Manuale breve su

LA PROTEZIONE DEI DATI NEL DIRITTO INTERNAZIONALE ED EUROPEO: IL RUOLO DELLE CORTI NAZIONALI NELL'APPLICAZIONE DELLA CARTA DEI DIRITTI FONDAMENTALI

PROGETTO "E-LEARNING NATIONAL ACTIVE CHARTER TRAINING (E-NACT)"

CO-FINANZIATO DAL PROGRAMMA "DIRITTI FONDAMENTALI E CITTADINANZA" DELLA COMMISSIONE EUROPEA

Il presente manuale è stato redatto da:

Elena Carpanelli
Alessandra Favi
Marco Inglese
Laura Pineschi

INDICE

1. Introduzione

L'esigenza di regole certe nella protezione dei dati personali è sempre più sentita a livello internazionale; purtroppo, però, il quadro giuridico complessivo si presenta frammentario e la prassi degli Stati non è ancora sufficientemente ampia e uniforme.

Il presente manuale intende offrire una panoramica della regolamentazione internazionale ed europea e dei più recenti sviluppi giurisprudenziali in materia. A tal fine, dopo una sintetica ricostruzione dei principali strumenti giuridici a livello universale e regionale rilevanti in materia di protezione dei dati personali, specifica attenzione sarà dedicata alla Carta dei diritti fondamentali dell'Unione europea e alla sua interpretazione e applicazione da parte della Corte di giustizia dell'Unione europea.

Tenuto conto del sempre più avanzato sistema multilivello di tutela dei diritti umani, questo manuale esplora tecniche di interazione tra corti nazionali e sovranazionali e il ruolo degli operatori giuridici nell'applicazione della Carta.

Nel prosieguo della trattazione, l'espressione "protezione dei dati personali" è intesa in senso ampio, ricomprendendo anche forme di tutela della riservatezza dell'individuo.

2. Il quadro giuridico internazionale: la regolamentazione a livello universale

A livello globale, non esiste un trattato multilaterale in materia di protezione dei dati. Considerato l'impatto delle nuove tecnologie sulle libertà personali, alcuni elementi essenziali di tutela sono stati ricavati dagli strumenti internazionali per la protezione dei diritti umani che enunciano, tra l'altro, il divieto di interferenze arbitrarie nella vita privata. Fra questi rientrano:

- la **Dichiarazione universale dei diritti umani (New York, 10 dicembre 1948)**[1], ove si afferma, all'art. 12 che:

  "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks";

- il **Patto internazionale sui diritti civili e politici (New York, 16 dicembre 1966**), entrato in vigore il 23 marzo 1976. Ai sensi dell'art. 17:

  "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
  2. Everyone has the right to the protection of the law against such interference or attacks".

Con la pubblicazione del *General Comment* n. 16 del 1988[2], il Comitato dei diritti umani ha interpretato l'art. 17 del Patto in modo tale da includere alcune garanzie a tutela dei dati personali. In particolare, è stato precisato che limitazioni del diritto alla *privacy* sono ammissibili qualora la raccolta delle informazioni relative alla vita privata degli individui sia da ritenersi di interesse

[1] Sulla natura giuridica dei diritti enunciati nella Dichiarazione universale, v. PINESCHI, *La tutela internazionale dei diritti umani. Norme, garanzie, prassi*, Milano, 2015, p. 71 ss.
[2] UN Doc. HRI/GEN/1/Rev.9, vol. I dell'8 aprile 1988.

essenziale per la società (par. 8). Occorre, però, che la raccolta e la conservazione dei dati personali sia disciplinata a livello legislativo. Si auspica, inoltre, che ogni individuo possa ottenere la rettifica o l'eliminazione dei dati che contengono informazioni non corrette o raccolte in violazione delle norme vigenti:

> "The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination" (par. 10).

Nell'ambito delle Nazioni Unite, non sono comunque mancati tentativi volti a indirizzare la condotta degli Stati verso il rispetto di alcune regole essenziali. In particolare, nel 1989, l'Assemblea generale ha approvato le c.d. *Linee guida per la regolamentazione dei* files *contenenti dati a carattere personale*[3], ove si precisano alcune garanzie minimali che dovrebbero essere presenti nelle legislazioni nazionali.

Più di recente, l'Assemblea generale, preoccupata per l'impatto che misure di sicurezza nazionale volte, prevalentemente, a contrastare il fenomeno del terrorismo, possono avere sul diritto alla vita privata, ha invitato l'Alto Commissario per i diritti umani a redigere un rapporto sulla *privacy* nell'era digitale[4]. Il documento è stato presentato e discusso nell'ambito del Consiglio dei diritti umani nel 2014[5]. L'anno successivo, lo stesso Consiglio ha designato un Relatore speciale sul diritto alla *privacy*, il quale ha identificato, tra i suoi obiettivi primari, l'elaborazione di uno strumento giuridico volto a regolare la sorveglianza nello spazio informatico, in modo tale da "(…) provide Member States with a number of options to be considered to help plug the gaps and fill the vacuum in international law"[6]. Nel 2017, il Relatore speciale ha presentato all'Assemblea generale un rapporto su "*Big Data – Open Data*", corredato da alcune raccomandazioni preliminari[7]. La prima bozza di uno strumento internazionale specificamente dedicato al tema della *privacy* e sorveglianza statale[8] è stato presentato e discusso nel 2018, nell'ambito di due eventi pubblici congiunti.

Sia le Linee guida del 1989 sia le raccomandazioni del Relatore Speciale sono atti privi di efficacia giuridica vincolante. Si tratta, però, di strumenti che testimoniano lo sforzo delle Nazioni Unite di promuovere la cooperazione internazionale in una materia complessa, al fine di porre le basi per una progressiva armonizzazione delle regole nazionali.

---

[3] *Guidelines for the Regulation of Computerized Personal Data*, ris. 44/132 del 15 dicembre 1989.
[4] V. ris. 68/187, adottata dall'Assemblea generale delle Nazioni Unite il 18 dicembre 2013.
[5] UN Doc. A/HRC/27/37* del 30 giugno 2014 e A/HRC/28/39 del 19 dicembre 2014.
[6] UN Doc. A/72/43103 del 19 ottobre 2017, p. 4.
[7] *Ibidem*, p. 7 ss.
[8] *Working Draft Legal Instrument on Government-led Surveillance and Privacy Including the Explanatory Memorandum*, 28 febbraio 2018, disponibile al sito: https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf.

3. La regolamentazione a livello europeo

3.1 Gli strumenti adottati nell'ambito del Consiglio d'Europa

Tra gli strumenti giuridici adottati nell'ambito del Consiglio d'Europa, di cui sono membri 47 Stati, tra i quali l'Italia, tre sono i trattati internazionali che assumono specifica rilevanza ai fini della tutela dei dati personali:

- la **Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (Roma, 4 novembre 1950)**, entrata in vigore il 3 settembre 1953 (in seguito: CEDU). Ai sensi dell'art. 8:

  "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
  2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

  Attraverso un'interpretazione estensiva, la Corte europea dei diritti umani ha ampliato l'ambito di applicazione dell'art. 8, par. 1, in modo tale da adeguarlo ai problemi derivanti dalle nuove trasformazioni tecniche e sociali[9].

  Analogamente all'art. 17 del Patto sui diritti civili e politici, anche il diritto alla vita privata enunciato nell'art. 8 della CEDU è un diritto derogabile. Pertanto, esso può essere sospeso in caso di pubblica emergenza (art. 15) o compresso nelle ipotesi in cui si trovi in contrasto con altri interessi meritevoli di tutela. Nel bilanciare gli interessi dell'individuo con quelli della collettività, vengono in rilievo i criteri di legittimità (le interferenze esercitate dalle pubbliche autorità devono essere previste dalla legge) e necessità nel quadro di una società democratica (art. 8, par. 2);

- la **Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Strasburgo, 18 gennaio 1981)**, entrata in vigore il 1° ottobre 1985 (**c.d. Convenzione n. 108)**.

  Gli Stati parti[10] a tale Convenzione s'impegnano a garantire a qualsiasi individuo, a prescindere dalla sua nazionalità o residenza, il rispetto del diritto alla tutela della sua vita privata, con specifico riferimento al trattamento automatizzato dei suoi dati personali (art. 1), ove per "trattamento dei dati" ("data processing") s'intende: "any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data" (art. 2.*b*).

  La Convenzione sancisce, inoltre, che alcune categorie speciali di dati (tra cui: dati genetici,

[9] V. *infra*, scheda 10.
[10] Della Convenzione sono parti 54 Stati: tutti gli Stati membri del Consiglio d'Europa, più Argentina, Burkina Faso, Capo Verde, Marocco, Mauritius, Messico, Senegal, Tunisia e Uruguay (dati aggiornati al 15 maggio 2019).

biometrici e alcuni dati personali) non possono essere elaborati automaticamente, a meno che il diritto interno preveda garanzie appropriate (art. 6).

Garanzie supplementari a tutela dei dati sensibili sono contenute nell'art. 8, che sancisce, tra l'altro, il diritto delle persone di richiedere la rettifica di tali dati o la loro cancellazione qualora questi ultimi siano stati elaborati in violazione delle disposizioni di diritto interno. Lo stesso articolo prevede, inoltre, la possibilità di presentare un ricorso qualora non venga dato seguito a una domanda di conferma, comunicazione, rettifica o cancellazione.

Infine, la Convenzione contiene norme volte a disciplinare il flusso transfrontaliero dei dati personali (art. 14).

La Convenzione è completata da un **Protocollo addizionale (Strasburgo, 8 novembre 2001)**, entrato in vigore il 1° luglio 2004, che impone, tra l'altro, agli Stati parti[11] di istituire autorità indipendenti, nell'ambito dei propri ordinamenti nazionali, al fine di garantire un controllo sulla tutela degli individui nel trattamento dei loro dati;

- la **Convenzione sulla criminalità informatica (Budapest, 23 novembre 2001)**, entrata in vigore il 1° luglio 2004, c.d. **Convenzione n. 185**.

  La Convenzione, che vincola un elevato numero di Stati[12], persegue l'obiettivo di assicurare una politica penale comune degli Stati parti, al fine di prevenire e reprimere atti di criminalità informatica, in particolare attraverso l'adozione di legislazioni nazionali appropriate. Un intero capitolo è dedicato alla regolamentazione della cooperazione internazionale, volta, tra l'altro, a promuovere la mutua assistenza nell'adozione di misure provvisorie e nella conduzione delle indagini.

  La Convenzione è completata da un **Protocollo addizionale, concernente l'incriminazione degli atti di natura razzista o xenofoba commessi tramite sistemi informatici (Strasburgo, 28 gennaio 2003)**, entrato in vigore il 1° marzo 2006. L'Italia ha firmato, ma non ratificato tale Protocollo.

3.2 Gli strumenti adottati nell'ambito dell'Unione europea

3.2.1 *Introduzione*

Solennemente proclamata in occasione del Trattato di Nizza (2001), la Carta dei diritti fondamentali dell'Unione europea[13] (la Carta) è diventata vincolante e con rango primario, ossia avente lo stesso valore giuridico dei Trattati (art. 6 Trattato sull'Unione europea, TUE), in seguito all'entrata in vigore del Trattato di Lisbona (2009).

La Carta codifica, rende visibili e sistematizza i diritti fondamentali dell'individuo tutelati nell'ordinamento giuridico dell'Unione europea. Inizialmente negletti, tali diritti, a partire dagli

[11] Del Protocollo addizionale sono parti 36 Stati membri del Consiglio d'Europa e 7 Stati non membri; l'Italia ha firmato, ma non ratificato (dati aggiornati al 15 maggio 2019).
[12] Hanno ratificato la Convenzione 63 Stati, di cui: 44 Stati membri del Consiglio d'Europa (non hanno ratificato Irlanda e Svezia; non ha né firmato né ratificato la Federazione Russa) e 19 Stati non membri del Consiglio d'Europa (tra cui: Australia, Canada, Giappone e Stati Uniti). Dati aggiornati al 15 maggio 2019.
[13] GU C/202, 7 giugno 2016, p. 389 ss.

anni ’70, sono stati enucleati dalla Corte di giustizia tramite un’ampia giurisprudenza che, a sua volta, rinviava alle tradizioni costituzionali comuni degli Stati membri[14]. In seguito, la Corte ha iniziato a riferirsi in maniera sempre più esplicita e puntuale al sistema di protezione offerto dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) secondo la giurisprudenza della Corte di Strasburgo[15].

Per garantire un maggiore livello di tutela e di organicità dei diritti fondamentali, oltre a una loro interpretazione coerente in un sistema c.d. multilivello, sin dagli anni ’90, si è discusso di una possibile adesione dell’Unione al sistema CEDU. Detta adesione era stata in un primo momento bloccata poiché il Trattato non prevedeva una base giuridica specifica[16]. L’art. 6 TUE rimedia a questa lacuna, prevedendo esplicitamente che l’Unione aderisca alle CEDU. Richiesta di un parere in merito, la Corte di giustizia ha statuito che il progetto di adesione comprometterebbe l’unitarietà dell’ordinamento giuridico dell’Unione[17]. Allo stato attuale di sviluppo del diritto dell’Unione, quindi, la tutela dei diritti fondamentali continua a scorrere su binari paralleli: da un lato, attraverso le disposizioni della Carta; dall’altro attraverso quelle della CEDU e l’interpretazione della Corte di Strasburgo.

Le intersezioni tra i due sistemi sono dovute, in primo luogo, all’art. 52, par. 3, della Carta a tenore del quale, in caso di diritti corrispondenti, ad essi debba riconoscersi lo stesso significato e la stessa portata di quanto previso dalla CEDU. In secondo luogo, le c.d. Spiegazioni relative alla Carta[18] fanno opportuno riferimento alla CEDU e alla giurisprudenza della Corte di Strasburgo, come si vedrà con particolare riferimento agli articoli 7 e 8 della Carta.

