggettivi che consentano ai suoi funzionari di verificare, da un lato, se e in che misura un riscontro positivo (hit) riguardi effettivamente un individuo che possa trovarsi implicato nei reati di terrorismo o nei reati gravi nonché, dall'altro il carattere non discriminatorio dei trattamenti automatizzati. In tale contesto, la Corte sottolinea inoltre che le autorità competenti devono assicurarsi che l'interessato possa comprendere il funzionamento dei criteri di valutazione prestabiliti e dei programmi che applicano tali criteri in modo che possa decidere, con piena

[19] Vale a dire le banche dati riguardanti persone o oggetti ricercati o segnalati ai sensi dell'articolo 6, paragrafo 3, lettera a), della direttiva PNR. Invece, analisi a partire da banche dati diverse potrebbero assumere la forma di valutazioni approfondite di dati (data mining) e potrebbero dar luogo a un uso sproporzionato di tali dati, fornendo i mezzi per delineare il profilo preciso degli interessati per il solo motivo che essi intendono viaggiare in aereo.

[20] I criteri prestabiliti devono essere mirati, proporzionati e specifici, ed essere periodicamente rivisti (articolo 6, paragrafo 4, della direttiva PNR). La valutazione preliminare secondo criteri prestabiliti deve essere effettuata in modo non discriminatorio. Ai sensi dell'articolo 6, paragrafo 4, quarta frase, della direttiva PNR, i criteri non sono in alcun caso basati sull'origine razziale o etnica, sulle opinioni politiche, sulla religione o sulle convinzioni filosofiche, sull'appartenenza sindacale, sullo stato di salute, sulla vita sessuale o sull'orientamento sessuale dell'interessato.

cognizione di causa, se esercitare o meno il suo diritto a un ricorso giurisdizionale. Parimenti, nell'ambito di un siffatto ricorso, il giudice incaricato del controllo sulla liceità della decisione adottata dalle autorità competenti nonché, al di fuori dei casi di minacce per la sicurezza dello Stato, l'interessato stesso devono poter conoscere tanto l'insieme dei motivi quanto gli elementi di prova sulla base dei quali è stata adottata tale decisione ivi compresi criteri di valutazione prestabiliti e il funzionamento dei programmi che applicano tali criteri.

- La comunicazione e la valutazione successive dei dati PNR, ossia dopo l'arrivo o la partenza dell'interessato, possono essere effettuate solo sulla base di nuove circostanze e di elementi oggettivi che o siano tali da fondare un sospetto ragionevole di implicazione di tale persona in reati gravi che hanno un collegamento oggettivo, quantomeno indiretto, con il trasporto aereo di passeggeri, oppure permettano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro reati di terrorismo che presentano un siffatto collegamento. La comunicazione dei dati PNR ai fini di una siffatta valutazione successiva deve, in linea di principio, salvo in casi di urgenza debitamente giustificata, essere subordinata a un controllo preventivo effettuato o da un giudice o da un'autorità amministrativa indipendente, su richiesta motivata delle autorità competenti, e ciò indipendentemente dalla questione se tale richiesta sia presentata prima o dopo la scadenza del termine di sei mesi successivo al trasferimento di tali dati all'UIP [21].

Sentenza del 22 novembre 2022 (Grande Sezione), Luxembourg Business Registers (C-37/20 e C-601/20, EU:C:2022:912)

Ai fini della lotta e della prevenzione contro il riciclaggio e il finanziamento del terrorismo, la direttiva antiriciclaggio [22] impone agli Stati membri di tenere un registro contenente informazioni sulla titolarità effettiva [23] di società e altre entità giuridiche costituite nel loro territorio. A seguito di una modifica di tale direttiva da parte della direttiva 2018/843 [24], alcune di tali informazioni devono essere rese accessibili in ogni caso al pubblico. Conformemente alla direttiva antiriciclaggio così modificata (in prosieguo: la «direttiva antiriciclaggio modificata»), la legge lussemburghese ha istituito un Registro dei titolari effettivi (in prosieguo: l'«RBE»), destinato a conservare e a mettere

[21] Ai sensi dell'articolo 12, paragrafi 1 e 3, della direttiva PNR, un siffatto controllo è espressamente previsto solo per le richieste di comunicazione dei dati PNR presentate dopo il termine di sei mesi successivi al trasferimento di tali dati all'UIP.

[22] Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione (GU 2015, L 141, pag. 73; in prosieguo: la «direttiva antiriciclaggio»).

[23] Ai sensi dell'articolo 3, punto 6, della direttiva antiriciclaggio, i titolari effettivi sono la persona o le persone fisiche che, in ultima istanza, possiedono o controllano il cliente e/o le persone fisiche per conto delle quali è realizzata un'operazione o un'attività.

[24] Direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio, del 30 maggio 2018, che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE (GU 2018, L 156, pag. 43).

a disposizione una serie di informazioni sui titolari effettivi delle entità registrate che sono accessibili a chiunque.

In tale contesto, il tribunal d'arrondissement de Luxembourg (Tribunale circoscrizionale di Lussemburgo, Lussemburgo) è stato investito di due cause, introdotte, rispettivamente, da WM e dalla Sovim SA, i quali contestano il rigetto, da parte del Luxembourg Business Registers, gestore dell'RBE, delle loro domande dirette ad impedire l'accesso del pubblico alle informazioni relative, nella prima causa, a WM in qualità di titolare effettivo di una société civile immobilière (società di gestione di patrimoni immobiliari) e, nella seconda, al titolare effettivo della Sovim SA. Nell'ambito di tali due cause, nutrendo dubbi in merito alla validità di talune disposizioni del diritto dell'Unione che istituiscono il sistema di accesso pubblico alle informazioni sulla titolarità effettiva, il tribunal d'arrondissement de Luxembourg (Tribunale circoscrizionale di Lussemburgo) ha sottoposto alla Corte una questione pregiudiziale per esame di validità.

Con la sua sentenza, la Corte, riunita in Grande Sezione, dichiara invalida la direttiva 2018/843 in quanto essa ha modificato la direttiva antiriciclaggio nel senso che gli Stati membri provvedono affinché le informazioni sulla titolarità effettiva delle società e delle altre entità giuridiche costituite nel loro territorio siano accessibili in ogni caso al pubblico [25].

Sotto un primo profilo, la Corte constata che l'accesso del pubblico alle informazioni sulla titolarità effettiva, previsto dalla direttiva antiriciclaggio modificata, costituisce una grave ingerenza nei diritti fondamentali al rispetto della vita privata e alla tutela dei dati personali, rispettivamente sanciti agli articoli 7 e 8 della Carta.

A tal riguardo, la Corte osserva che, dal momento che i dati in questione contengono informazioni su persone fisiche identificate, ossia i titolari effettivi delle società e delle altre entità giuridiche costituite nel territorio degli Stati membri, l'accesso del pubblico a queste ultime incide sul diritto fondamentale al rispetto della vita privata. Inoltre, metterli a disposizione del pubblico costituisce un trattamento di dati personali. Essa aggiunge che una simile messa a disposizione del pubblico costituisce un'ingerenza nei due citati diritti fondamentali, indipendentemente dall'uso successivo delle informazioni comunicate.

Per quanto riguarda la gravità di tale ingerenza, la Corte rileva che le informazioni messe a disposizione del pubblico, nella misura in cui si riferiscono all'identità del titolare effettivo nonché alla natura e all'entità dell'interesse beneficiario detenuto in società o in altre entità giuridiche, sono tali da permettere di delineare un profilo riguardante taluni dati d'identificazione personale, lo stato patrimoniale dell'interessato nonché i settori economici, i paesi e le imprese in cui quest'ultimo ha investito. Inoltre, tali informazioni

[25] Invalidità dell'articolo 1, punto 15, lettera c), della direttiva 2018/843, che modifica l'articolo 30, paragrafo 5, primo comma, lettera c), della direttiva antiriciclaggio.

diventano accessibili ad un numero potenzialmente illimitato di persone, cosicché un simile trattamento di dati personali può consentire anche a persone che, per ragioni estranee all'obiettivo perseguito da detta misura, cerchino di ottenere informazioni, in particolare, sulla situazione materiale e finanziaria del titolare effettivo, di accedere liberamente a dette informazioni. Tale possibilità risulta ancor più agevole quando i dati in questione possono essere consultati su Internet. Inoltre, le potenziali conseguenze per le persone interessate derivanti da un eventuale uso abusivo dei loro dati sono aggravate dalla circostanza che, una volta messi a disposizione del pubblico, tali dati possono non solo essere liberamente consultati, ma altresì essere conservati e diffusi e che per tali persone diventa vieppiù difficile, se non addirittura illusorio, difendersi efficacemente dagli abusi.

Sotto un secondo profilo, in sede di esame della giustificazione dell'ingerenza di cui trattasi, in primo luogo, la Corte osserva che, nel caso di specie, il principio di legalità è rispettato. Infatti, la limitazione dell'esercizio dei menzionati diritti fondamentali derivante dall'accesso del pubblico alle informazioni sulla titolarità effettiva è prevista da un atto legislativo, ossia la direttiva antiriciclaggio modificata. Inoltre, da un lato, tale direttiva precisa che tali informazioni devono essere adeguate, accurate e attuali ed elenca espressamente alcuni dati ai quali il pubblico deve essere autorizzato ad accedere. Dall'altro, essa stabilisce le condizioni alle quali gli Stati membri possono prevedere deroghe a un simile accesso.

In secondo luogo, essa precisa che l'ingerenza di cui trattasi non pregiudica il contenuto essenziale dei diritti fondamentali sanciti agli articoli 7 e 8 della Carta. Se è vero che la direttiva antiriciclaggio modificata non contiene un elenco tassativo dei dati ai quali il pubblico deve essere autorizzato ad accedere e che gli Stati membri sono autorizzati a dare accesso ad informazioni aggiuntive, resta il fatto che solo informazioni adeguate sui titolari effettivi e sull'interesse beneficiario detenuto possono essere ottenute, conservate e, pertanto, potenzialmente rese accessibili al pubblico, ciò che esclude, in particolare, informazioni che non abbiano una relazione adeguata con le finalità della direttiva antiriciclaggio modificata. Orbene, non risulta che la messa a disposizione del pubblico delle informazioni aventi una simile relazione arrecherebbe in qualche modo pregiudizio al contenuto essenziale dei diritti fondamentali in argomento.

In terzo luogo, la Corte sottolinea che, prevedendo l'accesso del pubblico alle informazioni sui titolari effettivi, il legislatore dell'Unione mira a prevenire il riciclaggio di denaro e il finanziamento del terrorismo creando, mediante il rafforzamento della trasparenza, un ambiente meno suscettibile di essere utilizzato a tali fini, il che costituisce un obiettivo di interesse generale che può giustificare ingerenze, anche gravi, nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta.

In quarto luogo, nell'ambito dell'esame del carattere idoneo, necessario e proporzionato dell'ingerenza di cui trattasi, la Corte constata che, certamente, l'accesso del pubblico alle informazioni sulla titolarità effettiva è atto a contribuire alla realizzazione di tale obiettivo.

Tuttavia, esso ritiene che tale ingerenza non possa essere considerata limitata allo stretto necessario. Da un lato, la stretta necessità di detta ingerenza non può essere dimostrata basandosi sul fatto che il criterio del «legittimo interesse» di cui, secondo la direttiva antiriciclaggio, nella sua versione anteriore alla sua modifica ad opera della direttiva 2018/843, doveva disporre qualsiasi persona che intendesse accedere alle informazioni sulla titolarità effettiva, era difficile da attuare e che la sua applicazione poteva dar luogo a decisioni arbitrarie. Infatti, l'eventuale esistenza di difficoltà nel definire con precisione le ipotesi e le condizioni in cui il pubblico può accedere alle informazioni sulla titolarità effettiva non può giustificare il fatto che il legislatore dell'Unione preveda l'accesso del pubblico a tali informazioni.

Dall'altro lato, neppure le spiegazioni contenute nella direttiva 2018/843 possono dimostrare la stretta necessità dell'ingerenza di cui trattasi [26]. Nella misura in cui, secondo tali spiegazioni, l'accesso del pubblico alle informazioni sulla titolarità effettiva mira a consentire un maggiore controllo delle informazioni da parte della società civile, segnatamente la stampa e le organizzazioni della società civile, la Corte rileva che tanto la stampa quanto le organizzazioni della società civile che presentano un collegamento con la prevenzione e la lotta contro il riciclaggio e il finanziamento del terrorismo hanno un legittimo interesse ad accedere alle informazioni di cui è causa. Lo stesso vale per i soggetti che desiderino conoscere l'identità dei titolari effettivi di una società o di un'altra entità giuridica per il fatto che potrebbero effettuare operazioni con queste ultime, o ancora per le istituzioni finanziarie e autorità che si occupano del contrasto dei reati in materia di riciclaggio di denaro o di finanziamento del terrorismo.

Inoltre, l'ingerenza di cui trattasi non presenta neppure un carattere proporzionato. A tal riguardo, la Corte constata che le norme sostanziali che disciplinano tale ingerenza non soddisfano il requisito di chiarezza e di precisione. In effetti, la direttiva antiriciclaggio modificata prevede l'accesso del pubblico «almeno» ai dati ivi previsti e conferisce agli Stati membri la facoltà di garantire l'accesso ad informazioni aggiuntive, comprese, «almeno», la data di nascita o le informazioni di contatto del titolare effettivo interessato. Orbene, utilizzando l'espressione «almeno», tale direttiva autorizza la messa a disposizione del pubblico di dati che non sono sufficientemente definiti né identificabili.

Inoltre, per quanto riguarda la ponderazione della gravità di detta ingerenza e l'importanza dell'obiettivo di interesse generale perseguito, la Corte riconosce che, tenuto conto della sua importanza, tale obiettivo può giustificare ingerenze, anche gravi, nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta.

Nondimeno, da un lato, la lotta contro il riciclaggio e il finanziamento del terrorismo spetta prioritariamente alle autorità pubbliche nonché alle entità, quali gli enti creditizi o gli istituti finanziari, che, in ragione delle loro attività, sono assoggettati ad obblighi

[26] Si fa riferimento alle spiegazioni contenute nel considerando 30 della direttiva 2018/843.

specifici in tale materia. Per tale motivo, la direttiva antiriciclaggio modificata prevede che le informazioni sulla titolarità effettiva debbano essere accessibili, in ogni caso, alle autorità competenti e alle unità di informazione finanziaria, senza alcuna restrizione, nonché ai soggetti obbligati, nell'ambito dell'adeguata verifica della clientela [27].

Dall'altro lato, rispetto al regime anteriore che prevedeva, oltre all'accesso da parte delle autorità competenti e di determinate entità alle informazioni sulla titolarità effettiva, quello da parte di qualunque persona od organizzazione che potesse dimostrare un legittimo interesse, il regime introdotto dalla direttiva 2018/843 rappresenta una lesione considerevolmente più grave dei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta, senza che tale aggravamento possa essere compensato dagli eventuali benefici che potrebbero derivare da quest'ultimo regime rispetto al primo, sotto il profilo della lotta contro il riciclaggio e il finanziamento del terrorismo.

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)

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.

[27] Articolo 30, paragrafo 5, primo comma, lettere a) e b), della direttiva antiriciclaggio modificata.

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 democratica, così come richiede detto articolo 15, paragrafo 1, letto alla luce dei summenzionati articoli della Carta.

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.

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.

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

1. Ambito di applicazione della normativa generale

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 [28], 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 [29] 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.

[28] 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).

[29] 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).

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.

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 riguardava un trattamento di dati personali che ne è escluso. La Corte, di conseguenza, ha annullato la decisione sull'adeguatezza.

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.

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.

In tale sentenza, 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.

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.

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 (Corte regionale di Praga capitale, 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.