I diritti contenuti nella Carta sono rubricati in sette titoli: dignità, libertà, uguaglianza, solidarietà, cittadinanza, giustizia, disposizioni generali che disciplinano l’interpretazione e l’applicazione. Il contenuto delle norme, *rectius*, la portata dei diritti, ricalca la giurisprudenza consolidata della Corte e trae ispirazione, senza soluzione di continuità, dal diritto derivato, dalle tradizioni costituzionali comuni e da una molteplicità di strumenti di diritto internazionale pattizio.

In linea con l’intento di delimitare in modo sempre più preciso le competenze dell’Unione, l’art. 6 TUE ricorda che la Carta non può né estenderle in alcun modo né può introdurne di nuove. La stessa affermazione è ripetuta nell’art. 51, par. 2, della Carta. Per quel che riguarda il campo di applicazione, l’art. 51, par. 1, della Carta stabilisce che essa sia applicabile alle istituzioni, organi e organismi dell’Unione e agli Stati membri esclusivamente nell’attuazione del diritto dell’Unione. Ne consegue che, da un lato, un atto dell’Unione può essere impugnato per violazione delle disposizioni della Carta tramite l’art. 263 del Trattato sul funzionamento dell’Unione europea (TFUE); dall’altro lato, gli Stati membri saranno chiamati a rispettare la Carta quando essi attuano il diritto dell’Unione, per esempio, nelle procedure di trasposizione delle direttive, nell’emanare i mandati di arresto o nelle decisioni di rimpatrio. Inoltre, si segnala che, nell’ambito della procedura legislativa ordinaria, la Commissione, nel proporre nuovi atti di diritto derivato, espleta una c.d. valutazione di impatto per verificare *ex ante* il rispetto dei diritti fondamentali.

---

[14] Corte di giustizia, causa 11/70, *Internationale Handelsgesellschaft mbH c. Einfuhr- und Vorratsstelle für Getreide und Futtermittel*, sentenza del 17 dicembre 1970; Corte di giustizia, causa 4/73, *J. Nold, Kohlen- und Baustoffgroßhandlung c. Commissione delle Comunità europee*, sentenza del 14 maggio 1974.

[15] Corte di giustizia, causa C-260/89, *Elliniki Radiophonia Tiléorassi AE c. Dimotiki Etairia Pliroforissis e Sotirios Kouvelas*, sentenza del 18 giugno 1991.

[16] Corte di giustizia, *Adesione della Comunità alla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, parere 2/94 del 28 marzo 1996.

[17] Corte di giustizia, *Progetto di accordo internazionale – Adesione dell’Unione europea alla Convenzione europea per la salvaguardia dei diritti dell’uomo e delle libertà fondamentali – Compatibilità di detto progetto con i Trattati UE e FUE*, parere 2/13 del 18 dicembre 2014.

[18] GU C/303, 14 dicembre 2007, p. 17 ss.

Infine, occorre ricordare che, nell'ordinamento giuridico dell'Unione europea, a differenze del sistema CEDU, non esiste un meccanismo diretto di ricorso per lamentare violazioni dei diritti fondamentali sanciti dalla Carta.

3.2.2. L'art. 7 della Carta: rispetto della vita privata e della vita familiare

Ai sensi dell'art. 7 della Carta:

> "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni".

Tale norma assume rilievo nella misura in cui impone la tutela, per quel che qui interessa, delle comunicazioni di un individuo. Inoltre, essa presenta uno stretto legame con l'art. 8 della Carta, dedicato, come si vedrà, alla protezione dei dati personali.

Le Spiegazioni della Carta precisano che la norma riflette il contenuto dell'art. 8 CEDU ma che, per tenere conto delle evoluzioni tecniche, il termine "corrispondenza" è stato sostituito con "comunicazioni". Le Spiegazioni, inoltre, nel ricalcare l'art. 8 CEDU, affermano che le ingerenze che possono essere apportate all'art. 7 della Carta devono consistere in "una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico dello Stato, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui". Tali limitazioni risultano applicabili, *mutatis mutandis*, anche all'art. 8 della Carta[19].

L'art. 7 della Carta non propone un ordine di importanza di beni giuridici da proteggere. Tuttavia, sembra che il rispetto delle proprie comunicazioni possa essere considerato un elemento ulteriore e necessario al fine di garantire l'effettivo godimento del rispetto della vita privata e familiare.

Gli artt. 7 e 8 della Carta coesistono e sono spesso simultaneamente invocati, ma ciò non significa che essi abbiano la stessa interpretazione e lo stesso campo di applicazione. Infatti, l'oggetto della comunicazione può essere particolarmente ampio e non è detto che attenga – o debba attenere – ai dati personali di un individuo. Nel caso *Digital Rights Ireland*[20], la Corte ha affermato che la conservazione per un certo periodo di tempo di dati rilevanti alla vita privata di una persona può costituire un'ingerenza nel diritto garantito dall'art. 7 della Carta; tuttavia essa non pregiudica il contenuto essenziale del diritto, poiché la conservazione dei dati non permetteva, nel caso di specie, di conoscerne il contenuto.

L'art. 7 della Carta, quindi, si pone a difesa di un ventaglio di diritti che passano anche, ma non solo, attraverso la protezione dei dati personali dell'individuo e sono ad essi direttamente collegati.

3.2.3. L'art. 8 della Carta: protezione dei dati di carattere personale

Ai sensi dell'art. 8 della Carta:

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

[19] V. *infra*, par. 3.2.3

[20] Corte di giustizia, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.*, sentenza dell'8 aprile 2014.

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

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

Le Spiegazioni della Carta indicano le fonti che hanno ispirato la stesura dell'art. 8. In primo luogo, viene richiamato nuovamente l'art. 8 CEDU sebbene, nella sfera che qui interessa, esso sia stato più di sovente interpretato ai fini del rispetto delle comunicazioni dei detenuti o per quel che riguarda la legittimità delle intercettazioni telefoniche. In secondo luogo, vengono menzionate le fonti di diritto primario e secondario proprie dell'ordinamento giuridico dell'Unione europea: i) l'art. 16 TFUE; ii) la direttiva 95/46/CE[21]; iii) il regolamento 45/2001[22]; iii) l'art. 39 TUE, significativamente inserito nel capo dedicato alle disposizioni sulla politica estera e di sicurezza comune.

L'art. 8 della Carta specifica i principi sottesi alla protezione dei dati personali: lealtà, determinazione, consenso dell'interessato ovvero altro fondamento legittimo al trattamento. Inoltre, esso indica due diritti complementari: il diritto di accesso ai propri dati e il diritto di rettifica degli stessi. Infine, è stabilito che un'autorità indipendente vigili sul rispetto di tali regole. A tal proposito si segnala sia la presenza di un'autorità europea di garanzia (*European Data Protection Superviror*) sia di autorità nazionali (per l'Italia, il Garante per la protezione dei dati personali).

I principi che si ricavano dall'art. 8 della Carta sono, a loro volta, di ispirazione per la legislazione di dettaglio del regolamento 2016/679[23] (GDPR)[24].

L'esistenza di esigenze di tutela dei dati di carattere personale può essere fatta risalire al caso *Stauder*[25], agli albori dell'esperienza di integrazione comunitaria. L'importanza dell'art. 8 della Carta è da ascriversi soprattutto all'aver codificato i principi cardine dell'azione dell'Unione in materia, rendendo quindi il diritto alla protezione dei dati personali un diritto fondamentale *tout court* e, come tale, parametro di validità dell'azione dell'Unione e degli Stati membri.

[21] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati GU L 281 del 23.11.1995, pp. 31–50.

[22] Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati GU L 8 del 12.1.2001, pp. 1–22. V. 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 (Testo rilevante ai fini del SEE.) PE/31/2018/REV/1 GU L 295 del 21.11.2018, pp. 39–98.

[23] 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 (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE) GU L 119 del 4.5.2016, pp. 1–88.

[24] V. *infra*, par. 3.2.4.

[25] Corte di giustizia, causa 29/69, *Erich Stauder c. Stadt Ulm – Sozialamt*, sentenza del 12 novembre 1969.

3.2.4. Dal diritto primario al diritto derivato: il regolamento generale sulla protezione dei dati

Il GDPR, che modifica il c.d. codice dei dati personali[26], è un atto legislativo di oltre 80 pagine, che include un centinaio di articoli, preceduto da 173 considerando: impossibile darne contezza in questa sede. Tuttavia, si possono proporre alcune osservazioni di carattere generale, soprattutto al fine di comprendere come l'atto in questione sia stato influenzato dall'art. 8 della Carta. Non è quindi una coincidenza che il primo considerando del GDPR affermi testualmente che "la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale".

La base giuridica del GDPR è l'art. 16 TFUE, norma espressamente dedicata alla protezione dei dati personali e contenuta nel Titolo II, disposizioni di applicazione generale. In questo modo, anche alla luce dello smantellamento della struttura in pilastri operata dal Trattato di Lisbona, la protezione dei dati personali può occupare tutti i settori di intervento dell'Unione, quindi anche in materia penale[27].

Sinteticamente, il GDPR ha per oggetto la protezione dei dati personali delle persone fisiche con riguardo al loro trattamento e la loro circolazione; aspetti da combinarsi attraverso i principi, su cui si ritornerà *infra*, che ispirano l'atto in commento (art. 1). Il GDPR si applica al trattamento interamente o parzialmente automatizzato dei dati personali e a quello non automatizzato degli stessi nella misura in cui essi siano contenuti in un archivio o possano figurarvi. Il GDPR non è applicabile quando i dati siano trattati dalle istituzioni dell'Unione o da autorità competenti in materia di prevenzione, indagine o accertamento di reati. A parte queste specifiche esclusioni, i problemi interpretativi maggiori sono da determinarsi nei casi di non applicazione del diritto dell'Unione europea (art. 2), poiché in tali ipotesi non sarebbe possibile invocare né il GDPR né la Carta.

Tenuto conto di queste limitazioni, il GDPR si applica essenzialmente in due situazioni: 1) quando il trattamento dei dati avviene nel contesto delle attività di un titolare o di un responsabile del trattamento che si trovano all'interno dell'Unione europea; 2) quando il trattamento di dati di individui che si trovano nell'Unione europea avviene da parte di un responsabile o di un titolare anche non ivi stabilito. Il campo di applicazione territoriale sembra quindi ritagliato secondo le motivazioni che hanno portato la Corte ad annullare la direttiva 2006/24[28] così come risulta dalla

[26] Decreto legislativo 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 (regolamento generale sulla protezione dei dati), (18G00129), GU Serie Generale n. 205 del 4 settembre 2018.

[27] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio GU L 119 del 4 maggio 2016, pp. 89–131.

[28] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006 , riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE GU L 105 del 13 aprile 2006, pp. 54–63.

sentenza *Digital Rights Ireland*[29]. Inoltre, anche il trasferimento dei dati verso Stati terzi deve rispettare i principi sanciti dall'art. 8 della Carta[30].

Il GDPR procede attraverso un puntuale elenco di definizioni, aggiornato secondo la nozione di "comunicazione" contenuta nelle Spiegazioni dell'art. 7 della Carta. Trovano quindi consacrazione, all'art. 4, le nozioni di profilazione, pseudonimizzazione, dati genetici e dati biometrici. Come anticipato, i principi concernenti il trattamento dei dati personali sono ricavabili dall'art. 8 della Carta e, di conseguenza, sono enucleati singolarmente all'art. 8 del GDPR. Essi possono così essere esaustivamente elencati: a) liceità, correttezza e trasparenza; b) limitazione delle finalità; c) minimizzazione dei dati; d) esattezza; e) limitazione della conservazione; integrità e riservatezza; f) responsabilizzazione (art. 5).

Trovano inoltre accoglimento nel GDPR nuovi c.d. micro-diritti, come il diritto alla portabilità dei dati (art. 20), il diritto di rettifica (art. 16) e il diritto alla cancellazione (c.d. diritto all'oblio, art. 17). L'introduzione di quest'ultimo, in particolare, è riconducibile alla giurisprudenza della Corte nel caso *Google Spain*[31].

Anche la lunga lista di limitazioni alla protezione dei dati personali è ricavata direttamente dalla giurisprudenza della Corte di Strasburgo e dalla Carta. Con un estremo livello di dettaglio, l'art. 23 fa espresso riferimento a limitazioni che rispettino l'essenza del diritto alla protezione dei dati personali e che siano necessarie e proporzionate in una società democratica. Oltre alle classiche esigenze riconducibili ai concetti di sicurezza nazionale e sicurezza pubblica, si segnalano gli interessi economici e finanziari dell'Unione o degli Stati membri, l'indipendenza della magistratura, l'esecuzione delle azioni civili. Anche in questo contesto, il contenuto della norma sembra ricalcare la giurisprudenza della Corte e, più precisamente, la sentenza *Tele2*[32].

Tra le novità introdotte dal GDPR si segnala la costituzione del Comitato europeo per la protezione dei dati (il Comitato). Dotato di personalità giuridica autonoma, esso "è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo della protezione dei dati" (art. 68, par. 3). Il Comitato garantisce l'applicazione "coerente" del GDPR (art. 70, par. 1). Tra le sue funzioni, ai fini che qui più interessano, occorre segnalare la pubblicazione di linee guida in materia di: cancellazione di *link* nei servizi accessibili al pubblico, nei casi di profilazione e di violazione dei dati personali; previsione di sanzioni amministrative; valutazione del livello di tutela dei dati personali negli Stati terzi in caso di trasferimento verso questi ultimi. Il Comitato, dunque, si configura come un organo consultivo a carattere tecnico di grande importanza nella gestione del diritto alla protezione dei dati personali, fungendo da raccordo tra il livello sovranazionale e quello interno.

Infine, l'intero Capo VIII del GDPR disciplina le azioni che possono essere intraprese in caso di violazione del regolamento. Innanzi tutto, è previsto per l'interessato il diritto di proporre reclamo di fronte all'autorità di controllo dello Stato membro nel quale egli risieda, lavori ovvero del luogo ove si sia verificata la violazione (art. 77). L'art. 78, invece, prevede il diritto a un ricorso giurisdizionale effettivo avverso i provvedimenti vincolanti dell'autorità di controllo, da esperirsi di

[29] Corte di giustizia, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.*, sentenza dell'8 aprile 2014.
[30] Corte di giustizia, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, sentenza del 6 ottobre 2015.
[31] Corte di giustizia, causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, sentenza del 13 maggio 2014.
[32] Corte di giustizia, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB c. Post- och telestyrelsen e Secretary of State for the Home Department c. Tom Watson e a.*, sentenza del 21 dicembre 2016.

fronte al giudice dello Stato membro ove è stabilita detta autorità. L'art. 79 sancisce il diritto a un ricorso giurisdizionale anche nei confronti del titolare o del responsabile del trattamento. Inoltre, mentre l'art. 82, par. 1, prevede il diritto al risarcimento del danno in caso di violazioni del GDPR da parte del titolare o del responsabile del trattamento, l'art. 83 afferma che le sanzioni debbano essere effettive, proporzionate e dissuasive ed elenca i parametri da considerare per fissarne l'ammontare. Più in particolare, sono menzionate la natura, la gravità e la durata della violazione, il carattere doloso o colposo della stessa, le categorie di dati personali interessate, l'adesione a codici di condotta.

Il GDPR è dunque l'atto di riferimento per ogni attività riguardante, anche solo *lato sensu*, il trattamento e la salvaguardia del diritto fondamentale alla protezione dei dati personali. Di conseguenza, il GDPR deve essere letto e interpretato, dagli operatori giuridici nazionali e dalle pubbliche amministrazioni, alla luce degli artt. 7 e 8 della Carta, al fine di garantire un elevato livello di protezione di quello che ormai è a tutti gli effetti un diritto fondamentale di ogni individuo.

3.2.5. Cenni conclusivi

L'analisi della Carta e dei suoi artt. 7 e 8 conferma che gli operatori giuridici si trovano di fronte a due norme dinamiche, pensate per affrontare situazioni in costante divenire. La sempre crescente attenzione alle nuove tecnologie – sia da parte della giurisprudenza della Corte, sia da parte dei giudici e degli operatori del diritto nazionali – dimostra che il diritto al rispetto della privata e della vita familiare, congiuntamente al diritto alla protezione dei dati di carattere personale, rappresentano le sfide più insidiose cui un sistema integrato, coeso e, soprattutto, multilivello dei diritti fondamentali è chiamato a rispondere. Da questa prospettiva, non può che accogliersi favorevolmente l'emanazione del GDPR da parte del Parlamento e del Consiglio e la tempestiva opera di adattamento da parte del legislatore italiano tramite il decreto legislativo 101/2018.

Il quadro di riferimento della protezione dei dati personali e delle comunicazioni, in uno spazio sociale, economico e giuridico sempre più globalizzato, può quindi definirsi completo e i suoi assi portanti sono l'individuo e la sua signoria sui dati che lo riguardano.

4. La giurisprudenza di orientamento

Le seguenti sentenze della Corte di giustizia dell'Unione europea sono rilevanti ai fini dello studio della materia:

Corte di giustizia, causa 29/69, *Erich Stauder c. Stadt Ulm – Sozialamt*, sentenza del 12 novembre 1969;

Corte di giustizia, causa 11/70, *Internationale Handelsgesellschaft mbH c. Einfuhr- und Vorratsstelle für Getreide und Futtermittel*, sentenza del 17 dicembre 1970;

Corte di giustizia, causa 4/73, *J. Nold, Kohlen- und Baustoffgroßhandlung c. Commissione delle Comunità europee*, sentenza del 14 maggio 1974;

Corte di giustizia, causa C-260/89, *Elliniki Radiophonia Tiléorassi AE c. Dimotiki Etairia Pliroforissis e Sotirios Kouvelas*, sentenza del 18 giugno 1991;

Corte di giustizia, *Adesione della Comunità alla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, parere 2/94 del 28 marzo 1996;

Corte di giustizia, cause riunite C-465/00, C-138/01 e C-139/01, *Rechnungshof c. Österreichischer Rundfunk e altri e Christa Neukomm e Joseph Lauermann c. Österreichischer Rundfunk*, sentenza del 20 maggio 2003;

Corte di giustizia, causa C-101/01, *Procedimento penale a carico di Bodil Lindqvist*, sentenza del 6 novembre 2003;

Corte di giustizia, cause riunite C-92/09 e C-93/04, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, sentenza del 9 novembre 2010;

Corte di giustizia, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.*, sentenza dell'8 aprile 2014;

Corte di giustizia, causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, sentenza del 13 maggio 2014;

Corte di giustizia, *Progetto di accordo internazionale – Adesione dell'Unione europea alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali – Compatibilità di detto progetto con i Trattati UE e FUE*, parere 2/13 del 18 dicembre 2014;

Corte di giustizia, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, sentenza del 6 ottobre 2015;

Corte di giustizia, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB c. Post- och telestyrelsen e Secretary of State for the Home Department c. Tom Watson e a.*, sentenza del 21 dicembre 2016.

Per l'esame dettagliato del contenuto di alcune di queste sentenze, si rinvia alle schede di seguito riportate.

Scheda n. 1 – La validità della normativa dell'Unione in materia di conservazione e memorizzazione delle impronte digitali integrate nel passaporto alla luce degli artt. 7 e 8 della Carta

- Corte di giustizia, sentenza del 17 ottobre 2013, *Schwarz*, causa C-291/12

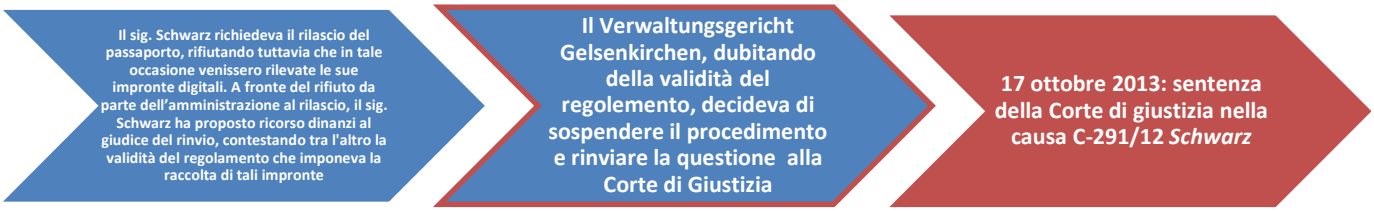
1. Aspetti centrali

Le impronte digitali rientrano nella nozione di dati personali: esse contengono, infatti, informazioni uniche su persone fisiche e consentono la loro precisa identificazione. Inoltre, il fatto che le autorità nazionali rilevino le impronte digitali e che tali impronte siano conservate sul supporto di memorizzazione integrato nel passaporto costituisce un trattamento di dati personali. Pertanto, il prelievo e la conservazione di impronte digitali disciplinati dal regolamento n. 2252/2004 da parte delle autorità nazionali costituiscono un pregiudizio fondamentale ai diritti al rispetto della vita privata e alla tutela dei dati personali.
Il regolamento n. 2252/2004 non implica un trattamento delle impronte digitali che eccede quanto necessario per impedire l'ingresso illegale di persone nel territorio dell'Unione europea.

2. A colpo d'occhio

Paese	Area	Riferimenti al diritto UE	Attori	Tecniche di Interazione giuridica	Esito
• Germania	• Protezione dei dati personali • Spazio di libertà sicurezza e giustizia	• Artt. 7, 8, 52(1) CDFUE • Regolamento n.2252/2004/CE	• Verwaltungsgericht Gelsenkirchen (Germania) • Corte di giustizia	• Verticale: Domanda di pronuncia pregiudiziale sulla validità del regolamento n.2252/2004	• Il regolamento n.2252/2004 sugli elementi biometrici dei passaporti è valido.

3. Cronologia



4. Descrizione

a. Fatti

Il sig. Schwarz richiedeva il rilascio del passaporto, rifiutando tuttavia che, in tale occasione, venissero rilevate le sue impronte digitali. A fronte del rifiuto di rilasciare il passaporto da parte dell'amministrazione competente, il sig. Schwarz proponeva ricorso dinanzi al giudice del rinvio perché fosse ingiunto di rilasciargli il documento in questione senza rilevare le sue impronte. Nel

ricorso, il sig. Schwarz contestava in particolare la validità del regolamento n. 2252/2004[33] che aveva introdotto l'obbligo del rilevamento delle impronte digitali. I motivi addotti riguardavano il fondamento giuridico dell'atto e la procedura seguita per la sua adozione, nonché la pretesa violazione degli articoli 7 e 8 della Carta.

Il *Verwaltungsgericht Gelsenkirchen*, dubitando della validità del regolamento, decideva di sospendere il procedimento e sollevare una questione in via pregiudiziale alla Corte di giustizia.

b. Ragionamento della Corte di giustizia

Innanzitutto, la Corte valuta i due rilievi relativi al fondamento giuridico del regolamento e alla procedura seguita per la sua adozione.

Per quanto riguarda il primo aspetto, la Corte rileva che l'art. 62 TCE [ora art. 77 TFUE] costituisce un fondamento giuridico adeguato per il regolamento n. 2252/2004, in quanto sia dalla formulazione sia dall'obiettivo di tale disposizione emerge che quest'ultima attribuisce all'Unione il compito di disciplinare i controlli relativi all'attraversamento alle frontiere esterne. Poiché tale verifica implica necessariamente la presentazione di documenti che consentono di dimostrare l'identità delle persone, la Corte ritiene che tale articolo autorizzi il legislatore dell'Unione ad adottare disposizioni normative relative a tali documenti e, in particolare, ai passaporti. Inoltre, l'articolo in questione si riferisce ai controlli delle "persone" senza ulteriori precisazioni; pertanto tale disposizione riguarda non soltanto i cittadini di Stati terzi, ma anche i cittadini dell'Unione e, di conseguenza, anche i passaporti di questi ultimi. Inoltre, si deve ritenere che il legislatore dell'Unione sia competente a prevedere caratteristiche di sicurezza per i passaporti dei cittadini dell'Unione equivalenti a quelle richieste per i visti e i permessi di soggiorno dei cittadini di Stati terzi, in modo da evitare che detti passaporti diventino oggetto di falsificazione e impieghi fraudolenti.

Il secondo aspetto preso in esame dalla Corte riguarda la mancata consultazione del Parlamento europeo dopo la modifica apportata dal Consiglio, nell'ambito del procedimento legislativo volto all'adozione del regolamento n. 2252/2004, relativa all'obbligo di memorizzazione delle impronte digitali da parte degli Stati membri. La Corte rileva, tuttavia, che il regolamento n. 444/2009 ha sostituito il testo della disposizione relativa all'obbligo di memorizzazione delle impronte digitali e che lo stesso è stato adottato secondo una procedura di co-decisione. Pertanto, secondo la Corte, l'asserito motivo di invalidità risulta essere inoperante.

La Corte procede poi all'analisi della validità del regolamento rispetto agli artt. 7 e 8 della Carta. In primo luogo verifica se il rilevamento delle impronte digitali e la loro conservazione nei passaporti costituiscano un pregiudizio al godimento dei diritti relativi alla tutela della vita privata e dei dati personali. Secondo la Corte, dal combinato disposto delle due disposizioni della Carta deriva che, in linea di principio, qualsiasi trattamento dei dati personali effettuato da un terzo è idoneo a costituire pregiudizio a tali diritti.

Nel caso di specie, la Corte riconosce che le impronte digitali rientrano nella nozione di dati personali, dato che contengono informazioni uniche su persone fisiche e consentono la loro precisa identificazione. Inoltre, il fatto che le autorità nazionali rilevino le impronte digitali delle persone

[33] Regolamento (CE) n. 2252/2004 del Consiglio, del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri (GU L 385, pag. 1), come modificato dal regolamento (CE) n. 444/2009 del Parlamento europeo e del Consiglio, del 6 maggio 2009 (GU L 142, pag. 1, e rettifica GU L 188, pag. 127; in prosieguo: il regolamento n. 2252/2004).

interessate e che tali impronte siano conservate sul supporto di memorizzazione integrato nel passaporto costituisce un trattamento di dati personali. Pertanto, secondo la Corte, il prelievo e la conservazione di impronte digitali da parte delle autorità nazionali, disciplinati dal regolamento n. 2252/2004, costituiscono un pregiudizio ai diritti al rispetto della vita privata e alla tutela dei dati personali.

La Corte esamina quindi se tale ingerenza nei citati diritti fondamentali sia giustificata. In base all'art. 8, par. 2, della Carta, i dati personali devono essere trattati in base al consenso della persona interessata o in forza di un altro fondamento legittimo previsto dalla legge. Per quanto riguarda il consenso, la Corte rileva che il possesso del passaporto è, di norma, indispensabile ai cittadini dell'Unione per spostarsi e che, in base alla normativa dell'Unione, tale documento deve contenere le impronte digitali. Pertanto, i cittadini dell'Unione che desiderano spostarsi non possono liberamente opporsi al trattamento delle loro impronte digitali e non si può quindi considerare che colui che richiede il passaporto presti il consenso a un simile trattamento.