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. 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.

Sentenza del 16 gennaio 2024 (Grande Sezione), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

Al fine di esaminare una possibile influenza politica sul Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Ufficio federale per la protezione della Costituzione e la lotta al terrorismo, Austria) [30], il Nationalrat (Consiglio nazionale,

[30] Il 1º dicembre 2021 detto ente è divenuto la «Direktion Staatsschutz und Nachrichtendienst» (Direzione per la sicurezza dello Stato e dei servizi di intelligence, Austria).

Austria) ha istituito una commissione di inchiesta (in prosieguo: la «commissione di inchiesta BVT»). Tale commissione ha ascoltato WK in qualità di testimone. Nonostante la sua richiesta di anonimizzazione, il resoconto della sua audizione nel quale venivano citati per intero il suo nome e cognome è stato pubblicato sul sito Internet del Parlament Österreich (Parlamento austriaco). Sostenendo che una siffatta divulgazione della sua identità era contraria al RGPD e alla normativa austriaca, WK ha presentato un reclamo presso l'Österreichische Datenschutzbehörde (Autorità per la protezione dei dati, Austria) (in prosieguo: la «Datenschutzbehörde»). Con decisione del 18 settembre 2019, la Datenschutzbehörde si è dichiarata incompetente a statuire sul reclamo, spiegando che il principio della separazione dei poteri escludeva che, in quanto organo del potere esecutivo, essa potesse controllare la commissione di inchiesta BVT, che rientra nel potere legislativo.

In seguito alla decisione del Bundesverwaltungsgericht (Tribunale amministrativo federale, Austria), che aveva accolto il ricorso di WK e aveva annullato la decisione della Datenschutzbehörde, quest'ultima ha adito la Corte amministrativa con un ricorso per cassazione («Revision») avverso la decisione del Tribunale amministrativo federale.

In tale contesto, il giudice del rinvio ha interrogato la Corte sulla questione se le attività di una commissione di inchiesta istituita dal Parlamento di uno Stato membro rientrino nell'ambito di applicazione del RGPD e se tale regolamento si applichi qualora tali attività riguardino la salvaguardia della sicurezza nazionale.

In primo luogo, la Corte ricorda che l'articolo 2, paragrafo 2, lettera a), del RGPD, che prevede che tale regolamento non si applichi ai trattamenti di dati personali effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, ha l'unico obiettivo di escludere dal suo ambito di applicazione i trattamenti effettuati dalle autorità statali nel contesto di un'attività diretta a salvaguardare la sicurezza nazionale o ascrivibile alla stessa categoria. Pertanto, il mero fatto che un'attività sia propria dello Stato o di un'autorità pubblica non è sufficiente ad escludere automaticamente l'applicazione del RGPD a una siffatta attività.

Tale interpretazione, che deriva dall'assenza di distinzione in funzione dell'identità dell'autore del trattamento interessato, è confermata dall'articolo 4, punto 7, del RGPD [31].

La Corte precisa che la natura parlamentare della commissione di inchiesta BVT non implica che le attività di quest'ultima siano escluse dall'ambito di applicazione del RGPD. Infatti, l'eccezione prevista all'articolo 2, paragrafo 2, lettera a), di tale regolamento si riferisce soltanto a categorie di attività che, per loro natura, non rientrano nell'ambito di applicazione del diritto dell'Unione e non a categorie di persone. Pertanto, la circostanza che il trattamento di dati personali sia effettuato da una commissione di inchiesta

[31] Quest'ultimo definisce la nozione di «titolare del trattamento» come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento».

istituita dal Parlamento di uno Stato membro nell'esercizio del suo potere di controllo del potere esecutivo non consente, in quanto tale, di dimostrare che tale trattamento sia effettuato nell'ambito di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione.

In secondo luogo, la Corte rileva che, sebbene spetti agli Stati membri definire i loro interessi essenziali in materia di sicurezza e decidere le misure idonee a garantirlo [32], la mera circostanza che una misura nazionale sia stata adottata ai fini della tutela della sicurezza nazionale non può comportare l'inapplicabilità del diritto dell'Unione e dispensare gli Stati membri dal necessario rispetto di tale diritto. Orbene, l'eccezione prevista all'articolo 2, paragrafo 2, lettera a), del RGPD si riferisce soltanto a categorie di attività che, per loro natura, non rientrano nell'ambito di applicazione del diritto dell'Unione. Al riguardo, la circostanza che il titolare del trattamento sia un'autorità pubblica la cui attività principale consiste nel garantire la sicurezza nazionale non può essere sufficiente, in quanto tale, ad escludere dall'ambito di applicazione del RGPD i trattamenti di dati personali che essa effettua nell'ambito delle altre attività da essa svolte.

Nel caso di specie, il controllo politico effettuato dalla commissione di inchiesta BVT non sembra costituire, in quanto tale, un'attività diretta a salvaguardare la sicurezza nazionale o ascrivibile alla stessa categoria. Pertanto, salvo verifica da parte del giudice del rinvio, tale attività non esula dall'ambito di applicazione del RGPD.

Ciò premesso, una commissione di inchiesta parlamentare può avere accesso a dati personali che, per ragioni attinenti alla sicurezza nazionale, devono beneficiare di una protezione particolare. Al riguardo, possono essere stabilite limitazioni, mediante misure legislative, agli obblighi e ai diritti derivanti dal RGPD per salvaguardare, in particolare, la sicurezza nazionale [33]. Potrebbero quindi essere giustificati, su tale fondamento, limitazioni riguardanti la raccolta dei dati personali, l'informazione degli interessati e il loro accesso a tali dati o ancora la divulgazione di questi ultimi, senza il consenso degli interessati, a persone diverse dal titolare del trattamento, purché tali limitazioni rispettino l'essenza dei diritti e delle libertà fondamentali degli interessati e siano una misura necessaria e proporzionata in una società democratica.

La Corte rileva tuttavia che dalle informazioni messe a sua disposizione non risulta che la commissione di inchiesta BVT abbia affermato che la divulgazione dei dati personali della persona interessata era necessaria per la salvaguardia della sicurezza nazionale e fondata su una misura legislativa nazionale prevista a tal fine, circostanza, questa, che spetta al giudice del rinvio, se del caso, verificare.

[32] Ai sensi dell'articolo 4, paragrafo 2, TFUE.
[33] Ai sensi dell'articolo 23 del RGPD.

2. Nozione di «dati personali»

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

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.

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.

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.

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

In quarto luogo, la Corte ha dichiarato che le risposte scritte fornite dal candidato durante un esame professionale e le eventuali annotazioni dell'esaminatore ad esse relative possono 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.

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.

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. 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.

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.1., intitolata «Ambito di applicazione della normativa generale»), la Corte ha 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. 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.

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

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

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 [34], 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 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» [35], per il quale il RGPD prevede una

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

[35] Articolo 10 del RGPD.

protezione maggiore in virtù del carattere particolarmente sensibile dei dati in questione.

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.

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 [36]. 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.

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 [37]. La Corte dichiara infatti che la CSDD, quando effettua detta comunicazione, non può essere considerata una siffatta «autorità competente» [38].

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» [39], 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 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

36 Articolo 2, paragrafo 2, lettera a), del RGPD.
37 Articolo 2, paragrafo 2, lettera d), del RGPD.
38 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).
39 Articolo 10 del RGPD.

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.

Sentenza del 5 dicembre 2023 (Grande Sezione), Nacionalinis visuomenės sveikatos centras (C-683/21,* EU:C:2023:949*)

Nel 2020, al fine di gestire meglio la pandemia di COVID-19, le autorità lituane hanno deciso di organizzare l'acquisizione di un'applicazione informatica mobile. Tale applicazione doveva contribuire a un monitoraggio epidemiologico, consentendo di registrare e di seguire dati delle persone esposte al virus della COVID-19.

A tal fine, il Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (Centro nazionale di sanità pubblica presso il Ministero della Sanità, Lituania; in prosieguo: il «CNSP»), incaricato di tale acquisizione, ha contattato la società UAB «IT sprendimai sėkmei» (in prosieguo: la «società ITSS»), chiedendole di procedere alla creazione di un'applicazione mobile di questo tipo. Successivamente, i dipendenti del CNSP hanno inviato a tale società messaggi di posta elettronica vertenti in particolare sulle questioni che dovevano comparire in tale applicazione.

Nel periodo tra aprile e maggio 2020, l'applicazione creata dalla società ITSS è stata messa a disposizione del pubblico. Di conseguenza, 3 802 persone ne hanno fatto uso e hanno fornito vari dati, richiesti da tale applicazione, che le riguardavano. Tuttavia, per mancanza di finanziamento, il CNSP non ha aggiudicato alla società ITSS nessun appalto pubblico diretto all'acquisizione ufficiale della sua applicazione mobile e ha messo fine alla procedura ad essa relativa.

Nel frattempo, l'autorità nazionale di controllo ha avviato un'inchiesta riguardante il trattamento dei dati personali risultante dall'uso di tale applicazione. Con decisione di tale autorità, adottata in esito all'inchiesta, sono state inflitte sanzioni amministrative pecuniarie tanto al CNSP quanto alla società ITSS considerata contitolare del trattamento.

Il CNSP ha contestato tale decisione dinanzi al Vilniaus apygardos administracinis teismas (Tribunale amministrativo regionale di Vilnius, Lituania). Nutrendo dubbi sull'interpretazione di varie disposizioni del RGPD, tale giudice ha adito la Corte in via pregiudiziale.

Nella sua sentenza la Corte, pronunciandosi in Grande Sezione, apporta precisazioni, tra l'altro, riguardo alla nozione di «trattamento». Essa indica, a tal proposito, che costituisce un trattamento ai sensi del RGPD l'uso di dati personali a fini di test informatici di un'applicazione mobile. Tuttavia, diverso è il caso se tali dati siano stati resi anonimi in modo da impedire o da non consentire più l'identificazione dell'interessato o si tratti di dati fittizi che non si riferiscono a una persona fisica esistente.

Infatti, da un lato, la questione se dati personali sono utilizzati a fini di test informatici o ad altro fine è irrilevante riguardo alla qualificazione dell'operazione di «trattamento». D'altro lato, solo un trattamento che riguardi dati personali può essere qualificato come «trattamento» ai sensi del RGPD. Orbene, i dati fittizi o anonimi non sono dati personali.

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.

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.

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

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.

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 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).

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.

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.

Sentenza del 5 dicembre 2023 (Grande Sezione), Nacionalinis visuomenės sveikatos centras (C-683/21,* EU:C:2023:949*)

In tale causa (v. altresì la rubrica II.3, intitolata «Nozione di "trattamento di dati personali"»), la Corte rileva che può essere considerato titolare del trattamento un ente che ha incaricato un'impresa di sviluppare un'applicazione informatica mobile e che, in tale contesto, ha partecipato alla determinazione delle finalità e dei mezzi del

trattamento dei dati personali effettuato mediante tale applicazione [40]. Tale considerazione non può essere messa in discussione dal fatto che detto ente non ha proceduto, esso stesso, a operazioni di trattamento di tali dati, non ha dato esplicitamente il proprio consenso alla realizzazione delle operazioni concrete di un siffatto trattamento o alla messa a disposizione del pubblico di detta applicazione mobile e non ha acquisito quella stessa applicazione mobile, salvo che, prima di tale messa a disposizione nei confronti del pubblico, il suddetto ente si sia espressamente opposto ad essa e al trattamento dei dati personali che ne è derivato.

6. Nozione di «contitolare del trattamento»

Sentenza del 5 dicembre 2023 (Grande Sezione), Nacionalinis visuomenės sveikatos centras (C-683/21,* EU:C:2023:949*)

In questa sentenza (v. altresì le rubriche II.3 e II.5, intitolate «Nozione di "trattamento di dati personali"» e «Nozione di "responsabile del trattamento di dati personali"»), la Corte osserva che la qualificazione di due enti come contitolari del trattamento non presuppone né l'esistenza di un accordo tra di essi sulla determinazione delle finalità e dei mezzi del trattamento dei dati personali di cui trattasi né l'esistenza di un accordo che fissi le condizioni relative alla contitolarità del trattamento. È vero che, in forza del RGPD [41], i contitolari del trattamento devono, mediante accordo tra loro, definire in modo trasparente i loro rispettivi obblighi al fine di garantire il rispetto dei requisiti di tale regolamento. Tuttavia, l'esistenza di un siffatto accordo costituisce non una condizione previa affinché due o più entità siano qualificate come «contitolari del trattamento», bensì un obbligo che il RGPD impone ai contitolari del trattamento, una volta qualificati come tali, al fine di garantire il rispetto degli obblighi di cui al RGPD gravanti su di essi. Pertanto, tale qualificazione deriva dal solo fatto che molteplici enti hanno partecipato alla determinazione delle finalità e dei mezzi del trattamento.

Quanto alla determinazione congiunta, da parte degli enti interessati, delle finalità e dei mezzi del trattamento, la Corte precisa che la loro partecipazione a tale determinazione può prendere forme diverse e risultare tanto dalla loro decisione comune quanto da loro decisioni convergenti. Orbene, in quest'ultimo caso, tali decisioni devono completarsi, cosicché ciascuna di esse abbia un effetto concreto sulla determinazione delle finalità e dei mezzi del trattamento.

[40] Ai sensi dell'articolo 4, punto 7, del RGPD.
[41] Articolo 26, paragrafo 1, del RGPD, letto alla luce del considerando 79 di tale regolamento.

7. Condizioni di liceità di un trattamento di dati personali

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

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 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.

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.

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.

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.

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.

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.

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.

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.

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 Naţională 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 [42] 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 [43]. A tal riguardo, il consenso non è validamente espresso in caso di silenzio, di preselezione di caselle o di inattività.

[42] Articolo 7 della direttiva 95/46 e articolo 6 del RGPD.
[43] Articolo 2, lettera a), della direttiva 95/46 e articolo 4, punto 11, del RGPD.

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.

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, 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.

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.

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.

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.

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» [44]. 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 essa può suscitare la disapprovazione sociale e comportare la stigmatizzazione della persona interessata.

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.

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.

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

[44] 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 (...)».

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.

III. Trattamento dei dati personali ai sensi della normativa settoriale

1. Trattamento dei dati personali nel settore delle comunicazioni elettroniche

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

La causa in argomento 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 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.

In tale contesto, la Corte ha precisato che, se è vero che nella sua sentenza Tele2 Sverige e Watson e a. [45] 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».

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)

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

[45] Sentenza della Corte del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, *EU:C:2016:970*).

Cour constitutionnelle (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.

La Corte ricorda poi che la direttiva 2002/58 [46] 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 [47], 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 [48].

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

[46] Articolo 15, paragrafi 1 e 3, della direttiva 2002/58.
[47] Articolo 5, paragrafo 1, della direttiva 2002/58.
[48] In particolare, articoli 7, 8 e 11 nonché articolo 52, paragrafo 1, della Carta.

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.

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.

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.

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 urgenza debitamente giustificata, il controllo deve intervenire entro termini brevi.

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, rientrano, allo stato attuale del diritto dell'Unione, unicamente nel diritto nazionale. Tuttavia, la Corte precisa che la direttiva 2002/58, 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.

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 [49] 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

[49] 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.

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. [50], 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 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.

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.

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

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

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.

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.

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.

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.

Sentenza del 5 aprile 2022 (Grande Sezione), Commissioner of An Garda Síochána e a. (C-140/20, EU:C:2022:258)

In tale causa, la domanda di pronuncia pregiudiziale è stata presentata dalla Supreme Court (Corte suprema, Irlanda) nell'ambito di un procedimento civile promosso da una persona condannata all'ergastolo per un omicidio commesso in Irlanda. Quest'ultima contestava la compatibilità con il diritto dell'Unione di talune disposizioni della legge nazionale relativa alla conservazione dei dati generati nell'ambito delle comunicazioni elettroniche. In forza di tale legge, dati relativi al traffico e dati relativi all'ubicazione di chiamate telefoniche dell'accusato erano stati conservati dai fornitori di servizi di comunicazione elettronica e resi accessibili alle autorità di polizia. I dubbi espressi dal giudice del rinvio vertevano in particolare sulla compatibilità con la direttiva 2002/58, letta alla luce della Carta, di un regime di conservazione generalizzata e indifferenziata di tali dati, in relazione alla lotta alla criminalità grave.