Per quanto riguarda la giustificazione del trattamento delle impronte digitali in forza di un altro fondamento legittimo previsto dalla legge, la Corte afferma che gli artt. 7 e 8 della Carta non possono essere considerati prerogative assolute e possono essere limitati sulla base dell'art. 52, par. 1, dello stesso strumento. In primo luogo, la limitazione derivante dal rilevamento e dalla conservazione di impronte digitali nel contesto del rilascio dei passaporti deve essere prevista *ex lege*; nel caso di specie, essa è prevista dal regolamento n. 2252/2004. In secondo luogo, il regolamento persegue un obiettivo di interesse generale riconosciuto dall'Unione, in quanto è diretto a impedire l'ingesso illegale di persone nel territorio dell'Unione. In terzo luogo, le limitazioni apportate all'esercizio dei diritti riconosciuti dagli artt. 7 e 8 della Carta rispettano il contenuto essenziale di tali diritti.

Infine, la Corte si sofferma sia sul requisito della proporzionalità di tali limitazioni rispetto agli scopi perseguiti dal regolamento sia sulla idoneità e necessità del ricorso ai mezzi ivi previsti. Per quanto riguarda l'idoneità dei mezzi impiegati al fine di prevenire la falsificazione e l'uso fraudolento dei passaporti, la Corte rileva che la tecnica sofisticata utilizzata per la conservazione delle impronte digitali su un supporto di memorizzazione securizzato appare idonea a ridurre il rischio di falsificazione e ad agevolare l'esame della loro autenticità. In questo caso, inoltre, non è determinante che tale metodo sia totalmente affidabile, in quanto è sufficiente che esso riduca considerevolmente il rischio di accettazione di persone non autorizzate alla frontiera esterna. Pertanto, il prelievo e la conservazione delle impronte digitali sono idonei al raggiungimento degli obiettivi perseguiti dal regolamento, ossia impedire l'ingresso illegale di persone nel territorio dell'Unione.

Per quanto riguarda l'aspetto dell'esame della necessità di siffatto trattamento, la Corte verifica la possibile esistenza di misure meno pregiudizievoli per i diritti di cui agli artt. 7 e 8 della Carta rispetto al prelevamento delle impronte digitali. La Corte constata che il rilevamento consiste soltanto nel prendere l'impronta di due dita, a cui si aggiunge la fotografia del volto. Secondo la Corte, non si può ritenere a priori che la somma di due operazioni d'identificazione delle persone comporti, di per sé, un pregiudizio più grave ai diritti riconosciuti agli artt. 7 e 8 della Carta rispetto alla situazione in cui tali operazioni fossero considerate isolatamente. Inoltre, l'unica reale alternativa al rilevamento delle impronte digitali consiste nella cattura dell'immagine dell'iride dell'occhio. Tuttavia, da un lato, non è possibile desumere che tale mezzo sia meno pregiudizievole per i diritti fondamentali; dall'altro lato, il livello di maturità tecnologica del metodo basato sul riconoscimento dell'iride non raggiunge quello basato sulle impronte digitali.

La Corte rileva che, allo stato attuale, non è possibile individuare l'esistenza di misure idonee che possano contribuire, in modo sufficientemente efficace, all'obiettivo di preservare i passaporti da un uso fraudolento, arrecando un pregiudizio minore ai diritti riconosciuti agli artt. 7 e 8 della Carta rispetto al pregiudizio arrecato dal metodo basato sulle impronte digitali.

Affinché tale rilevamento sia giustificato occorre, infine, che esso non ecceda quanto necessario per raggiungere l'obiettivo di prevenire l'uso fraudolento dei passaporti. Secondo la Corte, il legislatore dell'Unione deve assicurarsi che esistano garanzie specifiche dirette a tutelare efficacemente i dati personali contro trattamenti impropri e abusivi. A questo riguardo, il regolamento n. 2252/2004 precisa che le impronte digitali possono essere utilizzate soltanto allo scopo di verificare l'autenticità del passaporto e l'identità del suo titolare. Inoltre, i dati sono conservati su un supporto di memorizzazione integrato nel passaporto e altamente securizzato, il quale permane nell'esclusivo possesso del titolare. Ne consegue che, ad avviso della Corte, il regolamento in esame non implica un trattamento delle impronte digitali che eccede quanto necessario per la realizzazione dell'obiettivo di preservare i passaporti da un uso fraudolento.

La Corte riconosce conseguentemente la validità del regolamento n. 2252/2004, in quanto quest'ultimo non implica un trattamento delle impronte digitali che eccede quanto necessario per la realizzazione dell'obiettivo di preservare i passaporti da un uso fraudolento. Ciò considerato, la Corte non procede all'esame della necessità dei mezzi posti in essere dal regolamento ai fini del raggiungimento dell'ulteriore obiettivo perseguito dalla normativa, ossia la prevenzione della falsificazione dei passaporti.

c. Esito a livello nazionale

Non disponibile.

5. Analisi

a. Il ruolo della Carta

Nella presente sentenza la Carta e, in particolare, i suoi artt. 7 e 8, viene utilizzata dalla Corte di giustizia come parametro di validità di un atto dell'Unione, il regolamento n. 2252/2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti.

La Corte di giustizia rileva che, potenzialmente, in base al combinato disposto degli artt. 7 (diritto alla tutela della vita privata) e 8 (diritto alla protezione dei dati) della Carta, "qualsiasi trattamento dei dati personali effettuato da un terzo è idoneo a costituire un pregiudizio a tali diritti" (par. 25). Tuttavia, a fronte di tale affermazione, la Corte precisa che tali diritti non devono essere considerati prerogative assolute, ma possono essere soggetti a limitazioni.

Nel suo ragionamento, la Corte dedica quindi particolare attenzione alle caratteristiche che una disposizione di diritto dell'Unione che comporta limitazioni ai diritti fondamentali deve avere affinché possa essere giustificata ai sensi dell'art. 52, par. 1, della Carta. In particolare, la Corte si sofferma sui requisiti della proporzionalità e della necessità delle misure rispetto all'obiettivo perseguito dallo strumento normativo in esame (la lotta contro l'ingresso illegale di persone nel territorio dell'Unione).

Da un lato, la Corte rileva infatti che "occorre constatare che non è stata portata a [sua] conoscenza ... l'esistenza di misure idonee a contribuire, in modo sufficientemente efficace, all'obiettivo di preservare i passaporti da un uso fraudolento, arrecando un pregiudizio minore ai diritti riconosciuti dagli articoli 7 e 8 della Carta rispetto al pregiudizio arrecato dal metodo basato

sulle impronte digitali" (par. 53). Dall'altro lato, essa riconosce che, poiché "tale regolamento non prevede nessun'altra forma né alcun altro mezzo di conservazione delle impronte [digitali], esso non può essere interpretato, (…) come idoneo (…) all'impiego di questi ultimi a fini diversi da quello di impedire l'ingresso illegale di persone nel territorio dell'Unione" (par. 61).

Sulla base di tali rilievi, la Corte ritiene che il regolamento in questione non possa essere considerato invalido, in quanto esso non implica un trattamento delle impronte digitali – e, quindi, un pregiudizio agli artt. 7 e 8 della Carta – che eccede quanto necessario per il perseguimento dell'obiettivo di impedire l'ingresso illegale nel territorio dell'Unione.

b. Dialogo giuridico

Interazione verticale tra il giudice nazionale, il *Verwaltungsgericht Gelsenkrichen* tedesco, e la Corte di giustizia attraverso il meccanismo del rinvio pregiudiziale di validità.

c. Impatto della decisione della Corte di giustizia

La sentenza in oggetto rileva in particolare per il legislatore dell'Unione, il quale è più volte richiamato dalla Corte nel suo ragionamento. Infatti, la Corte riconosce la possibilità di apportare limitazioni ai diritti fondamentali (segnatamente gli artt. 7 e 8 della Carta) ma, affinché un atto dell'Unione non venga dichiarato invalido, tali restrizioni devono rispondere a requisiti ben precisi che il legislatore dell'Unione dovrebbe essere tenuto a verificare prima di adottare l'atto.

Tali requisiti riguardano in particolare il rispetto della proporzionalità e la necessità dell'atto adottato rispetto all'obiettivo perseguito. Spetta, infatti, al legislatore dell'Unione verificare se siano concepibili misure meno pregiudizievoli per i diritti riconosciuti dagli artt. 7 e 8 della Carta (par. 46). Inoltre, legislatore dovrà assicurarsi dell'esistenza di garanzie specifiche dirette a tutelare efficacemente i dati relativi alle impronte digitali contro trattamenti impropri e abusivi (par. 55).

d. Altri casi rilevanti

Sull'invalidità di un atto dell'Unione per violazione degli artt. 7, 8 e 52, par. 1, della Carta:

- Corte di giustizia, sentenza 8 aprile 2014, *Digital Rights Ireland*, causa C-293/12;
- Corte di giustizia, sentenza 6 ottobre 2015*, Schrems*, causa C-362/14.

Scheda n. 2 – Il bilanciamento tra l'esigenza di garantire la sicurezza delle persone presenti sul territorio dell'Unione e la tutela della vita privata e dei dati personali

- Corte di giustizia (Grande sezione), sentenza dell'8 aprile 2014, *Digital Rights Ireland*, cause riunite C-293/12 e C-594/12

1. Aspetti centrali

La direttiva 2006/24/CE relativa alla conservazione di dati generati e trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione comporta un'ingerenza nei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta. Tale ingerenza è di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione, senza che sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario.
Pertanto, adottando la direttiva 2006/24/CE, il legislatore dell'Unione ha ecceduto i limiti imposti dal rispetto del principio di proporzionalità alla luce degli artt. 7, 8 e 52, par. 1, della Carta.

2. A colpo d'occhio

Paese	Area	Riferimenti al diritto UE	Attori	Tecniche di Interazione giuridica	Esito
• Irlanda • Austria	• Protezione dei dati personali • Servizi di comunicazione elettronica	• Art. 7, 8, 11, 52(1) CDFUE • Direttiva 2006/24/CE	• High Court (Irlanda) • Verfassungsgerichtshof (Austria) • Corte di giustizia	• Verticale: Domanda di pronuncia pregiudiziale ai sensi dell'art. 267 TFUE sulla validità della direttiva 2006/24/CE • Orizzontale: riferimento della Corte di gustizia alla giurisprudenza della Corte EDU relativa all'art. 8 della Convenzione	• La Corte dichiare la direttiva 2006/24/CE invalida per violazione degli articoli 7, 8 e 52(1) della Carta

3. Cronologia

4. Descrizione

a. Fatti

Causa C-293/12

La società *Digital Rights Ireland* ricorreva innanzi alla *High Court* irlandese, contestando la legittimità di misure legislative e amministrative riguardanti la conservazione di dati relativi a comunicazioni elettroniche e chiedendo, in particolare, che il giudice nazionale dichiarasse la nullità

della direttiva 2006/24/CE[34]. Quest'ultima, infatti, imponeva ai fornitori di servizi di telefonia di conservare i dati relativi al traffico e all'ubicazione per un lasso di tempo specificato dalla legge a fini di prevenzione, accertamento, indagini o perseguimento dei reati e di protezione della sicurezza dello Stato.

Dubitando della legittimità della direttiva, la *High Court* decideva di sospendere il giudizio e di proporre un ricorso in via pregiudiziale alla Corte di giustizia.

Causa C-594/12

Numerosi ricorrenti si rivolgevano al *Verfassunggerichtshof*, chiedendo l'annullamento di un articolo della legge austriaca sulle telecomunicazioni, che era stata adottata per trasporre la direttiva 2006/24 nel diritto interno, in quanto contraria al diritto fondamentale dei privati alla protezione dei propri dati.

Il *Verfassunggerichtshof* si interrogava sulla compatibilità della direttiva 2006/24 con la Carta, in quanto tale norma permetteva di immagazzinare una massa di dati relativi a un numero illimitato di persone per un lungo periodo di tempo. Inoltre, la conservazione dei dati riguardava quasi esclusivamente persone il cui comportamento non giustificava la conservazione dei dati ad esse relativi. Nutrendo dubbi circa l'idoneità della direttiva a raggiungere gli obiettivi da essa perseguiti e la proporzionalità dell'ingerenza nei diritti fondamentali di cui agli artt. 7, 8 e 11 (libertà di espressione) della Carta, il *Verfassunggerichtshof* decideva di sospendere il procedimento e di rivolgersi in via pregiudiziale alla Corte di giustizia.

b. Ragionamento della Corte di giustizia

La Corte innanzitutto rileva che la direttiva 2006/24 ha, come obiettivo principale, quello di armonizzare le disposizioni degli Stati membri relative alla conservazione, da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, di determinati dati da essi generati o trattati, allo scopo di garantirne la disponibilità a fini di prevenzione, indagine, accertamento e perseguimento di reati gravi, come quelli legati alla criminalità organizzata e al terrorismo.

In particolare, i dati che i fornitori di servizi di comunicazione elettronica sono tenuti a conservare permettono di rintracciare e identificare la fonte di una comunicazione e la destinazione della stessa. Essi consentono, inoltre, di stabilire la data, l'ora, la durata e il tipo di una comunicazione, le attrezzature di comunicazione degli utenti, nonché l'ubicazione delle apparecchiature di comunicazione mobile adottate. Tra i dati che devono essere conservati 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.

Secondo la Corte, questi dati, presi nel loro complesso, possono permettere di trarre conclusioni molto precise sulla vita privata delle persone; di conseguenza, la loro conservazione riguarda in modo specifico i diritti garantiti dagli artt. 7 e 8 della Carta. Inoltre non è escluso che la conservazione dei dati possa incidere sull'utilizzo, da parte degli utenti, dei mezzi di comunicazione e, di conseguenza, sull'esercizio, da parte di questi ultimi, della loro libertà di espressione, garantita dall'art. 11 della Carta.

[34] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GU L 105, pag. 54)

La Corte prende quindi in esame la validità della direttiva alla luce degli artt. 7 e 8 della Carta, soffermandosi innanzitutto sull'esistenza di un'ingerenza in tali diritti.

Per accertare l'esistenza di un'ingerenza nel diritto fondamentale al rispetto della vita privata, secondo il giudice dell'Unione, poco importa che le informazioni relative alla vita privata abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza. L'obbligo imposto dalla direttiva ai fornitori di servizi di comunicazione elettronica di conservare per un certo periodo dati relativi alla vita privata di una persona e alle sue comunicazioni costituisce di per sé un'ingerenza nei diritti garantiti dall'art. 7 della Carta. Inoltre, anche l'accesso delle autorità nazionali competenti ai dati costituisce un'ingerenza supplementare in tale diritto fondamentale.

Ugualmente, la direttiva 2006/24 determina un'ingerenza nel diritto fondamentale alla protezione dei dati personali garantito dall'art. 8 della Carta, poiché prevede un trattamento di tali dati.

Pertanto, secondo la Corte, l'ingerenza della direttiva in tali diritti fondamentali è di vasta portata e deve essere considerata particolarmente grave. Inoltre, il fatto che la conservazione dei dati e l'utilizzo ulteriore degli stessi siano effettuati senza che l'abbonato o l'utente registrato ne siano informati può ingenerare nelle persone interessate la sensazione che la loro vita privata sia oggetto di costante sorveglianza.

Constatata l'ingerenza particolarmente grave nei diritti fondamentali di cui agli artt. 7 e 8 della Carta, la Corte si sofferma sull'esistenza di una giustificazione per tale ingerenza ai sensi dell'art. 52, par. 1, della Carta.

Per quanto riguarda il contenuto essenziale del diritto fondamentale al rispetto della vita privata e degli altri diritti sanciti dall'art. 7 della Carta, la Corte rileva che, sebbene la conservazione dei dati imposta dalla direttiva 2006/24 costituisca un'ingerenza particolarmente grave in tali diritti, essa non è tale da pregiudicare il diritto fondamentale in esame, poiché, in base alla disciplina contenuta nella direttiva, non è possibile venire a conoscenza del contenuto delle comunicazioni elettroniche.

La conservazione, secondo la Corte, non è neppure idonea a pregiudicare il contenuto essenziale del diritto fondamentale alla protezione dei dati personali, sancito all'art. 8 della Carta, considerato che la direttiva 2006/24 prevede una disciplina relativa alla protezione e alla sicurezza dei dati.

Per quanto concerne l'obiettivo di interesse generale perseguito dalla norma, la Corte riconosce che esso consiste nel garantire la disponibilità dei dati conservati a fini di indagine, accertamento e perseguimento di reati gravi, per come definiti da ciascuno Stato membro nella propria legislazione nazionale. Lo scopo sostanziale è pertanto quello di contribuire alla lotta contro la criminalità e, di conseguenza, alla sicurezza pubblica e può quindi essere considerato come un fine di interesse generale dell'Unione.

La Corte si sofferma poi sul rispetto del principio di proporzionalità, in base al quale gli atti dell'Unione devono essere idonei a realizzare gli obiettivi legittimi perseguiti dalla normativa in questione e non devono superare i limiti di ciò che è idoneo e necessario al conseguimento degli obiettivi stessi. Per quel che riguarda l'accertamento dell'idoneità della conservazione dei dati a realizzare l'obiettivo perseguito dalla direttiva 2006/24, la Corte constata che, tenuto conto della crescente importanza dei mezzi di comunicazione elettronica, i dati che debbono essere conservati in attuazione della direttiva richiamata permettono alle autorità nazionali competenti in materia di

perseguimento di reati di disporre di possibilità supplementari di accertamento dei reati gravi. Essi costituiscono, pertanto, uno strumento utile per le indagini penali. Ne consegue che la conservazione dei suddetti dati può essere considerata idonea a realizzare l'obiettivo perseguito dalla direttiva.

Quanto al carattere necessario della conservazione dei dati imposta dalla direttiva, sebbene la lotta contro la criminalità grave sia di capitale importanza per garantire la sicurezza pubblica e la sua efficacia possa dipendere dall'uso delle moderne tecniche di indagine, la Corte rileva che tale obiettivo non può di per sé giustificare il fatto che una misura di conservazione sia considerata necessaria ai fini della lotta alla criminalità. Le restrizioni ai diritti fondamentali devono, infatti, operare entro i limiti dello stretto necessario. Pertanto, secondo la Corte, la normativa dell'Unione di cui trattasi dovrebbe prevedere regole chiare e precise, che disciplinino la portata e l'applicazione della misura stessa e imporre requisiti minimi. In tal modo, le persone i cui dati sono stati conservati disporrebbero di garanzie sufficienti per proteggere efficacemente i loro dati personali contro il rischio di abusi e contro eventuali accessi e usi illeciti.

La Corte procede quindi con l'analisi dettagliata della disciplina contenuta nella direttiva 2006/24/CE, rilevando come essa implichi un'ingerenza nei diritti fondamentali della quasi totalità della popolazione europea. La direttiva prevede, infatti, la conservazione di tutti i dati relativi a qualsiasi mezzo di comunicazione elettronica, il cui uso è estremamente diffuso e di importanza crescente nella vita quotidiana di ciascuno. Inoltre, essa riguarda tutti gli abbonati e gli utenti registrati.

La Corte rileva, in particolare, che la direttiva, pur mirando a contribuire alla lotta contro la criminalità grave, non impone alcuna relazione tra i dati di cui prevede la conservazione e l'esistenza di una minaccia per la sicurezza pubblica. La normativa non limita la conservazione dei dati a quelli relativi a un determinato periodo di tempo e/o a un'area geografica determinata e/o a una cerchia di persone determinate che possano essere coinvolte, in un modo o nell'altro, in un reato grave, né alle persone la conservazione dei cui dati, per altri motivi, potrebbe contribuire alla prevenzione, all'accertamento o al perseguimento di reati gravi. Inoltre, la direttiva 2006/24 non prevede alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fini di prevenzione, di accertamento o di indagini penali riguardanti reati che possano, con riguardo alla portata e alla gravità dell'ingerenza nei diritti fondamentali sanciti agli artt. 7 e 8 della Carta, essere considerati sufficientemente gravi da giustificare siffatta ingerenza. Infine, la direttiva prevede la conservazione dei dati per un periodo di almeno sei mesi, senza che venga effettuata alcuna distinzione tra le categorie di dati, a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda della persona interessata.

Per questi motivi, la Corte ritiene che la direttiva 2006/24 non preveda norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta. Pertanto, tale direttiva comporta un'ingerenza nei diritti fondamentali di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione, senza che l'ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario. Inoltre, per quanto riguarda le norme relative alla sicurezza e alla protezione dei dati conservati, la direttiva non prevede garanzie sufficienti, come richieste dall'art. 8 della Carta, che permettano di assicurare una protezione efficace dei dati conservati contro i rischi di abuso, nonché contro eventuali accessi e usi illeciti di tali dati.

Pertanto, la Corte conclude che, adottando la direttiva 2006/24, il legislatore dell'Unione ha ecceduto i limiti imposti nel rispetto del principio di proporzionalità alla luce degli artt. 7 e 8 e 52, par. 1, della Carta.

c. Esito a livello nazionale

Non disponibile.

5. Analisi

e. Il ruolo della Carta

A fronte delle domande in via pregiudiziale poste dal giudice irlandese, e concernenti il rispetto del principio di leale collaborazione di cui all'art. 4, par. 3, TUE e il principio di proporzionalità ai sensi dell'art. 5, par. 4, TUE, la Corte di giustizia ha deciso di incentrare il proprio ragionamento sugli artt. 7 e 8 della Carta, che sanciscono rispettivamente il diritto alla protezione della vita privata e la tutela dei dati personali.

La Corte, quindi, dopo aver constatato che la direttiva implica un'ingerenza "di vasta portata e [quindi] particolarmente grave" (par. 37) rispetto ai diritti garantiti dagli artt. 7 e 8 della Carta, procede ad esaminare se tale ingerenza possa essere giustificata alla luce di quanto previsto dall'art. 52, par. 1. La Corte conclude che:

"*Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, 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*".

La Corte sofferma la propria analisi sul rispetto del principio di proporzionalità, il quale esige che gli atti delle istituzioni dell'Unione siano idonei a realizzare gli obiettivi da essi perseguiti e non superino i limiti di ciò che è appropriato e necessario al conseguimento degli obiettivi stessi.

Proprio in riferimento alla questione se l'ingerenza prevista dalla direttiva nei diritti fondamentali sia limitata a ciò che è "strettamente necessario", la Corte rileva che, pur perseguendo il fine della tutela della sicurezza pubblica, "tale direttiva comporta un'ingerenza nei [diritti fondamentali sanciti dagli artt. 7 e 8 della Carta] di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione, senza che siffatta ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario" (par. 65).

Per tali ragioni, la Corte rileva che il legislatore dell'Unione ha ecceduto i limiti imposti dal rispetto del principio di proporzionalità e dichiara invalida la direttiva.

I diritti fondamentali alla tutela della vita privata e alla protezione dei dati personali assumono quindi un ruolo centrale come parametro di validità degli atti dell'Unione, anche se questi ultimi hanno come obiettivo (legittimo) quello di garantire la sicurezza pubblica.

f. Dialogo giuridico

Interazione verticale tra i giudici nazionali, *High Court* (Irlanda) e *Verfassungsgerichtshof* (Austria), e la Corte di giustizia attraverso il meccanismo del rinvio pregiudiziale di validità.

Interazione orizzontale, attraverso il rinvio, da parte della Corte di giustizia, a numerose sentenze della Corte EDU relative al test di proporzionalità dell'ingerenza nei diritti fondamentali.

g. Impatto della decisione della Corte di giustizia

La sentenza *Digital Rights Ireland* rappresenta il primo caso in cui la Corte ha deciso di dichiarare invalido un atto di diritto dell'Unione per violazione dei diritti fondamentali di cui agli artt. 7 e 8 della Carta.

Già nella sentenza *Schwarz*[35], la Corte era stata investita di una questione riguardante la validità di una direttiva rispetto agli artt. 7 e 8 della Carta. Tuttavia, in quel caso, la Corte aveva ritenuto che l'ingerenza in tali diritti si limitasse a quanto strettamente necessario per raggiungere gli obiettivi prefissati dal regolamento relativo alla raccolta e conservazione delle impronte digitali nei passaporti. La Corte aveva pertanto concluso che il principio di proporzionalità fosse stato rispettato dal legislatore dell'Unione.

La sentenza in oggetto ha avuto un forte impatto sulla giurisprudenza successiva in materia di bilanciamento tra protezione dei dati personali e sicurezza. Nella sentenza *Tele2 Swerige*[36], la Corte ha precisato la portata della sentenza *Digital Rights Ireland* in un contesto nazionale, valutando la compatibilità, rispetto agli artt. 7 e 8 della Carta, di una normativa nazionale che prevedeva l'obbligo generale e indifferenziato di conservazione dei dati relativi al traffico e all'ubicazione di comunicazioni elettroniche, e che consentiva l'accesso a tali dati da parte di talune autorità nazionali.

Inoltre, la Corte è stata chiamata a rendere un parere[37] circa la compatibilità con la Carta di un progetto di accordo tra l'Unione europea e il Canada sul trasferimento dei dati relativi al codice di prenotazione dei passeggeri aerei. Anche nel parere, la Corte ha proceduto verificando se le interferenze con i diritti tutelati dagli artt. 7 e 8 della Carta potessero essere giustificate alla luce dell'art. 52, par. 1, della Carta, e richiamando quanto già affermato nella sentenza *Digital Rights Ireland*.

h. Altri casi rilevanti

- Corte di giustizia (Grande sezione), sentenza del 21 dicembre 2016*, Tele2 Sverige e Watson*, cause riunite C-203/15 e C-698/15 ;
- Parere della Corte di Giustizia (Grande sezione) del 26 luglio 2017, ai sensi dell'art. 218, par. 11, TFUE, sulla richiesta presentata il 30 gennaio 2015 dal Parlamento europeo.