Con la sua sentenza, pronunciata in Grande Sezione, la Corte conferma, precisandone la portata, la giurisprudenza derivante dalla sentenza La Quadrature du Net e a. [51], ricordando che la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione relativi alle comunicazioni elettroniche non è autorizzata ai fini della lotta alla criminalità grave e la prevenzione delle minacce gravi alla sicurezza pubblica. Essa conferma altresì la giurisprudenza scaturita dalla sentenza Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) [52] in particolare per quanto riguarda l'obbligo di subordinare l'accesso delle autorità nazionali competenti a detti dati conservati ad un controllo preventivo effettuato o da un giudice o da un organo amministrativo indipendente, nei confronti di un funzionario di polizia.

La Corte dichiara, in primo luogo, che la direttiva 2002/58, letta alla luce della Carta, osta a misure legislative che prevedano, a titolo preventivo, per finalità di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica, la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione. Infatti, tenuto conto, da un lato, degli effetti dissuasivi sull'esercizio dei diritti fondamentali [53] che tale conservazione può determinare e, dall'altro, della gravità dell'ingerenza che essa comporta, una siffatta conservazione deve costituire l'eccezione e non la regola al sistema istituito dalla direttiva, cosicché tali dati non possano essere oggetto di una conservazione sistematica e continuativa. La criminalità, anche particolarmente grave, non può essere equiparata a una minaccia per la sicurezza nazionale, in quanto una siffatta equiparazione potrebbe introdurre una categoria intermedia tra la sicurezza nazionale e la sicurezza pubblica, per applicare alla seconda i requisiti inerenti alla prima.

---

51 Sentenza del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, *EU:C:2020:791*).

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

53 Sanciti agli articoli da 7 a 11 della Carta.

Invece, la direttiva 2002/58, letta alla luce della Carta, non osta a misure legislative che prevedano, per fini di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica, la conservazione mirata dei dati relativi al traffico e dei dati relativi 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, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile. Essa aggiunge che una siffatta misura di conservazione riguardante luoghi o infrastrutture frequentati regolarmente da un numero molto elevato di persone o luoghi strategici, quali aeroporti, stazioni, porti marittimi o zone di pedaggio, può consentire alle autorità competenti di ottenere informazioni sulla presenza, in tali luoghi o aree geografiche, delle persone che vi utilizzano un mezzo di comunicazione elettronica e di trarne conclusioni sulla loro presenza e sulla loro attività in detti luoghi o aree geografiche per fini di lotta alla criminalità grave. In ogni caso, l'eventuale esistenza di difficoltà nel definire con precisione le ipotesi e le condizioni alle quali si può effettuare la conservazione mirata non può giustificare il fatto che gli Stati membri prevedano una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione.

Tale direttiva, letta alla luce della Carta, non osta neppure a misure legislative che prevedano, ai medesimi fini, la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario, nonché dei dati relativi all'identità civile degli utenti di comunicazioni elettroniche. Per quanto riguarda quest'ultimo aspetto, la Corte precisa in particolare che né la direttiva 2002/58, né alcun altro atto di diritto dell'Unione ostano a una normativa nazionale, avente ad oggetto la lotta alla criminalità grave, in forza della quale l'acquisizione di un mezzo di comunicazione elettronica, quale una carta SIM prepagata, è subordinata alla verifica di documenti ufficiali che provino l'identità civile dell'acquirente e alla registrazione, da parte del venditore, delle informazioni che ne derivano, essendo il venditore eventualmente tenuto a fornire alle autorità nazionali competenti tali informazioni.

Lo stesso dicasi per quanto attiene alle misure legislative che prevedano, sempre per fini di lotta alla criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica, il ricorso a un'ingiunzione che imponga ai fornitori di servizi di comunicazione elettronica, mediante un provvedimento dell'autorità competente soggetto a un controllo giurisdizionale effettivo, di procedere, per un periodo determinato, alla conservazione rapida («quick freeze») dei dati relativi al traffico e dei dati relativi all'ubicazione di cui dispongono. Infatti, solo la lotta alla criminalità grave e, a fortiori, la salvaguardia della sicurezza nazionale sono idonee a giustificare una simile conservazione, a condizione che tale misura e l'accesso ai dati conservati rispettino i limiti dello stretto necessario. La Corte ricorda che una simile misura di conservazione rapida può essere estesa ai dati relativi al traffico e ai dati relativi all'ubicazione di persone diverse da quelle sospettate di aver progettato o commesso un reato grave o un attentato alla sicurezza nazionale, purché tali dati possano contribuire, sulla base di

elementi oggettivi e non discriminatori, all'accertamento di un siffatto reato o attentato alla sicurezza nazionale, quali i dati della vittima o del suo ambiente sociale o professionale.

Tuttavia, la Corte precisa, poi, che tutte le summenzionate misure legislative devono garantire, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi sia subordinata al rispetto delle relative condizioni sostanziali e procedurali e che le persone interessate dispongano di garanzie effettive contro il rischio di abusi. Le diverse misure di conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione possono, a scelta del legislatore nazionale e nel rispetto dei limiti dello stretto necessario, essere applicate congiuntamente.

Inoltre, la Corte precisa che il fatto di autorizzare, per fini di lotta alla criminalità grave, l'accesso a simili dati conservati in modo generalizzato e indifferenziato, per far fronte a una minaccia grave alla sicurezza nazionale, sarebbe contrario alla gerarchia degli obiettivi di interesse generale in grado di giustificare una misura adottata in forza della direttiva 2002/58. Infatti, ciò significherebbe consentire che l'accesso possa essere giustificato da un obiettivo di importanza minore rispetto a quello che ha giustificato la conservazione, vale a dire la salvaguardia della sicurezza nazionale, rischiando in tal modo di privare di ogni effetto utile il divieto di procedere alla conservazione generalizzata e indifferenziata per fini di lotta alla criminalità grave.

In secondo luogo, la Corte decide che la direttiva 2002/58, letta alla luce della Carta, osta a una normativa nazionale, in forza della quale il trattamento centralizzato delle domande di accesso a dati conservati dai fornitori di servizi di comunicazione elettronica, provenienti dalla polizia nell'ambito della ricerca e del perseguimento di reati gravi, è affidato a un funzionario di polizia, anche se assistito da un'unità istituita all'interno della polizia, che gode di una certa autonomia nell'esercizio della sua missione e le cui decisioni possono essere successivamente sottoposte a controllo giurisdizionale. Infatti, da un lato, un funzionario di tale tipo non soddisfa i requisiti di indipendenza e di imparzialità che si impongono ad un'autorità amministrativa che esercita il controllo preventivo delle domande di accesso ai dati provenienti dalle autorità nazionali competenti, in quanto egli non ha la qualità di terzo rispetto a tali autorità. Dall'altro, sebbene la decisione di un funzionario di questo tipo possa essere oggetto di un controllo giurisdizionale esercitato a posteriori, tale controllo non può sostituirsi ad un controllo indipendente e, salvo casi di urgenza debitamente giustificata, preventivo.

In terzo luogo, infine, la Corte conferma la propria giurisprudenza secondo cui il diritto dell'Unione osta a che un giudice nazionale limiti nel tempo gli effetti di una declaratoria di invalidità ad esso spettante, in forza del diritto nazionale, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, a causa dell'incompatibilità di tale normativa con la direttiva 2002/58. Ciò premesso, la Corte ricorda che l'ammissibilità degli elementi di prova ottenuti mediante

una siffatta conservazione, conformemente al principio di autonomia procedurale degli Stati membri, rientra nel diritto nazionale, fatto salvo il rispetto, in particolare, dei principi di equivalenza e di effettività.

Sentenza del 20 settembre 2022 (Grande Sezione), VD e SR (C-339/20 e C-397/20, EU:C:2022:703)

A seguito di un'indagine dell'Autorità dei mercati finanziari (AMF, Francia), sono stati avviati procedimenti penali nei confronti di VD e di SR, due persone fisiche accusate di delitti di abuso di informazioni privilegiate, di abuso secondario di informazioni privilegiate, di favoreggiamento, di corruzione e di riciclaggio. Nell'ambito di tale indagine, l'AMF aveva utilizzato dati personali derivanti da telefonate di VD e di SR, generate sulla base del codice francese delle poste e delle comunicazioni elettroniche, nell'ambito della fornitura di servizi di comunicazione elettronica.

Essendo stati formalmente incriminati sulla base dei dati relativi al traffico forniti dall'AMF, VD e SR hanno proposto ciascuno un ricorso dinanzi alla cour d'appel de Paris (Corte d'appello di Parigi, Francia), deducendo, in particolare, un motivo vertente sulla violazione dell'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. Più in particolare, basandosi sulla giurisprudenza derivante dalla sentenza Tele2 Sverige e Watson e a. [54], VD e SR hanno contestato il fatto che l'AMF si era basata, per procedere alla raccolta di tali dati, sulle disposizioni nazionali in questione laddove, a loro avviso, tali disposizioni, da un lato, non erano conformi al diritto dell'Unione, in quanto prevedevano una conservazione generalizzata e indiscriminata dei dati di connessione e, dall'altro, non stabilivano alcun limite al potere degli inquirenti dell'AMF di richiedere i dati conservati.

Con due sentenze del 20 dicembre 2018 e del 7 marzo 2019, la cour d'appel de Paris (Corte d'appello di Parigi) ha respinto i ricorsi di VD e SR. Per respingere il motivo summenzionato, i giudici di merito si sono basati, in particolare, sul fatto che il regolamento sugli abusi di mercato [55] consente alle autorità competenti di richiedere, nella misura in cui il diritto nazionale lo autorizzi, le registrazioni esistenti dei dati relativi al traffico detenuti dagli operatori di servizi di comunicazione elettronica, qualora sussistano motivi per sospettare una violazione del divieto di abuso di informazioni privilegiate e tali registrazioni possano essere rilevanti ai fini delle indagini su tale violazione.

VD e SR hanno quindi impugnato tali sentenze dinanzi alla Cour de cassation (Corte di cassazione, Francia), giudice del rinvio nelle presenti cause.

---

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

[55] Regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, relativo agli abusi del mercato (regolamento sugli abusi di mercato) e che abroga la direttiva 2003/6 e le direttive 2003/124/CE, 2003/125/CE e 2004/72/CE della Commissione (GU 2014, L 173, pag. 1).

In tale contesto, detto giudice si interroga sulla conciliazione dell'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce della Carta, con i requisiti risultanti dall'articolo 12, paragrafo 2, lettere a) e d), della direttiva «abusi di mercato» [56] e dall'articolo 23, paragrafo 2, lettere g) e h), del regolamento relativo agli abusi di mercato. Tale interrogativo trae origine dalle misure legislative di cui trattasi nei procedimenti principali, le quali prevedono a titolo preventivo, in capo agli operatori di servizi di comunicazione elettronica, una conservazione generalizzata e indiscriminata dei dati relativi al traffico per un anno a partire dal giorno della registrazione, a fini di lotta contro i reati di abuso di mercato, tra i quali rientrano gli abusi di informazioni privilegiate. Nell'ipotesi in cui la Corte dovesse giudicare che la normativa sulla conservazione dei dati di connessione di cui trattasi nei procedimenti principali non sia conforme al diritto dell'Unione, il giudice del rinvio si pone la questione del mantenimento provvisorio degli effetti di tale normativa, al fine di evitare un'incertezza del diritto e di consentire che i dati in precedenza raccolti e conservati siano utilizzati ai fini dell'individuazione e del perseguimento degli abusi di informazioni privilegiate.

Con la sua sentenza, la Corte, riunita in Grande Sezione, dichiara che la conservazione generalizzata e indiscriminata dei dati relativi al traffico per un anno a decorrere dal giorno della registrazione da parte degli operatori di servizi di comunicazione elettronica non è autorizzata, in via preventiva, a fini di lotta contro i reati di abuso del mercato. Peraltro, essa conferma la propria giurisprudenza secondo cui il diritto dell'Unione osta a che un giudice nazionale limiti nel tempo gli effetti di una declaratoria di invalidità ad esso spettante in merito a disposizioni legislative nazionali incompatibili con il diritto dell'Unione.

La Corte ricorda anzitutto che, al fine di interpretare una disposizione del diritto dell'Unione, occorre non soltanto fare riferimento alla lettera della stessa, ma anche tener conto del suo contesto e degli scopi perseguiti dalla normativa di cui essa fa parte.

Per quanto riguarda la formulazione delle disposizioni di cui alle questioni pregiudiziali, la Corte constata che, mentre l'articolo 12, paragrafo 2, lettera d), della direttiva «abusi di mercato» si riferisce al potere dell'AMF di «richiedere le registrazioni telefoniche esistenti e le informazioni esistenti relative al traffico», l'articolo 23, paragrafo 2, lettere g) e h), del regolamento relativo agli abusi di mercato rinvia al potere di tale autorità di chiedere, da un lato, le «registrazioni esistenti relative (...) allo scambio di dati conservate da società di investimento, istituti di credito o istituti finanziari» e, dall'altro, «nella misura in cui ciò sia consentito dal diritto nazionale, le registrazioni esistenti relative allo scambio di dati conservate da un operatore di telecomunicazioni». Secondo la Corte, dal tenore letterale di tali disposizioni emerge inequivocabilmente che esse si limitano a circoscrivere il potere dell'AMF di «richiedere», o ancora, di «chiedere» i dati di cui dispongono tali operatori, il che corrisponde a un accesso a tali dati. Inoltre, il riferimento alle

[56] Direttiva 2003/6/CE del Parlamento europeo e del Consiglio, del 28 gennaio 2003, relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato (abusi di mercato) (GU 2003, L 96, pag. 16).

registrazioni «esistenti», quali «conservate» da detti operatori, lascia intendere che il legislatore dell'Unione non ha inteso disciplinare la possibilità, per il legislatore nazionale, di istituire un obbligo di conservazione di tali registrazioni. Secondo la Corte, tale interpretazione sarebbe peraltro corroborata sia dal contesto in cui si inseriscono dette disposizioni, sia dagli obiettivi perseguiti dalla normativa di cui queste stesse disposizioni fanno parte.

Per quanto riguarda il contesto in cui si collocano le disposizioni oggetto delle questioni pregiudiziali la Corte osserva che, se è vero che, ai sensi delle pertinenti disposizioni della direttiva «abusi di mercato» e del regolamento relativo agli abusi di mercato [57], il legislatore dell'Unione ha inteso imporre agli Stati membri l'obbligo di adottare le misure necessarie affinché le autorità competenti in materia finanziaria dispongano di un insieme di strumenti, competenze e risorse adeguate, nonché dei poteri di vigilanza e di indagine necessari per garantire l'efficacia dei loro compiti, tali disposizioni nulla dicono né sull'eventuale possibilità per gli Stati membri di imporre, a tali fini, a carico degli operatori di servizi di comunicazione elettronica, un obbligo di conservazione generalizzato e indiscriminato dei dati relativi al traffico, né sulle condizioni alle quali tali dati devono essere conservati dagli stessi operatori ai fini della loro eventuale consegna alle autorità competenti.