[35] Corte di giustizia, sentenza 17 ottobre 2013, *Schwarz*, C-291/12
[36] Corte di giustizia (Grande sezione), sentenza del 21 dicembre 2016, Tele2 Sverige e Watson, cause riunite C-203/15 e C-698/15
[37] Parere della Corte di giustizia (Grande sezione) del 26 luglio 2017, *parere 1/15*

Scheda n. 3 – Il diritto all'oblio

- Corte di giustizia (Grande sezione), sentenza del 13 maggio 2014, *Google Spain SL*, causa C-131/12

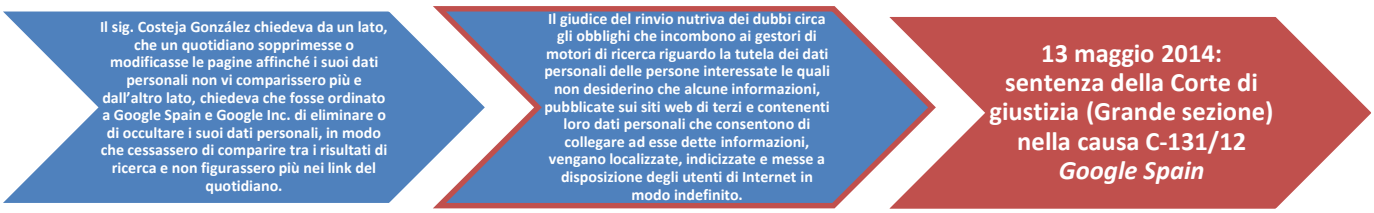
1. Aspetti centrali

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 secondo un determinato ordine di preferenza, deve essere qualificata come «trattamento di dati personali». Inoltre, nella misura in cui l'attività di un motore di ricerca può incidere, in modo significativo e in aggiunta all'attività degli editori di siti web, sui diritti fondamentali alla vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca, quale soggetto che determina le finalità e gli strumenti di questa attività, deve essere qualificato come responsabile del trattamento. Egli deve quindi assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che detta attività soddisfi le prescrizioni della direttiva 95/46, affinché le garanzie previste da quest'ultima possano sviluppare pienamente i loro effetti e possa essere effettivamente realizzata una tutela efficace e completa delle persone interessate, in particolare del loro diritto al rispetto della loro vita privata.
Un trattamento di dati personali deve essere considerato come effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro qualora il gestore di un motore di ricerca, con sede in uno Stato 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 si diriga agli abitanti di detto Stato membro.
Il gestore di un motore di ricerca è obbligato a sopprimere i *link* verso pagine web pubblicate da terzi, e contenenti informazioni relative a questa persona, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona. Tale obbligo sussiste ugualmente 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.
Sulla scorta dei diritti fondamentali derivanti dagli artt. 7 e 8 della Carta, l'interessato ha diritto a chiedere che un'informazione che lo riguarda non venga più messa a disposizione del grande pubblico mediante la sua inclusione in un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome. Tale diritto sussiste a prescindere dal fatto che l'inclusione dell'informazione nell'elenco arrechi pregiudizio alla persona interessata. Infatti, in linea di principio, i diritti fondamentali di cui agli artt. 7 e 8 della Carta prevalgono non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome della persona. Tuttavia, così non sarebbe qualora risultasse che, per ragioni particolari, l'ingerenza nei diritti fondamentali è giustificata dall'interesse preponderante del pubblico ad avere accesso, mediante l'inclusione summenzionata, all'informazione di cui trattasi.

2. A colpo d'occhio

Paese	Area	Riferimenti al diritto UE	Attori	Tecniche di Interazione giuridica	Esito
• Spagna	• Protezione dei dati personali	• Artt. 7, 8 CDFUE • Direttiva 95/46/CE [ora abrogata dal Regolamento 2016/679]	• Audiencia National (Spagna) • Corte di giustizia	• Verticale: Domanda di pronuncia pregiudiziale ai sensi dell'art. 267 TFUE sull'interpre tazione della direttiva 95/46/CE e dell'art. 8 della Carta	• L'interessato ha diritto, in base ai suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, a chiedere che un'informazione che lo riguarda non venga più messa a disposizione del grande pubblico mediante la sua inclusione in un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome

3. Cronologia



4. Descrizione

a. Fatti

Il sig. Costeja González, cittadino spagnolo con residenza in Spagna, presentava dinanzi all'autorità nazionale per la protezione dei dati un reclamo contro un quotidiano spagnolo di larga diffusione, nonché contro *Google Spain* e *Google Inc*. Infatti, nel momento in cui un utente inseriva il nome del sig. Costeja González nel motore di ricerca otteneva dei link verso le pagine del quotidiano sulle quali figurava l'annuncio di un pignoramento effettuato nei suoi confronti. Il sig. Costeja González chiedeva quindi, da un lato, che fosse ordinato al quotidiano di sopprimere o modificare tali pagine, affinché i suoi dati personali non vi comparissero più e, dall'altro lato, chiedeva che fosse ordinato a *Google Spain* e *Google Inc*. di eliminare o di occultare i suoi dati personali, in modo che cessassero di comparire tra i risultati di ricerca e non figurassero più nei link del quotidiano.

L'autorità nazionale aveva respinto il reclamo nella parte in cui era diretto contro il quotidiano, ritenendo che la pubblicazione delle informazioni in questione fosse giuridicamente giustificata dalla necessità di dare massima pubblicità alla vendita pubblica. L'autorità accoglieva, invece, il reclamo nella parte diretta contro *Google Spain* e *Google Inc*., ordinando la rimozione dei dati, nonché il divieto di accesso a taluni dati da parte dei gestori di motori di ricerca, qualora l'autorità stessa ritenga che la localizzazione e la diffusione degli stessi possano ledere il diritto fondamentale alla protezione dei dati e la dignità delle persone in senso ampio. Questo includerebbe anche la semplice volontà della persona interessata che tali dati non siano conosciuti da terzi. La stessa autorità aveva inoltre affermato che tale obbligo può incombere direttamente ai gestori di motori di

ricerca, senza che sia necessario cancellare i dati o le informazioni dal sito web in cui questi compaiono.

Google Spain e *Google Inc*. proponevano ricorso avverso tale decisione avanti *all'Audiencia Nacional*, la quale decideva di sospendere il procedimento e di sollevare più questioni pregiudiziali. Tali questioni riguardavano, in particolare, gli obblighi che incombono ai gestori di motori di ricerca per la tutela dei dati personali delle persone interessate, le quali non desiderino che alcune informazioni, pubblicate sui siti web di terzi e contenenti loro dati personali vengano localizzate, indicizzate e messe a disposizione degli utenti di Internet in modo indefinito. Secondo il giudice del rinvio, la risposta a tale quesito dipenderebbe dal modo in cui la direttiva 95/46 deve essere interpretata alla luce delle tecnologie che si sono affermate dopo la sua pubblicazione.

b. Ragionamento della Corte di giustizia

In primo luogo, la Corte di giustizia si sofferma sull'ambito di applicazione materiale della direttiva 95/46, in relazione alla questione se l'attività di un motore di ricerca quale fornitore di contenuti, 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, debba essere qualificata come "trattamento di dati personali" e, in caso affermativo, se il gestore di un motore di ricerca debba essere considerato come il "responsabile" del suddetto trattamento di dati personali.

Secondo la Corte, esplorando Internet in modo automatizzato, costante e sistematico alla ricerca delle informazioni ivi pubblicate, il gestore di un motore di ricerca "raccoglie" dati siffatti, che egli "estrae", "registra" e "organizza" successivamente nell'ambito dei suoi programmi di indicizzazione, "conserva" nei suoi server e, eventualmente, "comunica" e "mette a disposizione" dei propri utenti sotto forma di elenchi dei risultati delle loro ricerche. Tali operazioni, ai sensi della direttiva 95/46, sono qualificate come "trattamento", senza che rilevi il fatto che il gestore del motore di ricerca applichi le medesime operazioni anche ad altri tipi di informazioni e non distingua tra queste e i dati personali. Inoltre, non ha alcun rilievo il fatto che tali dati abbiano già costituito l'oggetto di pubblicazione su Internet e non vengano modificati dal motore di ricerca. Pertanto, tali operazioni devono essere considerate come "trattamento" ai sensi della direttiva anche nell'ipotesi in cui riguardino esclusivamente informazioni già pubblicate tali e quali nei media.

Per quanto riguarda la questione se il gestore del motore di ricerca debba essere considerato come il "responsabile del trattamento" dei dati personali, secondo la Corte è proprio il gestore del motore di ricerca a determinare le finalità e gli strumenti dell'attività in questione e, dunque, del trattamento di dati personali. Pertanto, è il gestore stesso a dover essere considerato come il "responsabile" del trattamento. A tale proposito, la Corte sottolinea che il trattamento di dati personali effettuato nell'ambito dell'attività di un motore di ricerca si distingue da (e si aggiunge a) quello effettuato dagli editori di siti web, consistente nel far apparire tali dati su una pagina Internet. Di conseguenza, non è rilevante il fatto che il gestore non eserciti alcun controllo sui dati personali pubblicati sulle pagine web da terzi. Inoltre, l'attività dei motori di ricerca svolge un ruolo decisivo nella diffusione globale dei dati, in quanto rende accessibili questi ultimi a qualsiasi utente di Internet che effettui una ricerca a partire dal nome della persona interessata, anche a quegli utenti che non avrebbero altrimenti trovato la pagina web su cui questi stessi dati sono pubblicati. A questo si deve aggiungere che l'organizzazione e l'aggregazione delle informazioni pubblicate su Internet, realizzate dai motori di ricerca allo scopo di facilitare ai loro utenti l'accesso a dette informazioni, possono avere come effetto che tali utenti, quando la loro ricerca viene effettuata a partire dal nome di una persona fisica, ottengono attraverso l'elenco di risultati una visione complessiva e strutturata delle informazioni relative a questa persona reperibili su Internet, che consente loro di stabilire un profilo più o meno dettagliato di quest'ultima.

Pertanto secondo la Corte, nella misura in cui l'attività di un motore di ricerca può incidere, in modo significativo e in aggiunta all'attività degli editori di siti web, sui diritti fondamentali alla vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca quale soggetto che determina le finalità e gli strumenti di questa attività deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che detta attività soddisfi le prescrizioni della direttiva 95/46. Le garanzie previste da quest'ultima devono, infatti, sviluppare pienamente i loro effetti; occorre, inoltre, e che una tutela efficace e completa delle persone interessate, in particolare del loro diritto al rispetto della loro vita privata, possa essere effettivamente realizzata.

In definitiva, quindi, la Corte ritiene che le attività poste in essere dal motore di ricerca siano qualificate come "trattamento dei dati personali" e il gestore del motore di ricerca debba essere considerato come "responsabile del trattamento" ai sensi della direttiva 95/46.

In secondo luogo, la Corte, si sofferma sull'ambito di applicazione territoriale della direttiva 95/46, al fine di stabilire a quali condizioni una filiale o succursale possa essere considerata responsabile del trattamento ai fini dell'applicazione della disciplina in materia di protezione dei dati personali. Infatti, nel caso di specie, *Google Inc*., società madre del gruppo Google con sede sociale negli Stati Uniti, gestisce *Google Search*, motore di ricerca con diverse versioni locali, destinato a indicizzare i siti web del mondo intero, e tra questi siti anche quelli ubicati in Spagna. In particolare, *Google Search* non si limita a dare accesso ai contenuti ospitati sui siti web indicizzati, ma sfrutta tale attività per includere, dietro pagamento, pubblicità associate ai termini di ricerca introdotti dagli utenti di Internet, a beneficio di imprese che desiderano utilizzare tale mezzo per offrire i loro beni o servizi a tali utenti. *Google Inc*. ha designato *Google Spain*, sua filiale, come responsabile per l'attività di promozione e vendita degli spazi pubblicitari per la Spagna.

La Corte prende quindi in considerazione il caso in cui il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale, destinata alla promozione e alla vendita degli spazi pubblicitari proposti dal motore di ricerca, e l'attività si diriga agli abitanti di tale Stato. Il giudice dell'Unione ritiene che, sebbene non sia dimostrato che *Google Spain* realizzi in Spagna un'attività direttamente connessa all'indicizzazione o alla memorizzazione di informazioni o di dati contenuti nei siti web di terzi, l'attività di promozione e di vendita degli spazi pubblicitari, di cui si occupa *Google Spain* per la Spagna, costituirebbe la parte essenziale dell'attività commerciale del gruppo Google e potrebbe essere considerata come strettamente connessa a *Google Search*.

In base alla direttiva, lo "stabilimento del responsabile del trattamento" implica l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile. Il fatto che la forma giuridica di siffatto stabilimento, si configuri come una semplice succursale o una filiale dotata di personalità giuridica, non è il fattore determinante a questo riguardo. Secondo la Corte, quindi, in base a quanto rilevato e alla nozione fornita dalla direttiva, *Google Spain*, filiale di *Google Inc*., si dedica all'esercizio effettivo e reale di un'attività mediante un'organizzazione in Spagna. Deve quindi essere considerato uno "stabilimento".

Inoltre, il trattamento di dati personali ad opera del responsabile deve essere effettuato nel contesto delle attività di uno stabilimento di questo, responsabile nel territorio di uno Stato membro. Secondo la Corte, il trattamento di dati personali realizzato per le esigenze di servizio di un motore di ricerca come *Google Search*, il quale venga gestito da un'impresa con sede in uno Stato terzo ma avente uno stabilimento in uno Stato membro, viene effettuato "nel contesto delle attività" di tale stabilimento qualora quest'ultimo sia destinato a garantire, in tale Stato membro, la promozione e la vendita degli spazi pubblicitari proposti dal suddetto motore di ricerca, che servono a rendere redditizio il servizio offerto da quest'ultimo. Infatti, in circostanze del genere, le attività del gestore

del motore di ricerca e quelle del suo stabilimento situato nello Stato membro interessato sono inscindibilmente connesse. Le attività relative agli spazi pubblicitari costituiscono, infatti, il mezzo per rendere il motore di ricerca in questione economicamente redditizio e il motore di ricerca è, al tempo stesso, lo strumento che consente lo svolgimento di dette attività. Inoltre, la visualizzazione di dati personali su una pagina di risultati di una ricerca è accompagnata, sulla stessa pagina, da quella di pubblicità correlate ai termini di ricerca. Si deve quindi constatare che il trattamento di dati personali in questione viene effettuato nel contesto dell'attività pubblicitaria e commerciale dello stabilimento del responsabile del trattamento nel territorio di uno Stato membro, nella fattispecie il territorio spagnolo.

Pertanto, 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, qualora il gestore di un motore di ricerca 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.

In terzo luogo, la Corte affronta la questione dell'estensione della responsabilità del gestore di un motore di ricerca. In particolare, viene affrontato il problema se quest'ultimo sia obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, 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 sia di per sé lecita.