Quanto agli obiettivi perseguiti dalla normativa di cui trattasi, la Corte rileva che sia dalla direttiva «abusi di mercato» sia dal regolamento relativo agli abusi di mercato [58], risulta che tali atti hanno lo scopo di garantire l'integrità dei mercati finanziari dell'Unione e di rafforzare la fiducia degli investitori in tali mercati, fiducia che riposa, in particolare, sul fatto che essi saranno posti su un piano di parità e tutelati contro l'utilizzazione illecita di informazioni privilegiate. Il divieto di abuso di informazioni privilegiate previsto da tali atti [59] è volto pertanto a garantire la parità dei partecipanti ad una compravendita di borsa evitando che uno di loro, che detenga un'informazione privilegiata e si trovi, perciò, in posizione avvantaggiata rispetto agli altri investitori, ne tragga profitto a scapito di coloro che la ignorano. Sebbene, ai sensi del regolamento relativo agli abusi di mercato [60], le registrazioni dei dati di connessione costituiscano una prova essenziale e talvolta l'unica che consenta di rilevare e dimostrare l'esistenza di un abuso di informazioni privilegiate o di una manipolazione del mercato, ciò non toglie che tale regolamento si riferisce unicamente alle registrazioni «detenute» dagli operatori di servizi di comunicazione elettronica, nonché al potere dell'autorità competente in materia finanziaria di «richiedere», presso tali operatori, la comunicazione dei dati «esistenti». Pertanto, da tale testo non risulta affatto che il legislatore dell'Unione abbia inteso, in tal modo, riconoscere agli Stati membri il potere di imporre agli operatori di

[57] Rispettivamente, articolo 12, paragrafo 1, della direttiva «abusi di mercato» e articolo 23, paragrafo 3, del regolamento relativo agli abusi di mercato, alla luce del considerando 62 di quest'ultimo.

[58] Rispettivamente, considerando 2 e 12 della direttiva «abusi di mercato» e articolo 1 del regolamento relativo agli abusi di mercato, alla luce dei considerando 2 e 24 del medesimo.

[59] Articolo 2, paragrafo 1, della direttiva «abusi di mercato» e articolo 8, paragrafo 1, del regolamento relativo agli abusi di mercato.

[60] Considerando 62 del regolamento relativo agli abusi di mercato.

servizi di comunicazione elettronica un obbligo generale di conservazione dei dati. Ne consegue che né la direttiva «abusi di mercato», né il regolamento relativo agli abusi di mercato possono costituire il fondamento giuridico di un obbligo generale di conservazione delle registrazioni di dati relativi al traffico detenuti dagli operatori di servizi di comunicazione elettronica ai fini dell'esercizio dei poteri conferiti all'autorità competente in materia finanziaria per tali atti.

La Corte ricorda poi che la direttiva 2002/58 costituisce l'atto di riferimento in materia di conservazione e, più in generale, di trattamento dei dati personali nel settore delle comunicazioni elettroniche, cosicché la sua interpretazione, come effettuata alla luce di tale direttiva, disciplina anche le registrazioni dei dati relativi al traffico detenuti dagli operatori di servizi di comunicazione elettronica che le autorità competenti in materia finanziaria, ai sensi della direttiva «abusi di mercato» e del regolamento relativo agli abusi di mercato [61], possono richiedere loro. La valutazione della liceità del trattamento delle registrazioni detenute dagli operatori di servizi di comunicazione elettronica [62] deve, pertanto, essere effettuata alla luce delle condizioni previste dalla direttiva 2002/58, nonché dell'interpretazione di tale direttiva da parte della Corte, nella sua giurisprudenza.

In tal senso, la Corte dichiara che la direttiva «abusi di mercato» e il regolamento relativo agli abusi di mercato, letti in combinato disposto con la direttiva 2002/58 e alla luce della Carta, ostano a misure legislative che prevedano, a titolo preventivo, a fini di lotta contro i reati di abuso del mercato, tra cui rientrano gli abusi di informazioni privilegiate, una conservazione temporanea, ossia di un anno a decorrere dal giorno della registrazione, ma generalizzata e indiscriminata, dei dati relativi al traffico, da parte degli operatori dei servizi di comunicazione elettronica.

Infine, la Corte conferma la propria giurisprudenza secondo cui il diritto dell'Unione osta a che un giudice nazionale limiti nel tempo gli effetti di una declaratoria di invalidità ad esso spettante, in forza del diritto nazionale, nei confronti di una normativa nazionale che, da un lato, impone agli operatori dei servizi di comunicazione elettronica la conservazione generalizzata e indiscriminata dei dati relativi al traffico e, dall'altro, consente la comunicazione di tali dati all'autorità competente in materia finanziaria, senza previa autorizzazione da parte di un giudice o di un'autorità amministrativa indipendente, a causa dell'incompatibilità di tale normativa con la direttiva 2002/58, letta alla luce della Carta. Ciò premesso, la Corte ricorda che l'ammissibilità degli elementi di prova ottenuti mediante una siffatta conservazione, conformemente al principio di autonomia procedurale degli Stati membri, rientra nel diritto nazionale, fatto salvo il rispetto, in particolare, dei principi di equivalenza e di effettività. Quest'ultimo principio impone al giudice penale nazionale di escludere informazioni ed elementi di prova ottenuti per mezzo di una conservazione generalizzata e indiscriminata incompatibile

[61] Rispettivamente, articolo 11 della direttiva «abusi di mercato» e articolo 22 del regolamento relativo agli abusi di mercato.

[62] Ai sensi dell'articolo 12, paragrafo 2, lettera d), della direttiva «abusi di mercato» e dell'articolo 23, paragrafo 2, lettere g) e h), del regolamento relativo agli abusi di mercato.

con il diritto dell'Unione, qualora gli interessati non siano in grado di commentare efficacemente tali informazioni e tali elementi di prova, che provengono da un settore che esula dalla conoscenza dei giudici e possono influenzare in modo preponderante la valutazione dei fatti.

Sentenza del 30 aprile 2024 (seduta plenaria), La Quadrature du Net e a. (Dati personali e lotta contro la contraffazione) (C-470/21, EU:C:2024:370)

Adita in via pregiudiziale dal Conseil d'État (Consiglio di Stato, Francia), la Corte in seduta plenaria sviluppa la sua giurisprudenza sulla direttiva 2002/58 fornendo precisazioni riguardanti, da un lato, le condizioni nelle quali si può considerare che una conservazione generalizzata di indirizzi IP da parte di fornitori di servizi di comunicazione elettronica non comporta un'ingerenza grave nei diritti al rispetto della vita privata, alla protezione dei dati personali nonché alla libertà di espressione garantiti dalla Carta [63], e, dall'altro, la possibilità, per un'autorità pubblica, di accedere a taluni dati personali conservati nel rispetto di tali condizioni, nell'ambito della lotta contro i reati concernenti violazioni dei diritti di proprietà intellettuale commessi online.

Nel caso di specie, quattro associazioni hanno presentato al Premier ministre (Primo ministro, Francia) una domanda di abrogazione del decreto relativo al trattamento automatizzato di dati personali [64]. Poiché tale domanda non ha sortito effetti, tali associazioni hanno adito il Consiglio d'État (Consiglio di Stato) con un ricorso diretto all'annullamento di tale decisione implicita di rigetto. A loro avviso, tale decreto nonché le disposizioni che ne costituiscono il fondamento normativo [65] violano il diritto dell'Unione.

In base alla legislazione francese, la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Hadopi) (Alta Autorità per la diffusione delle opere e la protezione dei diritti su Internet, Hadopi), per poter identificare i responsabili di lesioni dei diritti d'autore o dei diritti connessi commesse online, è autorizzata ad accedere a taluni dati che i fornitori di servizi di comunicazione elettronica sono tenuti a conservare. Tali dati riguardano l'identità civile di un interessato corrispondenti al suo indirizzo IP precedentemente raccolto da organismi degli aventi diritto. Una volta identificato il titolare dell'indirizzo IP utilizzato per attività che comportano una siffatta lesione, l'Hadopi segue la procedura della cosiddetta «risposta graduale». In concreto, essa è autorizzata ad inviare a tale persona due raccomandazioni assimilabili ad

63 Articoli 7, 8 e 11 della Carta.

64 Décret n. 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé «Système de gestion des mesures pour la protection des œuvres sur internet» (decreto n. 2010-236, del 5 marzo 2010, relativo al trattamento automatizzato di dati personali autorizzato dall'articolo L. 331-29 del codice della proprietà intellettuale denominato «Sistema di gestione delle misure per la protezione delle opere su Internet») (JORF n. 56 del 7 marzo 2010, testo n. 19), come modificato dal décret n. 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (decreto n. 2017-924, del 6 maggio 2017, relativo alla gestione dei diritti d'autore e dei diritti connessi da parte di un organismo di gestione di diritti e recante modifica del codice della proprietà intellettuale) (JORF n. 109 del 10 maggio 2017, testo n. 176).

65 In particolare, l'articolo L. 331-21, commi dal terzo al quinto, del codice della proprietà intellettuale.

avvertimenti e, se le attività persistono, una lettera che le notifica che le sue attività sono perseguibili penalmente. Infine, essa ha il diritto di adire il pubblico ministero ai fini dell'azione penale nei confronti di detta persona [66].

In tale contesto, il Conseil d'État (Consiglio di Stato) ha interrogato la Corte sull'interpretazione della direttiva 2002/58, letta alla luce della Carta [67].

In primo luogo, per quanto riguarda la conservazione dei dati relativi all'identità civile e dei corrispondenti indirizzi IP, la Corte sottolinea che non tutte le conservazioni generalizzate e indifferenziate degli indirizzi IP costituiscono necessariamente un'ingerenza grave nei diritti al rispetto della vita privata, alla protezione dei dati personali nonché alla libertà di espressione garantiti dalla Carta.

L'obbligo di garantire una siffatta conservazione può essere giustificato dall'obiettivo della lotta contro i reati in generale, qualora sia effettivamente escluso che tale conservazione possa generare ingerenze gravi nella vita privata dell'interessato per effetto della possibilità di trarre conclusioni precise su di essa, in particolare mettendo in relazione tali indirizzi IP con un insieme di dati relativi al traffico o all'ubicazione.

Pertanto, uno Stato membro che intenda imporre ai fornitori di servizi di comunicazione elettronica un siffatto obbligo deve assicurarsi che le modalità di conservazione di tali dati escludano che possano essere tratte conclusioni precise sulla vita privata degli interessati.

La Corte precisa che le modalità di conservazione devono, a tal fine, riguardare la struttura stessa della conservazione che, in sostanza, deve essere organizzata in modo da garantire una separazione effettivamente stagna delle diverse categorie di dati conservati. Pertanto, le norme nazionali relative a tali modalità devono garantire che ciascuna categoria di dati, compresi i dati relativi all'identità civile e gli indirizzi IP, sia conservata in modo completamente separato dalle altre categorie di dati conservati e che tale separazione sia effettivamente stagna, mediante un dispositivo informatico sicuro e affidabile. Inoltre, tali norme, allorché prevedono la possibilità di mettere in relazione gli indirizzi IP conservati con l'identità civile dell'interessato a fini di lotta contro i reati, devono consentire una siffatta messa in relazione solo mediante l'uso di un procedimento tecnico efficiente che non metta in discussione l'efficacia della separazione stagna di tali categorie di dati. L'affidabilità di tale separazione deve essere oggetto di un controllo regolare da parte di un'autorità pubblica terza. Sempre che la normativa nazionale applicabile preveda siffatti rigorosi requisiti, non può essere qualificata come «grave» l'ingerenza risultante da tale conservazione degli indirizzi IP.

---

66 A decorrere dal 1º gennaio 2022, l'Hadopi si è fusa con il Conseil supérieur de l'audiovisuel (CSA) (Consiglio superiore dell'audiovisivo, CSA), un'altra autorità pubblica indipendente, per costituire l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) (autorità di regolamentazione per la comunicazione audiovisiva e digitale, ARCOM). Tuttavia, la procedura di risposta graduale è rimasta sostanzialmente invariata.

67 Articolo 15, paragrafo 1, della direttiva 2002/58.

Pertanto, la Corte conclude che, in presenza di un dispositivo legislativo che garantisca che nessuna combinazione di dati consentirà di trarre conclusioni precise sulla vita privata delle persone i cui dati sono conservati, la direttiva 2002/58, letta alla luce della Carta, non osta a che uno Stato membro imponga un obbligo di conservazione generalizzata e indifferenziata degli indirizzi IP, per una durata che non ecceda lo stretto necessario, ai fini di un obiettivo di lotta contro i reati in generale.

In secondo luogo, per quanto riguarda l'accesso a dati relativi all'identità civile corrispondenti a indirizzi IP, la Corte dichiara che la direttiva 2002/58, letta alla luce della Carta, non osta, in linea di principio, a una normativa nazionale che consente l'accesso, da parte di un'autorità pubblica, a tali dati conservati dai fornitori di servizi di comunicazione elettronica in maniera separata ed effettivamente stagna, al solo scopo di permettere a tale autorità di identificare i titolari di tali indirizzi sospettati di essere responsabili di lesioni dei diritti d'autore e dei diritti connessi su Internet e di adottare misure nei loro confronti. In un caso del genere, la normativa nazionale deve vietare agli agenti che dispongono di siffatto accesso, anzitutto, di divulgare sotto qualsiasi forma informazioni sul contenuto dei file consultati da tali titolari, salvo al solo scopo di adire il pubblico ministero, inoltre, di effettuare qualsiasi tracciamento del percorso di navigazione di tali titolari e, infine, di utilizzare tali indirizzi IP a fini diversi dall'adozione delle suddette misure.

In tale contesto, la Corte ricorda in particolare che, pur se la libertà di espressione e la riservatezza dei dati personali sono preoccupazioni primarie, tali diritti fondamentali non sono tuttavia assoluti. Nell'ambito di un bilanciamento dei diritti e degli interessi in gioco, infatti, questi ultimi devono talvolta lasciare il passo dinanzi ad altri diritti fondamentali e ad imperativi di interesse generale quali la difesa dell'ordine pubblico e la prevenzione dei reati o la protezione dei diritti e delle libertà altrui. Ciò si verifica, in particolare, qualora la preponderanza accordata a dette preoccupazioni primarie sia tale da ostacolare l'efficacia di un'indagine penale, in particolare rendendo impossibile o eccessivamente difficile l'identificazione effettiva dell'autore di un reato e l'irrogazione di una sanzione nei suoi confronti.

In detto stesso contesto, la Corte fa altresì riferimento alla sua giurisprudenza secondo la quale, per quanto riguarda la lotta contro i reati che violano i diritti d'autore o i diritti connessi commessi online, la circostanza che l'accesso agli indirizzi IP possa costituire l'unico mezzo di indagine che consenta l'identificazione dell'interessato tende a dimostrare che la conservazione di tali indirizzi e l'accesso agli stessi sono strettamente necessari alla realizzazione dell'obiettivo perseguito e soddisfano quindi il requisito di proporzionalità. Non consentire un siffatto accesso comporterebbe inoltre un rischio reale di impunità sistemica di reati commessi online o la cui commissione o preparazione è agevolata dalle caratteristiche proprie di Internet. Ebbene, l'esistenza di un siffatto rischio costituisce una circostanza rilevante al fine di valutare, nell'ambito di un bilanciamento dei diversi diritti e interessi in gioco, se un'ingerenza nei diritti al

rispetto della vita privata, alla protezione dei dati personali nonché alla libertà di espressione sia una misura proporzionata rispetto all'obiettivo della lotta contro i reati.

In terzo luogo, pronunciandosi sulla questione se l'accesso dell'autorità pubblica a dati relativi all'identità civile corrispondenti a un indirizzo IP debba essere subordinato a un controllo previo da parte di un giudice o di un organismo amministrativo indipendente, la Corte ritiene che la necessità di un controllo siffatto si imponga qualora, nel contesto di una normativa nazionale, tale accesso comporti il rischio di una grave ingerenza nei diritti fondamentali della persona interessata, nel senso che esso potrebbe consentire a tale autorità pubblica di trarre conclusioni precise sulla vita privata di tale persona e, se del caso, di tracciarne il profilo dettagliato. Viceversa, tale necessità di un controllo preventivo non è destinata ad applicarsi quando non può essere qualificata come grave l'ingerenza nei diritti fondamentali.