La Corte rileva che qualsiasi persona può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali, e che tale autorità dispone di poteri investigativi e di poteri effettivi di intervento che le consentono di ordinare in particolare il congelamento, la cancellazione o la distruzione di dati, oppure di vietare a titolo provvisorio o definitivo un trattamento. Infatti, un trattamento di dati personali effettuato dal gestore di un motore di ricerca può incidere significativamente sui diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali nel caso in cui la ricerca, con l'aiuto di tale motore, venga effettuata a partire dal nome di una persona fisica. Detto trattamento consente, infatti, a qualsiasi utente di Internet di ottenere, mediante l'elenco di risultati, una visione complessiva strutturata delle informazioni relative a questa persona reperibili su Internet, che toccano potenzialmente una moltitudine di aspetti della sua vita privata e che, senza il suddetto motore di ricerca, non avrebbero potuto – o solo difficilmente avrebbero potuto – essere connesse tra loro. Ne consegue che, attraverso tale strumento, è possibile stabilire un profilo più o meno dettagliato di tale persona. Inoltre, l'effetto dell'ingerenza nei suddetti diritti della persona interessata risulta moltiplicato in ragione del ruolo importante che svolgono Internet e i motori di ricerca nella società moderna, i quali conferiscono alle informazioni contenute in un siffatto elenco di risultati a carattere ubiquitario.

Secondo la Corte, vista la gravità potenziale di tale ingerenza, quest'ultima non può essere giustificata dal semplice interesse economico del gestore di un motore di ricerca a questo trattamento di dati. Tuttavia, poiché la soppressione di link dall'elenco di risultati potrebbe, a seconda dell'informazione in questione, avere ripercussioni sul legittimo interesse degli utenti di Internet potenzialmente interessati ad avere accesso a quest'ultima, occorre ricercare, in situazioni quali quelle oggetto del procedimento principale, un giusto equilibrio, segnatamente tra tale interesse e i diritti fondamentali della persona di cui trattasi derivanti dagli artt. 7 e 8 della Carta. Se indubbiamente i diritti della persona interessata tutelati da tali artt. prevalgono, di norma, anche sull'interesse 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 suddetta, nonché dall'interesse del pubblico a disporre di tale informazione. Peraltro, tale interesse può variare a seconda del ruolo che tale persona riveste nella vita pubblica.

L'autorità di controllo nazionale può quindi ordinare al gestore di un motore di ricerca di sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a tale persona, senza che un'ingiunzione in tal senso presupponga che tale nome e tali informazioni siano previamente o simultaneamente cancellati dalla pagina web sulla quale sono stati pubblicati. Infatti, in primo luogo, non sarebbe possibile realizzare una tutela efficace e completa delle persone interessate nel caso in cui queste dovessero preventivamente, o contestualmente, ottenere dagli editori di siti web la cancellazione delle informazioni che le riguardano. In secondo luogo, il trattamento da parte dell'editore di una pagina web può, eventualmente, essere effettuato "esclusivamente a scopi giornalistici" e beneficiare così di deroghe alle prescrizioni dettate dalla direttiva 95/46/CE. Non sembra invece integrare tale ipotesi il trattamento effettuato dal gestore di un motore di ricerca. Infine, il bilanciamento degli interessi in gioco 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 web, in quanto, da un lato, i legittimi interessi che giustificano questi trattamenti possono essere differenti; dall'altro, le conseguenze che tali trattamenti hanno per la persona interessata, e segnatamente per la sua vita privata, non sono necessariamente le stesse. Infatti, l'inclusione nell'elenco di risultati – che appare a seguito di una ricerca effettuata a partire dal nome di una persona – di una pagina web e delle informazioni in essa contenute relative a questa persona, poiché facilita notevolmente l'accessibilità di tali informazioni a qualsiasi utente di Internet e può svolgere un ruolo decisivo per la diffusione di dette informazioni, è idonea a costituire un'ingerenza più rilevante nel diritto fondamentale al rispetto della vita privata della persona interessata che non la pubblicazione da parte dell'editore della suddetta pagina web.

Pertanto, la Corte ritiene che il gestore di un motore di ricerca è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, 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.

Infine, la Corte valuta la portata dei diritti garantiti all'individuo interessato, in particolare il diritto a che l'informazione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome. In proposito occorre sottolineare che la constatazione di un diritto siffatto non presuppone che l'inclusione dell'informazione in questione nell'elenco di risultati arrechi un pregiudizio all'individuo. Secondo la Corte, dato che quest'ultimo può, sulla scorta dei suoi diritti fondamentali derivanti dagli artt. 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 fondamentali prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di una 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 fosse giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, mediante l'inclusione summenzionata, all'informazione di cui trattasi.

La Corte affronta, infine, la questione relativa alla visualizzazione – nell'elenco di risultati che l'utente di Internet ottiene effettuando una ricerca a partire dal nome della persona interessata con

l'aiuto di *Google Search* – di link verso pagine degli archivi online di un quotidiano, contenenti annunci che menzionano il nome di tale persona e si riferiscono ad un'asta immobiliare legata ad un pignoramento effettuato per la riscossione coattiva di crediti previdenziali. A questo proposito, la Corte afferma che, tenuto conto del carattere sensibile delle informazioni contenute in tali annunci per la vita privata di detta persona, nonché del fatto che la loro pubblicazione iniziale era stata effettuata sedici anni prima, la persona interessata vanta un diritto a che tali informazioni non siano più collegate al suo nome attraverso un elenco siffatto. Inoltre, secondo la Corte, non sussistono ragioni particolari giustificanti un interesse preponderante del pubblico ad avere accesso a tali informazioni.

c. Esito a livello nazionale

Non disponibile.

5. Analisi

d. Il ruolo della Carta

Gli artt. 7 e 8 della Carta vengono in rilievo nella presente sentenza quale parametro interpretativo della direttiva 95/46, ora abrogata dal regolamento n. 267/16.

In particolare, in assenza di una specifica disposizione contenuta nella normativa secondaria, la Corte ha fatto discendere dall'interpretazione degli artt. 7 e 8 della Carta il diritto di un singolo a che l'informazione riguardante la sua persona non venga più collegata al suo nome da un elenco di risultati che appare a seguito di un ricerca effettuata su un motore di ricerca a partire dal suo nome (c.d. diritto all'oblio).

La Corte ha, infatti, effettuato un bilanciamento tra i diritti fondamentali sanciti dagli artt. 7 e 8 della Carta e da un lato, l'interesse economico del gestore del motore di ricerca e, dall'altro lato, l'interesse del pubblico ad accedere all'informazione in occasione di una ricerca sul motore di ricerca relativa al nome della persona interessata. La Corte ha in ogni caso ritenuto prevalenti i primi rispetto all'interesse economico del motore di ricerca e all'interesse del pubblico a essere informato.

e. Dialogo giuridico

Interazione verticale tra il giudice nazionale, *l'Audiencia National* (Spagna) e la Corte di giustizia attraverso il meccanismo del rinvio pregiudiziale.

f. Impatto della decisione della Corte di giustizia

Con l'entrata in vigore del GDPR, si distingue la nozione di "titolare del trattamento" e di "responsabile del trattamento": il primo è definito 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 di dati personali" (art. 4, par. 7). È invece definito "responsabile del trattamento" "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" (art. 4, par. 8). Nel caso di specie, seguendo la definizione del regolamento, il gestore del motore di ricerca dovrebbe quindi essere definito "titolare del trattamento".

Nella sentenza in oggetto, la Corte di giustizia ha riconosciuto, per la prima volta, il diritto all'oblio. Con l'entrata in vigore del regolamento 679/16, che ha abrogato la direttiva 95/46, è stato introdotto l'art. 17, relativo al diritto alla cancellazione (o diritto all'oblio), il quale riprende quanto affermato dalla Corte di giustizia nella sentenza *Google Spain*.

In base a tale articolo, infatti,

"*1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:*

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) *per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria*".

g. Altri casi rilevanti

Sulla responsabilità delle filiali e società:

- Corte di giustizia (Grande sezione), sentenza del 5 giugno 2018, *Wirtschaftakedemie*, C-2010/16.

Scheda n. 4 – Trasferimento dei dati personali verso Stati terzi che non assicurano un livello di protezione adeguato

- Corte di giustizia (Grande sezione), sentenza del 6 ottobre 2015, *Schrems*, causa C-362/14

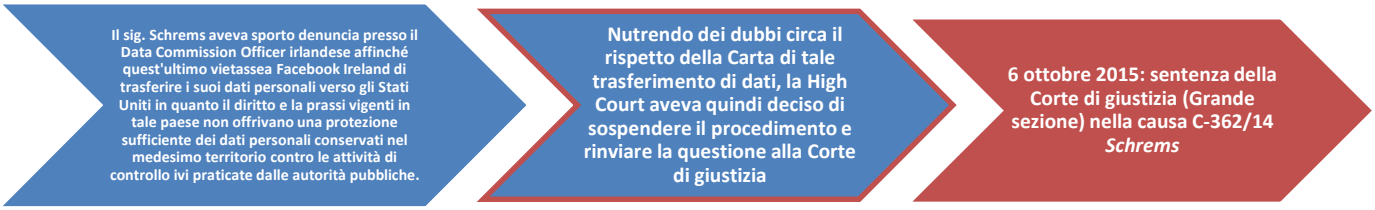
1. Aspetti centrali

Anche in presenza di una decisione della Commissione che constati che uno Stato terzo garantisce un livello di protezione adeguato, le autorità nazionali di controllo investite da una persona di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei dati personali che la concernono, devono poter verificare, in piena indipendenza, se il trasferimento di tali dati verso lo Stato terzo oggetto della decisione rispetti i requisiti fissati dal diritto dell'Unione.
Se, all'esito di tale esame, l'autorità pervenga alla conclusione che gli elementi addotti a sostegno di una tale domanda siano privi di fondamento e, per questo motivo, la respinga, la persona interessata deve avere accesso ai mezzi di ricorso giurisdizionali che le consentono di contestare la decisione adottata dalla Commissione dinanzi ai giudici nazionali. Tali giudici dovranno quindi sospendere la decisione e investire la Corte di un procedimento pregiudiziale per accertamento di validità.
Nell'ipotesi, invece, in cui l'autorità reputi fondate le censure sollevate dalla persona che l'ha investita di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei suoi dati personali, questa stessa autorità deve promuovere azioni giudiziarie affinché i giudici nazionali procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, a un rinvio pregiudiziale di validità.
La decisione adottata dalla Commissione, con la quale essa constata che gli Stati Uniti garantiscono un livello di protezione adeguato, viola i requisiti fissati dalla direttiva 95/46 letta alla luce della Carta ed è, pertanto, invalida.

2. A colpo d'occhio

Paese	Area	Riferimenti al diritto UE	Attori	Tecniche di Interazione giuridica	Esito
• Irlanda	• Protezione dei dati personali • Trasfrimento dei dati verso Paesi terzi	• Art. 7, 8 e 47 CDFUE • Direttiva 95/46/CE • Decisione della Commissione 2000/529/CE	• High Court (Corte d'appello, Irlanda) • Corte di giustizia	• Verticale: Domanda di pronuncia pregiudiziale ai sensi dell'art. 267 TFUE sull'interpre tazione della direttiva 95/46/CE • Verticale: domanda di pronuncia pregiudiziale sulla validità della decisione della Commissione	• La decisione della Commissione che constata un livello di tutela adeguato negli Stati Uniti è invalida

3. Cronologia



4. Descrizione

a. Fatti

Il sig. Schrems, cittadino austriaco residente in Austria, aveva aperto un profilo su Facebook. L'iscrizione sul social network comporta la sottoscrizione di un contratto con *Facebook Ireland*, una controllata di *Facebook Inc*., situata negli Stati Uniti. I dati personali degli utenti di Facebook residenti nel territorio dell'Unione vengono quindi trasferiti, in tutto o in parte, su server di *Facebook Inc*. ubicati nel territorio degli Stati Uniti, ove essi sono oggetto di trattamento.

A seguito delle rivelazioni fatte da Edward Snowden, informatico e attivista statunitense, relative alle attività di sorveglianza elettronica e di intercettazione dei dati da parte dei servizi di intelligence degli Stati Uniti, il sig. Schrems aveva sporto denuncia presso il *Data Protection Commissioner* irlandese, affinché quest'ultimo vietasse a *Facebook Ireland* di trasferire i suoi dati personali verso gli Stati Uniti. In particolare, il sig. Schrems sosteneva che il diritto e la prassi vigenti in tale Stato non offrivano una protezione sufficiente dei dati personali conservati nel medesimo territorio contro le attività di controllo ivi praticate dalle autorità pubbliche.

Il *Data Protection Commissioner* aveva respinto la denuncia, in quanto priva di fondamento. In particolare, il ricorrente aveva richiamato la decisione 2000/520/CE della Commissione[38], adottata sulla base della direttiva 95/46/CE, la quale attribuisce alla Commissione o agli Stati membri la competenza a constatare che uno Stato terzo assicura un livello di protezione adeguato dei diritti fondamentali. Con tale decisione, la Commissione aveva constatato che gli Stati Uniti assicuravano un livello di protezione adeguato.