A tal riguardo, la Corte precisa che, nel caso in cui sia istituito un dispositivo di conservazione che garantisca una separazione effettivamente stagna delle diverse categorie di dati conservati, l'accesso dell'autorità pubblica ai dati relativi all'identità civile corrispondenti agli indirizzi IP non è, in linea di principio, subordinato al requisito di un controllo previo. Un siffatto accesso al solo scopo di identificare il titolare di un indirizzo IP non costituisce, infatti, di regola, una grave ingerenza nei diritti summenzionati.

Tuttavia, la Corte non esclude che, in situazioni atipiche, sussista il rischio che, nell'ambito di un procedimento come il procedimento di risposta graduata di cui trattasi nel procedimento principale, l'autorità pubblica possa trarre conclusioni precise sulla vita privata dell'interessato, in particolare qualora questi compia attività che ledono i diritti d'autore o i diritti connessi, su reti tra pari (peer to peer), in modo ripetuto, se non su larga scala, in relazione ad opere protette di tipo particolare, atte a rivelare informazioni, eventualmente sensibili, sulla vita privata di detta persona.

Nel caso di specie, un titolare di un indirizzo IP può essere particolarmente esposto a un rischio siffatto qualora l'autorità pubblica sia chiamata a decidere se adire o meno il pubblico ministero affinché egli sia perseguito penalmente. Infatti, l'intensità della lesione del diritto al rispetto della vita privata può aumentare man mano che la procedura di risposta graduata, che opera secondo un processo sequenziale, percorra le diverse fasi che la compongono. L'accesso dell'autorità competente al complesso dei dati, relativi alla persona interessata e accumulati nel corso delle varie fasi di tale procedimento, può consentire di trarre conclusioni precise sulla vita privata di quest'ultima. Di conseguenza, la normativa nazionale deve prevedere un controllo previo, il quale deve avvenire prima che l'autorità pubblica possa mettere in relazione i dati relativi all'identità civile e siffatto insieme di dati, e prima dell'eventuale invio della lettera di notifica in cui si constata che tale persona ha compiuto fatti perseguibili penalmente. Tale controllo deve peraltro preservare l'efficacia della procedura di risposta graduata consentendo, in particolare, di individuare i casi di possibile nuova reiterazione del comportamento illecito di cui trattasi. A tal fine, detta procedura deve

essere organizzata e strutturata in modo tale che i dati relativi all'identità civile di una persona corrispondenti a indirizzi IP precedentemente raccolti su Internet non possano essere automaticamente messi in relazione, ad opera delle persone incaricate dell'esame dei fatti in seno all'autorità pubblica competente, con elementi di cui quest'ultima già dispone e che potrebbero consentire di trarre conclusioni precise sulla vita privata di tale persona.

Inoltre, per quanto riguarda l'oggetto del controllo preventivo, la Corte rileva che, nel caso in cui la persona interessata sia sospettata di aver commesso un reato rientrante negli illeciti penali in generale, il giudice o l'organismo amministrativo indipendente incaricato di tale controllo deve negare l'accesso qualora quest'ultimo consenta all'autorità pubblica di trarre conclusioni precise sulla vita privata di detta persona. Per contro, dovrebbe essere consentito anche un accesso che consenta di trarre siffatte conclusioni precise nel caso in cui l'interessato sia sospettato di aver commesso reati considerati dallo Stato membro interessato lesivi di un interesse fondamentale della società e rientranti quindi nelle forme gravi di criminalità.

La Corte precisa altresì che un controllo preventivo non può in alcun caso essere completamente automatizzato poiché, trattandosi di un'indagine penale, un siffatto controllo richiede il bilanciamento, da un lato, degli interessi legittimi connessi alla lotta contro la criminalità e, dall'altro, del rispetto della vita privata e della protezione dei dati personali. Tale bilanciamento richiede l'intervento di una persona fisica, è ciò è tanto più necessario in quanto l'automaticità e la grande scala del trattamento di dati di cui trattasi comportano rischi per la vita privata.

La Corte conclude, pertanto, che la possibilità, per le persone incaricate dell'esame dei fatti in seno all'autorità pubblica, di mettere in relazione dati relativi all'identità civile di una persona corrispondenti a un indirizzo IP con i file contenenti elementi che consentono di conoscere il titolo di opere protette la cui messa a disposizione su Internet ha giustificato la raccolta degli indirizzi IP da parte di organismi degli aventi diritto deve essere subordinata, in ipotesi di una nuova reiterazione di un'attività lesiva dei diritti d'autore o dei diritti connessi da parte di una stessa persona, ad un controllo da parte di un giudice o di un organismo amministrativo indipendente. Tale controllo non può essere interamente automatizzato e deve avvenire prima di tale messa in relazione, che può consentire, in ipotesi del genere, di trarre precise conclusioni sulla vita privata di detto soggetto, il cui indirizzo IP sia stato utilizzato per attività che possono ledere i diritti d'autore o i diritti connessi.

In quarto e ultimo luogo, la Corte rileva che il sistema di trattamento di dati utilizzato dall'autorità pubblica deve essere oggetto, a intervalli regolari, di un controllo da parte di un organismo indipendente avente la qualità di terzo rispetto a tale autorità pubblica. Tale controllo mira a verificare l'integrità del sistema, comprese le garanzie effettive contro i rischi di accesso e uso impropri o illeciti di tali dati, nonché la sua efficacia e affidabilità nell'individuare eventuali violazioni.

In tale contesto, la Corte osserva che, nel caso di specie, il trattamento automatizzato dei dati personali effettuato dall'autorità pubblica sulla base delle informazioni relative alle contraffazioni constatate dagli organismi degli aventi diritto può comportare un certo numero di falsi positivi e soprattutto il rischio che un numero di dati potenzialmente molto elevato sia sviato da terzi a fini abusivi o illeciti, il che spiega la necessità di un siffatto controllo. Inoltre, essa aggiunge che tale trattamento deve rispettare le norme specifiche di protezione dei dati personali previste dalla direttiva 2016/680. Infatti, nel caso di specie, anche se l'autorità pubblica non dispone di poteri decisionali propri nell'ambito della procedura cosiddetta di risposta graduata, essa deve essere qualificata come «autorità pubblica» coinvolta nella prevenzione e nell'individuazione dei reati, e rientra quindi nel suo ambito di applicazione. Pertanto, le persone coinvolte in un siffatto procedimento devono beneficiare dell'insieme di garanzie sostanziali e procedurali prescritte dalla direttiva 2016/680, riguardo alle quali spetta al giudice del rinvio verificare se esse siano previste dalla normativa nazionale.

2. Trattamento dei dati personali in materia penale

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 [68] sia all'articolo 50 della Carta, vieta segnatamente che una persona che sia

[68] 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»)

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 [69].

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.

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 [70]. 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 [71]. Tale trattamento, da parte delle autorità degli Stati membri, può del resto risultare indispensabile proprio al fine di verificare l'applicabilità di detto principio.

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

[69] 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).

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

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

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 [72].

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.

Sentenza del 21 giugno 2022 (Grande Sezione), Ligue des droits humains (C-817/19, EU:C:2022:491)

In tale causa (v. altresì la rubrica I.1., intitolata «Conformità del diritto derivato dell'Unione al diritto alla protezione dei dati personali»), la Corte, dopo aver constatato la validità della direttiva PNR, fornisce precisazioni quanto all'interpretazione di talune disposizioni di tale direttiva [73].

In primo luogo, essa rileva che la direttiva elenca tassativamente gli obiettivi perseguiti dal trattamento dei dati PNR. Pertanto, tale direttiva osta a una normativa nazionale che autorizza il trattamento di dati PNR per finalità diverse dalla lotta contro i reati di terrorismo e i reati gravi. In tal senso, una normativa nazionale che, in aggiunta, come finalità del trattamento dei dati PNR, ammette il controllo delle attività contemplate dai servizi segreti e di sicurezza rischia di disattendere il carattere tassativo di tale elenco. Parimenti, il sistema istituito dalla direttiva PNR non può essere previsto ai fini del miglioramento dei controlli alle frontiere e della lotta all'immigrazione illegale. Ne consegue altresì che i dati PNR non possono essere conservati in una banca dati unica che può essere consultata per perseguire tanto finalità della direttiva PNR quanto altre finalità.

In secondo luogo, la Corte chiarisce la nozione di autorità nazionale indipendente, competente a verificare se le condizioni per la comunicazione dei dati PNR, ai fini della loro valutazione successiva, siano soddisfatte e ad approvare una siffatta

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

[73] In particolare, l'articolo 2 («Applicazione della [direttiva] ai voli intra-UE»), l'articolo 6 («Trattamento dei dati PNR»), e l'articolo 12 («Periodo di conservazione dei dati e anonimato»), della direttiva PNR.

comunicazione. In particolare, l'autorità istituita come UIP non può essere qualificata come tale poiché essa non ha la qualità di terzo rispetto all'autorità che chiede l'accesso ai dati. Infatti, poiché i membri del suo personale possono essere agenti distaccati da parte delle autorità abilitate a chiedere un siffatto accesso, l'UIP risulta necessariamente legata a tali autorità. Pertanto, la direttiva PNR osta a una normativa nazionale ai sensi della quale l'autorità istituita come UIP ha anche la qualità di autorità nazionale competente abilitata ad approvare la comunicazione dei dati PNR alla scadenza dei sei mesi successivi al trasferimento di tali dati all'UIP.

In terzo luogo, per quanto riguarda il termine di conservazione dei dati PNR, la Corte giudica che l'articolo 12 della direttiva PNR, alla luce degli articoli 7 e 8 nonché dell'articolo 52, paragrafo 1, della Carta, osta a una normativa nazionale che prevede un periodo generale di conservazione di tali dati di cinque anni, applicabile indistintamente a tutti i passeggeri aerei.

Infatti, secondo la Corte, dopo la scadenza del periodo iniziale di conservazione di sei mesi, la conservazione dei dati PNR non appare limitata allo stretto necessario per quanto riguarda i passeggeri aerei per i quali né la valutazione preliminare, né le eventuali verifiche effettuate durante il periodo di conservazione iniziale di sei mesi, né alcun'altra circostanza abbiano rivelato l'esistenza di elementi obiettivi – quale il fatto che i dati PNR dei passeggeri interessati abbiano dato luogo a un riscontro positivo verificato nell'ambito della valutazione preliminare – atti a determinare un rischio in materia di reati di terrorismo o di reati gravi aventi un collegamento oggettivo, quantomeno indiretto, con il viaggio aereo effettuato da tali passeggeri. Invece, essa afferma che, nel corso del periodo iniziale di sei mesi, la conservazione dei dati PNR di tutti i passeggeri aerei assoggettati al sistema istituito da tale direttiva non sembra, in linea di principio, eccedere i limiti dello stretto necessario.

In quarto luogo, la Corte fornisce indicazioni concernenti un'eventuale applicazione della direttiva PNR, ai fini della lotta contro i reati di terrorismo e i reati gravi, ad altri mezzi di trasporto che conducono passeggeri nell'Unione. Orbene, la direttiva, alla luce dell'articolo 3, paragrafo 2, TUE, dell'articolo 67, paragrafo 2, TFUE e dell'articolo 45 della Carta, osta a un sistema di trasferimento e trattamento dei dati PNR di tutti i trasporti effettuati con altri mezzi all'interno dell'Unione in assenza di minaccia terroristica reale e attuale o prevedibile alla quale sia confrontato lo Stato membro interessato. In una situazione del genere, come per i voli intra-UE, l'applicazione del sistema istituito dalla direttiva PNR deve essere limitata ai dati PNR dei trasporti relativi, in particolare, a determinati collegamenti o modalità di viaggio o ancora a determinate stazioni o a determinati porti marittimi per i quali esistano indicazioni che giustifichino tale applicazione. Spetta allo Stato membro interessato selezionare i trasporti per i quali esistono siffatte indicazioni e riesaminare regolarmente tale applicazione, in base all'evoluzione delle condizioni che hanno giustificato la loro selezione.

IV. Trasferimento di dati personali verso paesi terzi

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

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.

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.

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

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 [74], la Commissione aveva considerato che, nel contesto del cosiddetto

[74] 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).

regime dell'«approdo sicuro» (in inglese, «safe harbour») [75], 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.

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 fondamentali della persona. 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.

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

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

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.

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. 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. 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.

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 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.

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.).

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.

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.

In terzo luogo, la Corte ha constatato che il diritto fondamentale al rispetto della vita privata, sancito dall'articolo 7 della Carta, 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.

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

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 protezione adeguato [76]. 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 [77]. Il RGPD stabilisce precisamente, inoltre, a quali condizioni può avvenire un trasferimento siffatto in mancanza di una decisione di adeguatezza o di garanzie adeguate [78].

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 [79], 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») [80].

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 [81]. 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

[76] Articolo 45 del RGPD.
[77] Articolo 46, paragrafi 1 e 2, lettera c), del RGPD.
[78] Articolo 49 del RGPD.
[79] Decisione della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 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).
[80] Sentenza della Corte del 6 ottobre 2015, Schrems, C-362/14, *EU:C:2015:650*.
[81] 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).

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 [82].

Con la sua domanda di pronuncia pregiudiziale, il giudice del rinvio interroga la Corte 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 non emerge alcun elemento idoneo ad inficiarne la validità. Essa dichiara invece invalida la decisione 2016/1250.

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.

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.

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

[82] 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).

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.

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.

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.

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.

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 le rubriche II.1. e II.3., intitolate «Ambito di applicazione della normativa generale» e «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.

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. 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. 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.

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.

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)

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») [83], 2001/29/CE, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione [84], 2004/48/CE, sul rispetto dei diritti di proprietà intellettuale [85], 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 delle medesime che entri in conflitto con detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come il principio di proporzionalità.

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.

[83] 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).

[84] 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).

[85] 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).

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.

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.

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.

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)

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 [86], 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 [87].

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.

[86] Articolo 8, paragrafo 1, della direttiva 95/46 e articolo 9, paragrafo 1, del regolamento 2016/679.
[87] Articolo 8, paragrafo 5, della direttiva 95/46 e articolo 10 del regolamento 2016/679.

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 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.

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 [88], 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 [89].

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.

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

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

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.

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

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 [90].

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 [91] 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

[90] Articolo 4, paragrafo 1, lettera a), della direttiva 95/46, e articolo 3, paragrafo 1, del regolamento 2016/679.
[91] Articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46, e articolo 17, paragrafo 1, del regolamento 2016/679.

attualmente previsti per quanto riguarda la portata di una deindicizzazione al di fuori dell'Unione.

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 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.

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.

Sentenza dell'8 dicembre 2022 (Grande Sezione), Google (Deindicizzazione di contenuti asseritamente inesatti) (C-460/20, EU:C:2022:962)

I ricorrenti nel procedimento principale, TU, che occupa posizioni di responsabilità e detiene partecipazioni in diverse società, e RE, che era la sua compagna e, fino a maggio 2015, procuratrice di una di dette società, sono stati oggetto di tre articoli pubblicati su un sito Internet nel 2015 dalla G LLC, gestore del sito Internet in questione. Tali articoli, uno dei quali era corredato di quattro fotografie dei ricorrenti che suggerivano che essi godessero di un tenore di vita lussuoso, presentavano in modo critico il modello di investimento di molte delle loro società. L'accesso a detti articoli poteva avvenire inserendo nel motore di ricerca gestito da Google LLC (in prosieguo: «Google»), i nomi e cognomi dei ricorrenti, sia isolatamente sia in combinazione con taluni nomi di società. L'elenco dei risultati rinviava ai suddetti articoli mediante un link e alle fotografie visualizzate sotto forma di miniature («thumbnails»).

I ricorrenti nel procedimento principale hanno chiesto a Google, in qualità di titolare del trattamento dei dati personali effettuato dal suo motore di ricerca, da un lato, di deindicizzare dall'elenco dei risultati di ricerca i link verso gli articoli di cui trattasi, in quanto essi conterrebbero affermazioni inesatte e opinioni diffamatorie, e, dall'altro, di

ritirare le miniature dall'elenco dei risultati della ricerca. Google si è rifiutata di dare seguito a tale richiesta.

A seguito del rigetto delle loro domande sia in primo grado che in appello, i ricorrenti nel procedimento principale hanno proposto dinanzi al Bundesgerichtshof (Corte federale di giustizia, Germania) un ricorso per cassazione («Revision»), nell'ambito del quale il Bundesgerichtshof ha sottoposto alla Corte una domanda pregiudiziale vertente sull'interpretazione del RGPD e della direttiva 95/46 [92].

Con la sua sentenza, pronunciata dalla Grande Sezione, la Corte sviluppa la propria giurisprudenza sulle condizioni applicabili alle domande di deindicizzazione rivolte al gestore di un motore di ricerca sulla base delle disposizioni in materia di protezione dei dati personali. In particolare, essa esamina, da un lato, la portata degli obblighi e delle responsabilità incombenti al gestore di un motore di ricerca nel trattare una domanda di deindicizzazione fondata sull'asserita inesattezza delle informazioni incluse nel contenuto indicizzato e, dall'altro, l'onere della prova gravante sull'interessato per quanto riguarda tale inesattezza. Essa si pronuncia, inoltre, sulla necessità, ai fini dell'esame di una domanda diretta all'eliminazione di fotografie visualizzate sotto forma di miniature nell'elenco dei risultati di una ricerca di immagini, di tener conto del contesto iniziale della pubblicazione delle suddette fotografie in Internet.

In primo luogo, la Corte dichiara che, nell'ambito del bilanciamento tra, da un lato, i diritti al rispetto della vita privata e alla protezione dei dati personali e, dall'altro, il diritto alla libertà di espressione e di informazione [93], ai fini dell'esame di una richiesta di deindicizzazione rivolta al gestore di un motore di ricerca e diretta ad ottenere l'eliminazione, dall'elenco dei risultati di una ricerca, del link verso un contenuto che include informazioni asseritamente inesatte, tale deindicizzazione non è subordinata alla condizione che la questione dell'esattezza del contenuto indicizzato sia stata risolta, almeno provvisoriamente, nel quadro di un'azione legale intentata dal richiedente contro il fornitore del contenuto.

In via preliminare, per esaminare a quali condizioni il gestore di un motore di ricerca sia tenuto ad accogliere una richiesta di deindicizzazione e quindi a cancellare dall'elenco dei risultati, visualizzato in esito ad una ricerca effettuata a partire dal nome dell'interessato, il link verso una pagina Internet contenente affermazioni che detta persona ritiene inesatte, la Corte ha ricordato anzitutto quanto segue:

• nei limiti in cui l'attività di un motore di ricerca può incidere, in modo significativo e in aggiunta all'attività degli editori di siti Internet, sui diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca in quanto soggetto che determina le finalità e gli strumenti di detta attività deve garantire, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che le

[92] Rispettivamente, l'articolo 17, paragrafo 3, lettera a), del RGPD e l'articolo 12, lettera b), e l'articolo 14, primo comma, lettera a), della direttiva 95/46.

[93] Diritti fondamentali garantiti, rispettivamente, dagli articoli 7, 8 e 11 della Carta.

garanzie previste dalla direttiva 95/46 e dal RGPD possano spiegare pienamente i loro effetti e che possa essere realizzata una tutela efficace e completa delle persone interessate;

• quando riceve una richiesta di deindicizzazione, il gestore di un motore di ricerca deve verificare se l'inserimento del link verso la pagina Internet in questione nell'elenco visualizzato sia necessario per l'esercizio del diritto alla libertà di informazione degli utenti di Internet potenzialmente interessati ad avere accesso a tale pagina Internet mediante una ricerca siffatta, tutelata dalla libertà di espressione e di informazione;

• il RGPD prevede espressamente il requisito del bilanciamento tra, da un lato, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali e, d'altro lato, il diritto fondamentale alla libertà di informazione.

La Corte osserva anzitutto che, sebbene i diritti al rispetto della vita privata e alla protezione dei dati personali dell'interessato prevalgano, di regola, sul legittimo interesse degli utenti di Internet ad avere accesso all'informazione in questione, tale equilibrio può nondimeno dipendere dalle circostanze rilevanti di ciascun caso, in particolare dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata dell'interessato, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica.

La questione dell'esattezza o meno del contenuto indicizzato costituisce altresì un elemento pertinente nell'ambito di detta valutazione. È così che, in taluni casi, il diritto all'informazione degli utenti di Internet e la libertà di espressione del fornitore di contenuti possono prevalere sui diritti alla protezione della vita personale e alla protezione dei dati personali, in particolare, quando l'interessato svolge un ruolo nella vita pubblica. Tuttavia, tale relazione è in ogni caso capovolta quando le informazioni oggetto della domanda di deindicizzazione, almeno per una parte che non abbia un carattere secondario rispetto alla totalità del contenuto, si rivelano inesatte. In un'ipotesi del genere, infatti, il diritto di informazione e il diritto di essere informati non possono essere presi in considerazione, poiché essi non possono includere il diritto di diffondere informazioni di tal genere e di avere accesso ad esse.

Per quanto riguarda poi, da un lato, gli obblighi concernenti l'accertamento dell'esattezza o meno delle informazioni presenti nel contenuto indicizzato, la Corte precisa che la persona che richiede la deindicizzazione per l'inesattezza di tali informazioni deve dimostrare l'inesattezza manifesta delle informazioni o, quanto meno, di una parte di tali informazioni che non abbia un carattere secondario rispetto alla totalità di tale contenuto. Tuttavia, al fine di evitare di far gravare su tale persona un onere eccessivo idoneo a minare l'effetto utile del diritto alla deindicizzazione, essa è tenuta unicamente a fornire gli elementi di prova che, tenuto conto delle circostanze del caso di specie, si può ragionevolmente richiedere a quest'ultima di ricercare. In linea di principio, tale persona non può essere tenuta a produrre, fin dalla fase precontenziosa,

a sostegno della sua richiesta di deindicizzazione, una decisione giurisdizionale ottenuta contro l'editore del sito Internet in questione, fosse pure in forma di decisione adottata in sede di procedimento sommario.

Dall'altro lato, per quanto riguarda gli obblighi e le responsabilità incombenti al gestore del motore di ricerca, la Corte sottolinea che quest'ultimo, al fine di verificare, a seguito di una richiesta di deindicizzazione, se un contenuto possa continuare ad essere incluso nell'elenco dei risultati delle ricerche effettuate mediante il suo motore di ricerca, deve fondarsi sull'insieme dei diritti e degli interessi in gioco nonché su tutte le circostanze del caso di specie. Tuttavia, detto gestore non può essere obbligato a indagare sui fatti e ad organizzare, a tal fine, uno scambio in contraddittorio con il fornitore di contenuto, diretto ad ottenere elementi mancanti riguardo all'esattezza del contenuto indicizzato. L'obbligo di contribuire all'accertamento della correttezza o meno del contenuto indicizzato farebbe gravare su tale gestore un onere che eccede quanto ci si può ragionevolmente da esso attendere alla luce delle sue responsabilità, competenze e possibilità. Tale soluzione comporterebbe un serio rischio che siano deindicizzati contenuti che rispondono ad una legittima e preponderante esigenza di informazione del pubblico e che divenga quindi difficile reperirli in Internet. Sussisterebbe così un rischio reale di effetto dissuasivo sull'esercizio della libertà di espressione e di informazione se un siffatto gestore procedesse a una deindicizzazione in modo pressoché sistematico, al fine di evitare di dover sopportare l'onere di indagare sui fatti pertinenti per accertare l'esattezza o meno del contenuto indicizzato.

Pertanto, nel caso in cui il soggetto che ha presentato una richiesta di deindicizzazione apporti elementi di prova atti a dimostrare il carattere manifestamente inesatto delle informazioni incluse nel contenuto indicizzato o, quantomeno, di una parte di tali informazioni che non abbia un carattere secondario rispetto alla totalità di tale contenuto, il gestore del motore di ricerca è tenuto ad accogliere detta richiesta. Lo stesso vale qualora detto richiedente apporti una decisione giudiziaria adottata nei confronti dell'editore del sito Internet e basata sulla constatazione che informazioni incluse nel contenuto indicizzato, che non hanno un carattere secondario rispetto alla totalità di quest'ultimo, sono, almeno a prima vista, inesatte. Per contro, nel caso in cui l'inesattezza di tali informazioni non appaia in modo manifesto alla luce degli elementi di prova forniti dall'interessato, il gestore del motore di ricerca non è tenuto, in mancanza di una decisione giudiziaria del genere, ad accogliere la richiesta di deindicizzazione. Qualora le informazioni di cui trattasi siano idonee a contribuire a un dibattito di interesse generale, occorre, alla luce di tutte le altre circostanze del caso di specie, attribuire un'importanza particolare al diritto alla libertà di espressione e di informazione.

La Corte aggiunge infine che, qualora il gestore di un motore di ricerca non dia seguito alla richiesta di deindicizzazione, l'interessato può adire l'autorità di controllo o l'autorità giudiziaria affinché queste effettuino le verifiche necessarie e ingiungano a tale gestore di adottare le misure che ne conseguono. A questo proposito, spetta segnatamente alle

autorità giudiziarie garantire la ponderazione degli interessi concorrenti, giacché esse si trovano nella posizione migliore per effettuare un bilanciamento complesso e approfondito, che tenga conto di tutti i criteri e di tutti gli elementi fissati dalla pertinente giurisprudenza.

In secondo luogo, la Corte dichiara che, nell'ambito del bilanciamento dei diritti fondamentali succitati, ai fini dell'esame di una richiesta di deindicizzazione diretta ad ottenere l'eliminazione, dai risultati di una ricerca di immagini effettuata a partire dal nome di una persona fisica, delle fotografie visualizzate sotto forma di miniature raffiguranti tale persona, occorre tener conto del valore informativo di tali fotografie indipendentemente dal contesto iniziale della loro pubblicazione nella pagina Internet da cui sono state tratte. Tuttavia, occorre prendere in considerazione qualsiasi elemento testuale che accompagna direttamente la visualizzazione di tali fotografie nei risultati della ricerca e che può apportare chiarimenti riguardo al loro valore informativo.

Per pervenire a tale conclusione, la Corte sottolinea che le ricerche di immagini effettuate mediante un motore di ricerca in Internet a partire dal nome di una persona sono soggette agli stessi principi applicabili alle ricerche di pagine Internet e alle informazioni ivi contenute. Essa osserva che la visualizzazione, a seguito di una ricerca per nome, sotto forma di miniature, di fotografie della persona interessata è atta a costituire un'ingerenza particolarmente significativa nei diritti alla tutela della vita privata e dei dati personali di tale persona.

Pertanto, il gestore di un motore di ricerca, quando riceve una richiesta di deindicizzazione diretta ad ottenere l'eliminazione, dai risultati di una ricerca di immagini effettuata a partire dal nome di una persona, delle fotografie visualizzate sotto forma di miniature che raffigurano tale persona, deve verificare se la visualizzazione delle fotografie in questione sia necessaria per l'esercizio del diritto alla libertà di informazione degli utenti di Internet potenzialmente interessati ad avere accesso a tali fotografie mediante una ricerca siffatta.

Orbene, poiché il motore di ricerca visualizza fotografie dell'interessato al di fuori del contesto nel quale esse sono pubblicate nella pagina Internet indicizzata, il più delle volte al fine di illustrare gli elementi testuali contenuti in tale pagina, occorre stabilire se debba essere nondimeno preso in considerazione tale contesto in sede del bilanciamento che va effettuato tra i diritti e gli interessi concorrenti. In tale ambito, la questione se detta valutazione debba includere anche il contenuto della pagina Internet in cui è inserita la fotografia di cui è chiesta l'eliminazione della visualizzazione sotto forma di miniatura dipende dall'oggetto del trattamento e dalla natura di cui trattasi.

Per quanto riguarda, in primo luogo, l'oggetto del trattamento di cui trattasi, la Corte rileva che la pubblicazione di fotografie come mezzo di comunicazione non verbale può avere un impatto più forte sugli utenti di Internet rispetto alle pubblicazioni testuali. Le fotografie sono infatti, in quanto tali, un mezzo importante per attirare l'attenzione degli utenti di Internet e possono suscitare un interesse ad accedere agli articoli che esse

illustrano. Orbene, a causa, in particolare, del fatto che esse si prestano spesso a varie interpretazioni, la loro visualizzazione quali miniature nell'elenco dei risultati della ricerca può comportare un'ingerenza particolarmente grave nel diritto della persona interessata alla protezione della sua immagine, circostanza che deve essere presa in considerazione nell'ambito del bilanciamento tra i diritti e gli interessi concorrenti. Si impone un bilanciamento distinto a seconda che siano in discussione, da un lato, articoli provvisti di fotografie pubblicate dall'editore della pagina Internet e che, inserite nel loro contesto di origine, illustrano le informazioni fornite in tali articoli e le opinioni ivi espresse e, dall'altro, fotografie visualizzate, sotto forma di miniature nell'elenco dei risultati, ad opera del gestore di un motore di ricerca al di fuori del contesto in cui esse sono state pubblicate nella pagina Internet originaria.

A tal proposito, la Corte ricorda che non soltanto il motivo che giustifica la pubblicazione di un dato personale in un sito Internet non coincide necessariamente con quello che si applica all'attività dei motori di ricerca, ma che, anche quando tale coincidenza sussista, il risultato del bilanciamento dei diritti e degli interessi in gioco che deve essere effettuato può divergere a seconda che si tratti del trattamento effettuato dal gestore di un motore di ricerca o di quello effettuato dall'editore di detta pagina Internet. Da un lato, i legittimi interessi che giustificano tali trattamenti possono essere diversi e, dall'altro, le conseguenze che tali trattamenti hanno per l'interessato, e segnatamente per la sua vita privata, non sono necessariamente le stesse.

Per quanto riguarda, in secondo luogo, la natura del trattamento effettuato dal gestore del motore di ricerca, la Corte constata che, reperendo le fotografie di persone fisiche pubblicate in Internet e visualizzandole separatamente, sotto forma di vignette, nei risultati di una ricerca di immagini, il gestore di un motore di ricerca offre un servizio che implica un trattamento di dati personali autonomo e distinto rispetto al trattamento effettuato dall'editore della pagina Internet da cui sono tratte le fotografie e dal trattamento, di cui tale gestore è parimenti responsabile, relativo all'indicizzazione di tale pagina.

Di conseguenza, è necessaria una valutazione autonoma dell'attività del gestore del motore di ricerca, consistente nel visualizzare i risultati di una ricerca di immagini, sotto forma di miniature, dato che la lesione aggiuntiva dei diritti fondamentali risultante da siffatta attività può essere particolarmente intensa a causa dell'aggregazione, in occasione di una ricerca per nome, di tutte le informazioni relative all'interessato che si trovano in Internet. Nell'ambito di tale valutazione autonoma, occorre tener conto del fatto che tale visualizzazione costituisce in sé il risultato perseguito dall'utente di Internet, indipendentemente dalla sua successiva decisione di accedere o meno alla pagina Internet originaria.

La Corte osserva, tuttavia, che siffatto specifico bilanciamento, che tiene conto della natura autonoma del trattamento effettuato dal gestore del motore di ricerca, non pregiudica l'eventuale pertinenza di elementi testuali che possono direttamente accompagnare la visualizzazione di una fotografia nell'elenco dei risultati di una ricerca,

dato che tali elementi possono fornire un chiarimento sul valore informativo di tale fotografia per il pubblico e, pertanto, influire sul bilanciamento dei diritti e degli interessi in gioco.

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

Sentenza del 1º ottobre 2019 (Grande Sezione), Planet49 (C-673/17, EU:C:2019:801)

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 [94], letta in combinato disposto con la direttiva 95/46/CE [95], nonché con il RGPD [96].

In primo luogo, la Corte ha osservato che l'articolo 2, lettera h), della direttiva 95/46/CE, 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

[94] 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).
[95] Articolo 2, lettera h), della direttiva 95/46.
[96] Articolo 6, paragrafo 1, lettera a), del regolamento 2016/679.

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 [97], 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.

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.

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.

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.

5. Trattamento dei dati personali sui social network online

Sentenza del 4 luglio 2023 (Grande Sezione), Meta Platforms e a. (Condizioni generali di utilizzo di un social network) (C-252/21, EU:C:2023:537)

La società Meta Platforms è proprietaria del social network online «Facebook», il quale è gratuito per gli utenti privati. Il modello economico di tale social network si basa sul

[97] *Idem*.

finanziamento attraverso la pubblicità online, che viene effettuata su misura per i suoi singoli utenti. Il presupposto tecnico per questo tipo di pubblicità è la creazione automatizzata di profili dettagliati degli utenti del network e dei servizi online offerti a livello del gruppo Meta. Pertanto, per poter utilizzare detto social network, gli utenti devono, al momento della loro iscrizione, accettare le condizioni generali stabilite da Meta Platforms, che rinviano alle regole sull'uso dei dati e dei marcatori (cookies) adottate da tale società. In forza di queste ultime, oltre ai dati che tali utenti forniscono direttamente all'atto della loro iscrizione, Meta Platforms raccoglie anche i dati riferiti alle attività di detti utenti all'interno e all'esterno del social network e li mette in relazione con gli account Facebook degli utenti interessati. Per quanto riguarda i dati da ultimo menzionati, denominati anche «dati *off* Facebook», si tratta, da un lato, dei dati concernenti la consultazione di pagine Internet e di applicazioni di terzi e, dall'altro, dei dati riguardanti l'utilizzo di altri servizi online appartenenti al gruppo Meta (fra i quali Instagram e WhatsApp). Il quadro generale dei dati così raccolti consente di trarre conclusioni dettagliate sulle preferenze e sugli interessi dei medesimi utenti.

Con decisione del 6 febbraio 2019, il Bundeskartellamt (autorità federale garante della concorrenza, Germania) ha vietato a Meta Platforms, da un lato, di subordinare, nelle condizioni generali a quell'epoca vigenti, l'uso del social network Facebook da parte di utenti privati residenti in Germania al trattamento dei loro dati off Facebook e, dall'altro, di procedere, senza il loro consenso, al trattamento di tali dati. Inoltre, l'autorità federale garante della concorrenza le ha imposto di adeguare tali condizioni generali, in modo tale che da esse risulti in modo chiaro che detti dati non saranno raccolti, messi in relazione con gli account degli utenti Facebook e utilizzati senza il consenso degli utenti interessati. Infine, tale autorità ha sottolineato che un siffatto consenso non era valido quando costituiva una condizione per l'utilizzo del social network. Essa ha motivato la sua decisione con il fatto che il trattamento dei dati in questione, che non sarebbe conforme al RGPD, costituirebbe uno sfruttamento abusivo della posizione dominante di Meta Platforms sul mercato dei social network online.

Meta Platforms ha presentato un ricorso dinanzi all'Oberlandesgericht Düsseldorf (Tribunale superiore del Land, Düsseldorf, Germania). Nutrendo dubbi, in particolare, in ordine all'interpretazione e all'applicazione di talune disposizioni del RGPD, il Tribunale superiore del Land, Düsseldorf, ha adito la Corte in via pregiudiziale.

Con la sua sentenza, la Corte, riunita in Grande Sezione, fornisce talune precisazioni sulla possibilità del trattamento, da parte di un operatore di un social network, di dati personali «sensibili» dei suoi utenti, sui presupposti di liceità del trattamento dei dati effettuato da un tale operatore nonché sulla validità del consenso, prestato ai fini di un simile trattamento da parte di detti utenti a un'impresa in posizione dominante sul mercato nazionale dei social network online.

Per quanto riguarda, segnatamente, il trattamento di categorie particolari di dati personali [98], la Corte considera che, nel caso in cui un utente di un social network online consulti siti Internet o applicazioni relative a una o più di tali categorie e, se del caso, vi inserisca dati iscrivendosi o effettuando ordini online, il trattamento di dati personali da parte dell'operatore di tale social network online [99] debba essere considerato un «trattamento di categorie particolari di dati personali», ai sensi dell'articolo 9, paragrafo 1, del RGPD, qualora consenta di rivelare informazioni rientranti in una di tali categorie particolari, indipendentemente dal fatto che tali informazioni riguardino un utente di tale social network o qualsiasi altra persona fisica. Un trattamento di dati di questo tipo è in linea di principio vietato, fatte salve talune deroghe [100].

A quest'ultimo riguardo, la Corte precisa che un utente di un social network online, allorché consulta siti Internet oppure applicazioni correlati a una o più delle suddette categorie particolari di dati, non rende manifestamente pubblici [101] i dati relativi a tale consultazione, raccolti dall'operatore di detto social network online mediante cookie o simili tecnologie di registrazione. Inoltre, quando inserisce dati in tali siti Internet o applicazioni nonché quando attiva pulsanti di selezione integrati in questi ultimi, come i pulsanti «Mi piace» o «Condividi» o i pulsanti che consentono all'utente di identificarsi su tali siti o applicazioni utilizzando gli identificativi di connessione collegati al suo account di utente del social network, il suo numero di telefono o il suo indirizzo di posta elettronica, tale utente rende manifestamente pubblici i dati così inseriti o risultanti dall'attivazione di tali pulsanti soltanto se abbia esplicitamente espresso preliminarmente, se del caso sulla base di un'impostazione individuale di parametri effettuata con piena cognizione di causa, la sua scelta di rendere i dati che lo riguardano pubblicamente accessibili a un numero illimitato di persone.

Per quanto riguarda, più in generale, i presupposti di liceità di un trattamento di dati personali, la Corte ricorda che, in forza del RGPD, il trattamento di dati è lecito se, e nella misura in cui, l'interessato vi ha acconsentito per una o più finalità specifiche [102]. In mancanza di un siffatto consenso, o qualora tale consenso non sia stato espresso in modo libero, specifico, informato e inequivocabile, un trattamento di questo tipo è

---

98 Previste all'articolo 9, paragrafo 1, del RGPD. Tale disposizione prevede che «è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

99 Tale trattamento, da parte di detto operatore, consiste nel raccogliere, tramite interfacce integrate, cookie o simili tecnologie di registrazione, dati risultanti dalla consultazione di tali siti e di tali applicazioni nonché dati inseriti dall'utente, nel mettere in relazione l'insieme di tali dati con l'account del social network di quest'ultimo e nell'utilizzare detti dati.

100 Previste all'articolo 9, paragrafo 2, del RGPD. Tale disposizione enuncia quanto segue: «[i]l paragrafo 1 non si applica se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; (...)

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

(...)».

101 Ai sensi dell'articolo 9, paragrafo 2, del RGPD.

102 Ai sensi dell'articolo 6, paragrafo 1, primo comma, lettera a), del RGPD.

nondimeno giustificato qualora soddisfi uno dei requisiti di necessità [103], che devono essere interpretati in maniera restrittiva. Orbene, il trattamento di dati personali dei suoi utenti effettuato da un operatore di un social network online può essere considerato necessario all'esecuzione del contratto di cui tali utenti sono parti solo a condizione che tale trattamento sia oggettivamente indispensabile per realizzare una finalità facente parte integrante della prestazione contrattuale destinata a detti utenti, in modo tale che l'oggetto principale del contratto non potrebbe essere raggiunto in assenza di tale trattamento.

Inoltre, secondo la Corte, il trattamento di dati di cui è causa può essere considerato necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi solo a condizione che il suddetto operatore abbia indicato agli utenti presso i quali i dati sono stati raccolti un legittimo interesse perseguito dal loro trattamento, che tale trattamento sia effettuato entro i limiti di quanto strettamente necessario alla realizzazione di tale legittimo interesse e che dal contemperamento dei contrapposti interessi, alla luce di tutte le circostanze pertinenti, risulti che le libertà e i diritti fondamentali e gli interessi di tali utenti non prevalgono su detto legittimo interesse del titolare del trattamento o di terzi. Orbene, la Corte considera in particolare che, in mancanza di un loro consenso, gli interessi e i diritti fondamentali di detti utenti prevalgono sull'interesse dell'operatore di un social network online alla personalizzazione della pubblicità mediante la quale esso finanzia la propria attività.

Infine, la Corte precisa che il trattamento di dati di cui trattasi è giustificato allorché è effettivamente necessario per adempiere un obbligo legale al quale il titolare del trattamento è soggetto, in forza di una disposizione del diritto dell'Unione o del diritto dello Stato membro interessato, che tale base giuridica risponde ad un obiettivo di interesse pubblico ed è proporzionata all'obiettivo legittimo perseguito e che tale trattamento è effettuato nei limiti dello stretto necessario.

Per quanto riguarda la validità del consenso degli utenti interessati dal trattamento dei loro dati in forza del RGPD, la Corte ricorda che la circostanza che l'operatore di un social network online occupi una posizione dominante sul mercato dei social network online non osta, di per sé, a che gli utenti di tale social network possano validamente acconsentire al trattamento dei loro dati personali effettuato da tale operatore. Tuttavia, dato che una siffatta posizione può incidere sulla libertà di scelta di tali utenti e creare uno squilibrio manifesto tra questi ultimi e detto operatore, essa costituisce un elemento importante per determinare se il consenso sia stato effettivamente prestato

[103] Menzionate all'articolo 6, paragrafo 1, primo comma, lettere da b) a f), del RGPD. In forza di tali disposizioni, il trattamento è lecito solo se, e nei limiti in cui, tra l'altro, è necessario per l'esecuzione di un contratto di cui l'interessato è parte [articolo 6, paragrafo 1, primo comma, lettera b), del RGPD], per adempiere un obbligo legale al quale il titolare del trattamento è soggetto [articolo 6, paragrafo 1, primo comma, lettera c), del RGPD] o per il perseguimento dei legittimi interessi perseguiti dal titolare del trattamento o di terzi [articolo 6, paragrafo 1, primo comma, lettera f), del RGPD].

validamente e, in particolare, liberamente, circostanza che spetta al medesimo operatore dimostrare [104].

In particolare, gli utenti del social network in questione devono disporre della libertà di rifiutare individualmente, nell'ambito della procedura contrattuale, di prestare il loro consenso a operazioni particolari di trattamento di dati non necessarie all'esecuzione del contratto, senza essere per questo tenuti a rinunciare integralmente alla fruizione di detto social network online, il che implica che a detti utenti venga proposta, se del caso a fronte di un adeguato corrispettivo, un'alternativa equivalente non accompagnata da simili operazioni di trattamento di dati. Inoltre, deve essere possibile fornire un consenso distinto per il trattamento dei dati off Facebook.

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)

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 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.

[104] In forza dell'articolo 7, paragrafo 1, del RGPD.

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.

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.

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.

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.

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.

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

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.

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.

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 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.

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

Sentenza del 1º ottobre 2015, Weltimmo (C-230/14, EU:C:2015:639)

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.

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. 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.

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.

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.

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.

Sentenza del 5 giugno 2018 (Grande Sezione), Wirtschaftsakademie Schleswig-Holstein (C-210/16, 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).

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.

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 [105] 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 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 causa in argomento. 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 [106] 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

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

[106] 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».

irlandese per la protezione dei dati sarebbe competente ad intentare un'azione inibitoria, sotto il controllo dei giudici irlandesi.

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 [107], pur non essendo l'autorità di controllo capofila per tale trattamento.

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 [108].

Infatti, per i trattamenti transfrontalieri, il RGPD prevede il meccanismo dello «sportello unico» [109], 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 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 [110], mentre la competenza delle altre autorità nazionali di controllo ad adottare una siffatta decisione, anche in via provvisoria, costituisce l'eccezione [111]. 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.

[107] Ai sensi dell'articolo 4, punto 23, del RGPD.
[108] Previste agli articoli 56 e 60 del RGPD.
[109] Articolo 56, paragrafo 1, del RGPD.
[110] Articolo 60, paragrafo 7, del RGPD.
[111] L'articolo 56, paragrafo 2, e l'articolo 66 del RGPD stabiliscono le eccezioni al principio della competenza decisionale dell'autorità di controllo capofila.

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 [112] 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.

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 [113] 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 [114], il che presuppone che il titolare del trattamento o il responsabile del trattamento transfrontaliero disponga di uno stabilimento nel territorio dell'Unione.

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 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.

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

---

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

[113] In forza dell'articolo 58, paragrafo 5, del RGPD.

[114] 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».

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.

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.

Sentenza del 16 gennaio 2024 (Grande Sezione), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

In tale causa (v. altresì la rubrica II.1., intitolata «Ambito di applicazione della normativa generale»), la Corte rileva che le disposizioni del RGPD relative alla competenza delle autorità di controllo nazionali e al diritto di reclamo [115] non richiedono l'adozione di misure nazionali di attuazione e sono sufficientemente chiare, precise e non condizionate per produrre un effetto diretto. Ne consegue che, sebbene il RGPD lasci agli Stati membri un margine di discrezionalità quanto al numero di autorità di controllo da istituire [116], esso fissa, per contro, la portata della loro competenza per sorvegliare l'applicazione del RGPD. Pertanto, nel caso in cui uno Stato membro decida di istituire un'unica autorità di controllo nazionale, quest'ultima è necessariamente dotata di tutte le competenze previste da tale regolamento. Qualsiasi diversa interpretazione rimetterebbe in questione l'effetto utile di tali disposizioni e rischierebbe di ridurre l'effetto utile di tutte le altre disposizioni del RGPD che possano essere oggetto di un reclamo.

Per quanto riguarda la circostanza che le disposizioni nazionali di rango costituzionale escludono la possibilità per un'autorità di controllo che dipende dal potere esecutivo di sorvegliare l'applicazione del RGPD da parte di un organo che rientra nel potere legislativo, la Corte sottolinea che è proprio nel rispetto della struttura costituzionale degli Stati membri che il RGPD si limita ad esigere che questi ultimi istituiscano almeno un'autorità di controllo, offrendo loro al contempo la possibilità di istituirne varie. Tale

[115] Rispettivamente, l'articolo 55, paragrafo 1, e l'articolo 77, paragrafo 1, del RGPD.
[116] Conformemente all'articolo 51, paragrafo 1, del RGPD.

regolamento riconosce quindi a ciascuno Stato membro un margine di discrezionalità che consente ad ognuno di essi di istituire tante autorità di controllo quante ne esiga, in particolare, la sua struttura costituzionale.

Inoltre, il fatto che uno Stato membro invochi disposizioni di diritto nazionale non può pregiudicare l'unità e l'efficacia del diritto dell'Unione. Infatti, gli effetti derivanti dal principio del primato del diritto dell'Unione si impongono a tutti gli organi di uno Stato membro, senza che, in particolare, le disposizioni interne, ivi comprese quelle di rango costituzionale, possano opporvisi.

Pertanto, qualora uno Stato membro abbia scelto di istituire un'unica autorità di controllo, esso non può invocare disposizioni di diritto nazionale, quand'anche di rango costituzionale, al fine di sottrarre trattamenti di dati personali rientranti nell'ambito di applicazione del RGPD al controllo di tale autorità.

4. Condizioni per infliggere sanzioni amministrative pecuniarie

Sentenza del 5 dicembre 2023 (Grande Sezione), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

In tale sentenza (v. altresì le rubriche II.3., II.5. e II.6., intitolate «Nozione di "trattamento di dati personali"», «Nozione di "responsabile del trattamento di dati personali"» e «Nozione di "contitolare del trattamento di dati personali"»), la Corte constata che, ai sensi dell'articolo 83 del RGPD, una sanzione amministrativa pecuniaria può essere irrogata ad un titolare del trattamento solo qualora sia accertato che questi ha commesso, con dolo o colpa, una violazione delle regole contenute in tale regolamento [117].

A tal riguardo, essa precisa che il legislatore dell'Unione non ha lasciato agli Stati membri un margine discrezionale per quanto riguarda le condizioni sostanziali che devono essere rispettate da un'autorità di controllo quando quest'ultima decide di infliggere ad un titolare del trattamento una sanzione amministrativa pecuniaria in forza di tale disposizione. Il fatto che il RGPD offra agli Stati membri la possibilità di stabilire eccezioni in relazione alle autorità pubbliche e agli organismi pubblici stabiliti nel loro territorio [118] e requisiti relativi alla procedura che le autorità di controllo devono seguire nell'irrogare una sanzione amministrativa pecuniaria [119] non significa in alcun modo che tali Stati possano anche stabilire siffatte condizioni sostanziali.

[117] Violazione di cui all'articolo 83, paragrafi da 4 a 6.

[118] Ai sensi dell'articolo 83, paragrafo 7, del RGPD «(...) ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro».

[119] Ai sensi dell'articolo 83, paragrafo 8, del RGPD, letto alla luce del considerando 129 di tale regolamento.

Per quanto riguarda tali condizioni, la Corte rileva che tra gli elementi enumerati nel RGPD in base ai quali l'autorità di controllo infligge una sanzione amministrativa pecuniaria al titolare del trattamento compare «il carattere doloso o colposo della violazione» [120]. Invece, nessuno di tali elementi indica una qualsiasi possibilità che il titolare del trattamento sia considerato responsabile in assenza di un suo comportamento colpevole. Per contro, nessuno di tali elementi menziona una qualsivoglia possibilità che la responsabilità del titolare del trattamento sorga in assenza di un suo comportamento colpevole. Pertanto, solo le violazioni delle disposizioni del RGPD commesse dal titolare del trattamento con dolo o con colpa possono condurre all'irrogazione a quest'ultimo di una sanzione amministrativa pecuniaria in applicazione dell'articolo 83 di tale regolamento.

La Corte aggiunge che tale interpretazione è corroborata dall'economia e dalla finalità del RGPD. In tale contesto, essa precisa che l'esistenza di un sistema di sanzioni ai sensi del RGPD, che permette di infliggere una sanzione amministrativa pecuniaria, quando le circostanze specifiche di ciascun caso lo giustificano, crea, per i titolari del trattamento e i responsabili del trattamento, un incentivo a conformarsi a tale regolamento e che, per il loro effetto dissuasivo, le sanzioni amministrative pecuniarie contribuiscono a rafforzare la protezione degli interessati. Tuttavia, il legislatore dell'Unione non ha ritenuto necessario prevedere l'irrogazione di sanzioni amministrative pecuniarie in assenza di colpa. Tenuto conto del fatto che il RGPD mira ad un livello di protezione nel contempo equivalente e omogeneo e che, a tal fine, deve essere applicato in modo coerente in tutta l'Unione, sarebbe contrario a tale finalità permettere agli Stati membri di prevedere un regime di tal genere di irrogazione di una sanzione pecuniaria.

Inoltre, la Corte conclude che una sanzione pecuniaria siffatta può essere inflitta a un titolare del trattamento in relazione a operazioni di trattamento di dati personali effettuate per suo conto da un responsabile del trattamento, salvo che, nell'ambito di tali operazioni, detto responsabile del trattamento abbia effettuato trattamenti per finalità che gli sono proprie o abbia trattato tali dati in modo incompatibile con il quadro o le modalità del trattamento quali erano stati determinati dal titolare del trattamento o in modo tale che non si può ragionevolmente ritenere che tale titolare abbia a ciò acconsentito. In tal caso il responsabile del trattamento deve essere considerato titolare di un trattamento del genere.

Sentenza del 5 dicembre 2023 (Grande Sezione), Deutsche Wohnen (C-807/21, EU:C:2023:950)

La Deutsche Wohnen SE (in prosieguo: la «DW») è una società immobiliare che detiene indirettamente, tramite partecipazioni in diverse società, numerose unità commerciali e abitative. Essa tratta, nell'ambito delle sue attività commerciali, i dati personali dei locatari di tali unità.

[120] Articolo 83, paragrafo 2, lettera b), del RGPD.

A seguito di due controlli effettuati nel 2017 e nel 2019, la Berliner Beauftragte für den Datenschutz (autorità di controllo di Berlino, Germania) ha constatato una serie di violazioni del RGPD commesse dalla DW. Con decisione del 30 ottobre 2019, detta autorità di controllo le ha inflitto talune sanzioni pecuniarie amministrative a tale titolo.

La DW ha proposto ricorso avverso detta decisione dinanzi al Landgericht Berlin (Tribunale del Land di Berlino, Germania), il quale ha archiviato il procedimento. Tale tribunale ha rilevato che, in forza della legge tedesca [121], un illecito amministrativo potrebbe essere constatato solo nei confronti di una persona fisica e non nei confronti di una persona giuridica. Inoltre, nel caso di un coinvolgimento della responsabilità di una persona giuridica, a questa potrebbero essere imputati solo gli atti dei membri dei suoi organi o dei suoi rappresentanti. La Staatsanwaltschaft Berlin (procura di Berlino, Germania) ha proposto ricorso avverso tale decisione dinanzi al Kammergericht Berlin (Tribunale superiore del Land di Berlino, Germania). In tale contesto, detto giudice ha adito la Corte in via pregiudiziale in merito all'interpretazione del RGPD.

Nella sua sentenza la Corte, riunita in Grande Sezione, si pronuncia sulle condizioni per infliggere sanzioni amministrative pecuniarie ai sensi del RGPD. In primo luogo, essa esamina la questione se gli Stati membri possano subordinare l'irrogazione di una sanzione amministrativa pecuniaria ad una persona giuridica alla condizione che la violazione di tale regolamento sia previamente imputata a una persona fisica identificata. In secondo luogo, in linea con la sentenza Nacionalinis visuomenės sveikatos centras (v. *supra*), essa si sofferma anche sulla questione se la violazione delle disposizioni del RGPD sanzionata debba essere commessa con dolo o colpa.

Per quanto riguarda l'imposizione di una sanzione pecuniaria amministrativa in forza del RGPD a una persona giuridica, la Corte rileva, anzitutto, che i principi, i divieti e gli obblighi stabiliti dal RGPD si rivolgono, in particolare, ai «titolari del trattamento» la cui responsabilità si estende a qualsiasi trattamento di dati personali effettuato direttamente o che altri abbiano effettuato per loro conto. È tale responsabilità che, in caso di violazioni delle disposizioni del RGPD, costituisce il fondamento per l'irrogazione di una sanzione amministrativa pecuniaria al titolare del trattamento ai sensi dell'articolo 83 di tale regolamento. Tuttavia, il legislatore dell'Unione non ha operato, ai fini della determinazione di siffatta responsabilità, una distinzione tra persone fisiche e persone giuridiche; tale responsabilità è subordinata all'unica condizione che queste, da sole o insieme ad altri, determinino le finalità e gli strumenti del trattamento di dati personali [122]. Pertanto, in linea di principio, ogni persona che soddisfi la suindicata condizione è responsabile, in particolare, per qualsiasi violazione del RGPD, commessa dalla stessa o per suo conto. Ciò implica, da un lato, che le persone giuridiche sono responsabili non solo delle violazioni commesse dai loro rappresentanti, dirigenti o

[121] Gesetz über Ordnungswidrigkeiten (legge in materia di infrazioni amministrative), del 24 maggio 1968 (BGBl. 1968 I, pag. 481), nella versione di cui alla comunicazione del 19 febbraio 1987 (BGBl. 1987 I, pag. 602), quale adattata dalla legge del 19 giugno 2020 (BGBl. 2020 I, pag. 1350).

[122] Ai sensi dell'articolo 4, punto 7, del RGPD.

amministratori, ma anche da qualsiasi altra persona che agisca nell'ambito dell'attività commerciale di tali persone giuridiche e per loro conto. Dall'altro, le sanzioni amministrative pecuniarie previste dal RGPD in caso di siffatte violazioni devono poter essere inflitte direttamente alle persone giuridiche ove queste possano essere qualificate come titolari del trattamento.

Poi, la Corte osserva che nessuna disposizione del RGPD consente di ritenere che l'irrogazione di una sanzione amministrativa pecuniaria a una persona giuridica, in quanto titolare del trattamento, sia subordinata alla previa constatazione che tale violazione sia stata commessa da una persona fisica identificata. Inoltre, il legislatore dell'Unione non ha lasciato agli Stati membri un margine di discrezionalità al riguardo. Il fatto che il RGPD conceda a questi ultimi la facoltà di prevedere requisiti relativi alla procedura che le autorità di controllo devono seguire per infliggere una sanzione amministrativa pecuniaria [123] non significa affatto che essi siano parimenti autorizzati a prevedere condizioni sostanziali supplementari rispetto a quelle stabilite dal RGPD.

In tale contesto, la Corte precisa che consentire agli Stati membri di richiedere unilateralmente e quale condizione necessaria per imporre una sanzione pecuniaria amministrativa, ai sensi dell'articolo 83 del RGPD, a un titolare del trattamento che sia una persona giuridica, che la violazione in questione sia previamente imputata o imputabile a una persona fisica identificata sarebbe contrario alla finalità del RGPD. Inoltre, un siffatto requisito supplementare rischierebbe, in definitiva, di indebolire l'efficacia e l'effetto dissuasivo delle sanzioni amministrative pecuniarie inflitte a persone giuridiche in quanto titolari del trattamento.

Infine, la Corte sottolinea che la nozione di «impresa», ai sensi degli articoli 101 e 102 TFUE [124], non incide sulla questione se e a quali condizioni una sanzione amministrativa pecuniaria possa essere inflitta in forza del RGPD a un titolare del trattamento che sia una persona giuridica ed assume rilievo solo in sede di determinazione dell'importo della sanzione.

Pertanto, la Corte conclude che il RGPD [125] osta a una normativa nazionale in forza della quale una sanzione amministrativa pecuniaria può essere inflitta a una persona giuridica, nella sua qualità di titolare del trattamento, per una violazione di detto regolamento [126] solo a condizione che tale violazione sia stata previamente imputata a una persona fisica identificata.

Per quanto riguarda la questione se gli Stati membri possano prevedere l'imposizione di una sanzione amministrativa pecuniaria anche qualora la violazione sanzionata non sia stata commessa con dolo o colpa, la Corte ricorda, anzitutto, che le condizioni sostanziali che un'autorità di controllo deve soddisfare nell'infliggere una simile sanzione a un

123 Come risulta dall'articolo 58, paragrafo 4, e dall'articolo 83, paragrafo 8, del RGPD, letti alla luce del suo considerando 129.
124 Cui rinvia il considerando 150 del RGPD.
125 Articolo 58, paragrafo 2, lettera i), e articolo 83, paragrafi da 1 a 6, del RGPD.
126 Di cui all'articolo 83, paragrafi da 4 a 6, del RGPD.

titolare del trattamento ricadono esclusivamente nel diritto dell'Unione e che gli Stati membri non dispongono di alcun margine di manovra al riguardo. Seguendo un ragionamento identico a quello adottato nella summenzionata sentenza Nacionalinis visuomenės sveikatos centras, la Corte dichiara che, in forza dell'articolo 83 del RGPD, una sanzione amministrativa pecuniaria può essere inflitta solo qualora venga accertato che il titolare del trattamento, che sia al contempo una persona giuridica e un'impresa, ha commesso, con dolo o colpa, una violazione delle norme contenute in tale regolamento.

5. Articolazione delle competenze delle autorità nazionali di controllo con le competenze delle altre autorità nazionali

Sentenza del 4 luglio 2023 (Grande Sezione), Meta Platforms e a. (Condizioni generali di utilizzo di un social network) (C-252/21, EU:C:2023:537)

In tale sentenza (v. altresì la rubrica V.5., intitolata «Trattamento dei dati personali sui social network online»), pronunciandosi sulla competenza di un'autorità garante della concorrenza a constatare la non conformità al RGPD di un trattamento di dati personali, la Corte considera che – fermo restando il rispetto del suo obbligo di leale cooperazione [127] con le autorità di controllo della protezione dei dati – una tale autorità può constatare, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa [128], che le condizioni generali d'uso fissate da tale impresa in materia di trattamento dei dati personali e la loro applicazione non sono conformi a detto regolamento, qualora tale constatazione sia necessaria per accertare l'esistenza di un tale abuso. Tuttavia, quando un'autorità garante della concorrenza rileva una violazione del RGPD nell'ambito della constatazione di un abuso di posizione dominante, essa non si sostituisce alle autorità di controllo.

Pertanto, alla luce del principio di leale cooperazione, laddove siano chiamate, nell'esercizio delle loro competenze, ad esaminare la conformità di un comportamento di un'impresa alle disposizioni del RGPD, le autorità garanti della concorrenza devono concertarsi e cooperare lealmente con le autorità nazionali di controllo interessate o con l'autorità di controllo capofila. Tutte queste autorità sono quindi tenute a conformarsi ai loro rispettivi poteri e competenze, così che gli obblighi derivanti dal RGPD nonché gli obiettivi di tale regolamento siano rispettati e il loro effetto utile sia preservato. Ne consegue che qualora, nell'ambito dell'esame diretto a constatare un abuso di posizione dominante da parte di un'impresa, un'autorità nazionale garante della concorrenza ritenga che sia necessario esaminare la conformità di un comportamento di tale

[127] Sancito all'articolo 4, paragrafo 3, TUE.
[128] Ai sensi dell'articolo 102 TFUE.

impresa alle disposizioni del RGPD, detta autorità deve verificare se tale comportamento o un comportamento simile sia già stato oggetto di una decisione da parte dell'autorità nazionale di controllo competente o dell'autorità di controllo capofila o, ancora, della Corte. Se così fosse, l'autorità nazionale garante della concorrenza non potrebbe discostarsene, pur restando libera di trarne le proprie conclusioni sotto il profilo dell'applicazione del diritto della concorrenza.

Laddove nutra dubbi sulla portata della valutazione effettuata dall'autorità nazionale di controllo competente o dall'autorità di controllo capofila, laddove il comportamento di cui trattasi o un comportamento simile sia, al contempo, oggetto di esame da parte di tali autorità, o ancora laddove, in assenza di un'indagine di dette autorità, ritenga che un comportamento di un'impresa non sia conforme alle disposizioni del RGPD, l'autorità nazionale garante della concorrenza deve consultare tali autorità e chiederne la cooperazione, al fine di fugare i propri dubbi o di determinare se si debba attendere l'adozione di una decisione da parte dell'autorità di controllo interessata prima di iniziare la propria valutazione. In assenza di obiezioni o di risposta di queste ultime entro un termine ragionevole, l'autorità nazionale garante della concorrenza può proseguire la propria indagine.

CORTE DI GIUSTIZIA
DELL'UNIONE EUROPEA

Direzione della Ricerca e documentazione

Luglio 2024