Il sig. Schrems aveva quindi proposto ricorso dinanzi alla *High Court* (Corte d'appello irlandese), la quale aveva constato che la sorveglianza elettronica e l'intercettazione dei dati personali trasferiti dall'Unione verso gli Stati Uniti rispondevano a finalità necessarie e indispensabili per l'interesse pubblico. Tuttavia, una volta che i dati personali erano stati trasferiti verso gli Stati Uniti, i competenti organi federali potevano avere accesso a tali dati nell'ambito della sorveglianza e delle intercettazioni indifferenziate da essi praticate su larga scala. Nutrendo dubbi circa il rispetto dell'art. 8 della Carta, la *High Court* aveva quindi deciso di sospendere il procedimento e di rinviare la questione in via pregiudiziale alla Corte di giustizia. In particolare, i giudici nazionali chiedevano se il *Data Protection Officer* fosse vincolato dalla constatazione effettuata dalla Commissione nella sua decisione, secondo la quale gli Stati Uniti garantiscono un livello di protezione adeguato, oppure se l'art. 8 della Carta autorizzasse il *Data Protection Officer* a discostarsi, nel caso, da una siffatta constatazione.

b. Ragionamento della Corte di giustizia

[38] Decisione 2000/520/CE della Commissione del 26 luglio 2000, a norma della direttiva 95/46 sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "Domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti (GU L 215, p.7)

La Corte decide di analizzare congiuntamente le due domande in via pregiudiziale. Con esse veniva chiesto dal giudice nazionale se una decisione come quella adottata dalla Commissione - in cui si rileva che uno Stato terzo assicura un livello di protezione adeguato - impedisca a un'autorità di controllo di uno Stato membro di esaminare la domanda di una persona relativa al trattamento di dati personali trasferiti da uno Stato membro a quello Stato terzo. Questo in particolare qualora l'individuo affermi che il diritto e la prassi in vigore nello Stato in questione non assicurino un livello di protezione adeguato.

La Corte, in primo luogo, prende in esame i poteri delle autorità di controllo degli Stati membri, in presenza di una decisione della Commissione che costata l'adeguatezza della protezione assicurata al trattamento dei dati da uno Stato terzo.

Secondo la Corte, se da un lato, tali autorità non dispongono di poteri con riguardo ai trattamenti di dati effettuati nel territorio di uno Stato terzo, dall'altro lato l'operazione consistente nel far trasferire dati personali da uno Stato membro verso uno Stato terzo costituisce, di per sé, un trattamento di dati personali effettuato nel territorio di uno Stato membro. Le autorità nazionali di controllo sono quindi investite della competenza a verificare se un trasferimento di dati personali dal proprio Stato membro verso uno Stato terzo rispetti i requisiti fissati dalla direttiva 95/46/CE.

In particolare, tale direttiva pone come requisito che siffatti trasferimenti di dati verso paesi terzi che non offrono un livello di protezione adeguato devono essere vietati. A questo proposito, la direttiva 95/46/CE riconosce che sia la Commissione sia gli Stati membri possono constatare che uno Stato terzo assicura tale livello di protezione. Qualora la Commissione adotti una siffatta decisione, gli Stati membri sono tenuti ad adottare le misure necessarie per conformarvisi. Pertanto, fino a che la decisione della Commissione non sia stata dichiarata invalida dalla Corte, gli Stati membri e i loro organi non possono adottare misure contrarie a tale decisione.

Tuttavia, una decisione della Commissione non può impedire alle persone i cui dati personali sono stati o potrebbero essere trasferiti verso uno Stato terzo di investire le autorità nazionali di controllo di una domanda relativa ai propri diritti e alle loro libertà con riguardo al trattamento dei dati. Infatti una decisione di tale natura non può né elidere né ridurre i poteri espressamente riconosciuti alle autorità nazionali di controllo dall'art. 8, par. 3, della Carta. Inoltre, sarebbe contrario al sistema predisposto dalla direttiva 95/46/CE se una decisione della Commissione avesse come effetto di impedire a una autorità nazionale di controllo di esaminare la domanda di una persona relativa alla protezione dei suoi dati personali che sono stati o potrebbero essere trasferiti verso lo Stato terzo interessato.

In definitiva, secondo la Corte, anche in presenza di una decisione della Commissione, le autorità nazionali di controllo investite da una persona di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei dati personali che la riguardano, devono poter verificare, in piena indipendenza, se il trasferimento di tali dati verso Paesi terzi rispetti i requisiti fissati dal diritto dell'Unione. Infatti, se così non fosse, le persone i cui dati personali sono stati o potrebbero essere trasferiti verso lo Stato terzo sarebbero private del diritto, garantito dall'art. 8, par. 1 e 3, della Carta, di investire le autorità nazionali di controllo di una domanda ai fini della protezione dei loro diritti fondamentali.

In tal caso, una domanda con la quale una persona, i cui dati sono stati o potrebbero essere trasferiti verso uno Stato terzo, fa valere che il diritto e la prassi di tale Stato non assicurano un livello di protezione adeguato, deve essere intesa nel senso che essa verte sulla compatibilità di tale decisione con la protezione della sua vita privata e delle sue libertà e diritti fondamentali.

Tuttavia, in questo caso, in base a una giurisprudenza consolidata della Corte di giustizia, le autorità nazionali di controllo non sono competenti a constatare esse stesse l'invalidità di una tale decisione. La Corte indica, quindi, le modalità attraverso le quali è possibile contestare la validità della decisione che constata il livello di protezione adeguato, partendo dalla premessa che l'autorità di controllo dovrà esaminare la domanda della persona con tutta la diligenza richiesta. Se, all'esito di tale esame, l'autorità pervenga alla conclusione che gli elementi addotti a sostegno di una tale domanda siano privi di fondamento, e per questo motivo, la respinga, in base alla direttiva 95/46, in combinato disposto con l'art. 47 della Carta, la persona interessata deve avere accesso ai mezzi di ricorso giurisdizionali che le consentono di contestare la decisione adottata dalla Commissione dinanzi ai giudici nazionali. Tali giudici dovranno quindi sospendere la decisione e investire la Corte di un procedimento pregiudiziale per accertamento di validità.

Nell'ipotesi, invece, in cui l'autorità nazionale reputi fondate le censure sollevate dalla persona che l'ha investita di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei suoi dati personali, questa stessa autorità deve promuovere azioni giudiziarie. A tal riguardo, la Corte esorta il legislatore nazionale a prevedere dei mezzi di ricorso che consentano all'autorità nazionale di controllo di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, a un rinvio pregiudiziale di validità.

In secondo luogo, la Corte esamina la validità della decisione della Commissione con cui si constata che gli Stati Uniti assicurano un livello di protezione adeguato, rispetto ai requisiti posti dalla direttiva 95/46/CE letta alla luce della Carta.

La Corte rileva che nessuna disposizione di diritto dell'Unione stabilisce che cosa debba intendersi per "livello di protezione adeguato". Tuttavia, è possibile ritenere che, se da un lato, tale espressione deve essere intesa nel senso che non possa esigersi da uno Stato terzo un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione, dall'altro lato, l'espressione "livello di protezione adeguato" deve essere intesa nel senso che tale Stato deve assicurare effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione. Infatti, in assenza di un siffatto requisito, l'obiettivo della continuità del livello elevato di tale protezione in caso di trasferimento di dati sarebbe disatteso. Inoltre, il livello elevato di protezione garantito dalla direttiva 95/46, letta alla luce della Carta, potrebbe essere facilmente eluso da trasferimenti di dati personali dall'Unione verso Stati terzi ai fini del loro trattamento in tali paesi.

La Commissione è, quindi, tenuta a valutare se il contenuto delle norme applicabili nello Stato terzo sia idoneo a garantire un livello di protezione adeguato. Allo stesso modo, incombe alla Commissione, successivamente all'adozione di una decisione, verificare periodicamente se la constatazione relativa al livello di protezione adeguato assicurato dallo Stato terzo continui ad essere giustificata in fatto e in diritto. Il potere discrezionale della Commissione in ordine all'adeguatezza del livello di protezione assicurato da uno Stato terzo risulta così ridotto alla luce, da un lato, del ruolo importante svolto dalla protezione dei dati personali sotto il profilo del diritto fondamentale al rispetto della vita privata e, dall'altro, del numero significativo di persone i cui diritti fondamentali possono essere violati in caso di trasferimento di dati personali verso uno Stato terzo che non assicura un livello di protezione adeguato.

La Corte prende quindi in esame, da un lato, il livello di protezione garantito dall'ordinamento degli Stati Uniti e, dall'altro lato, il livello di protezione delle libertà e dei diritti fondamentali garantito all'interno dell'Unione. La Corte, richiamando la precedente sentenza *Digital Rights*

Ireland, sottolinea, in particolare, che una normativa dell'Unione, che comporta un'ingerenza nei diritti fondamentali garantiti dagli artt. 7 e 8 della Carta, deve prevedere regole chiare e precise in relazione alla portata e all'applicazione della misura restrittiva. Le stesse norme devono imporre requisiti minimi, in modo tale che le persone interessate dispongano di garanzie sufficienti a proteggere efficacemente i loro dati contro il rischio di abusi, nonché contro eventuali accessi e usi illeciti dei suddetti dati. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi. Inoltre deroghe e restrizioni alla tutela dei dati personali devono operare entro i limiti dello stretto necessario.

Partendo da tali presupposti, la Corte rileva, in particolare, due aspetti della normativa degli Stati Uniti non in linea con il livello di tutela dei diritti fondamentali, in particolare del diritto alla tutela della vita privata, garantito all'interno dell'Unione. In primo luogo, secondo la Corte, non è limitata allo stretto necessario una normativa che autorizzi in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati siano stati trasferiti dall'Unione verso gli Stati Uniti 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 e 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, garantito dall'art. 7 della Carta.

In secondo luogo, 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 a una tutela giurisdizionale effettiva, quale sancito all'art. 47 della Carta. A tal riguardo, l'esistenza stessa di un controllo giurisdizionale effettivo, destinato ad assicurare il rispetto delle disposizioni del diritto dell'Unione, è inerente all'esistenza di uno Stato di diritto.

Infine, la decisione della Commissione priva le autorità nazionali di controllo dei poteri che sono loro attribuiti dalla direttiva 95/46/CE nel caso in cui una persona adduca elementi idonei a rimettere in discussione il fatto che una decisione della Commissione che ha constatato che uno Stato terzo garantisce un livello di protezione adeguato, sia compatibile con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

Per tali ragioni, la Corte ritiene che il livello di tutela garantito dalla normativa degli Stati Uniti non sia almeno equivalente a quello assicurato all'interno dell'Unione e che pertanto, la decisione adottata dalla Commissione sia invalida.

c. Esito a livello nazionale

Non disponibile.

5. Analisi

h. Il ruolo della Carta

Nella sentenza, la Corte è chiamata a pronunciarsi sia sull'interpretazione della direttiva 95/46/CE [ora abrogata dal regolamento 16/279/UE] alla luce degli artt. 7 (diritto al rispetto della vita privata), 8 (diritto alla protezione dei dati di carattere personale) e 47 (diritto ad un ricorso

effettivo e a un giudice imparziale) sia sulla decisione 2000/529/CE della Commissione relativa all'adeguatezza della protezione offerta dagli Stati Uniti d'America.

In primo luogo, la Corte, interpretando la direttiva alla luce della Carta, e in particolare del suo art. 8, amplia i poteri di controllo attribuiti alle autorità nazionali. Infatti, anche in presenza di una decisione della Commissione che constati l'adeguatezza della protezione offerta da uno stato terzo, l'autorità nazionale deve poter comunque verificare, in piena indipendenza, se il trasferimento dei dati verso tale stato terzo rispetti i requisiti fissati dal diritto dell'Unione. Secondo la Corte, infatti, "[s]e così non fosse, le persone i cui dati personali sono stati o potrebbero essere trasferiti verso lo Stato terzo di cui trattasi sarebbero private del diritto, garantito all'art. 8, parr. 1 e 3, della Carta, di investire le autorità nazionali di controllo di una domanda ai fini della protezione dei loro diritti fondamentali" (par. 58).

Inoltre, dal combinato disposto della direttiva e dell'art. 47 della Carta, la Corte traccia le modalità attraverso le quali un singolo può contestare la validità di una decisione adottata dalla Commissione, sia nel caso in cui l'autorità nazionale ritenga che gli elementi addotti a sostegno della domanda siano privi di fondamento, sia quando tale autorità reputi fondate le censure sollevate dalla persona.

In secondo luogo, la Carta è utilizzata quale parametro di validità dalla Corte di giustizia rispetto a una decisione adottata dalla Commissione e relativa all'adeguatezza della protezione offerta da uno Stato terzo. In questo caso, la Corte interpreta la nozione di "protezione adeguata" come "sostanzialmente equivalente" e riscontra una violazione della direttiva 95/46/CE letta alla luce della Carta, in quanto la tutela offerta negli Stati Uniti non poteva essere considerata sostanzialmente equivalente a quella prevista a livello di Unione europea.

i. Dialogo giuridico

Interazione verticale tra il giudice nazionale, la *High Court* irlandese e la Corte di giustizia attraverso il meccanismo del rinvio pregiudiziale.

j. Impatto della decisione della Corte di giustizia

La sentenza *Schrems* rappresenta una tappa importante nella giurisprudenza della Corte. Viene infatti riconosciuto il ruolo centrale rivestito dalle autorità nazionali incaricate della protezione dei dati nel tutelare i diritti fondamentali dei singoli, in particolare il diritto alla tutela della vita privata e alla protezione dei dati. La Corte ha inoltre avuto modo di chiarire le modalità attraverso le quali valutare il livello di tutela "adeguato" e, in tal senso, i diversi compiti attribuiti alla Commissione europea, alle corti nazionali e alla Corte di giustizia, nonché alle autorità di controllo nazionali.

Con l'entrata in vigore del regolamento 16/279/UE, che ha abrogato la direttiva 95/46/CE, il Capo V (artt. 44-50) è ora dedicato a "Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali". La disciplina attuale appare più dettagliata rispetto a quella contenuta nella direttiva e, in parte, recepisce la giurisprudenza della Corte di giustizia in materia.

k. Altri casi rilevanti

Sulle limitazioni ai diritti fondamentali:

- Corte di giustizia (Grande sezione), sentenza dell'8 aprile 2014, *Digital Rights Ireland*, cause riunite C-293/12 e C-594/12.

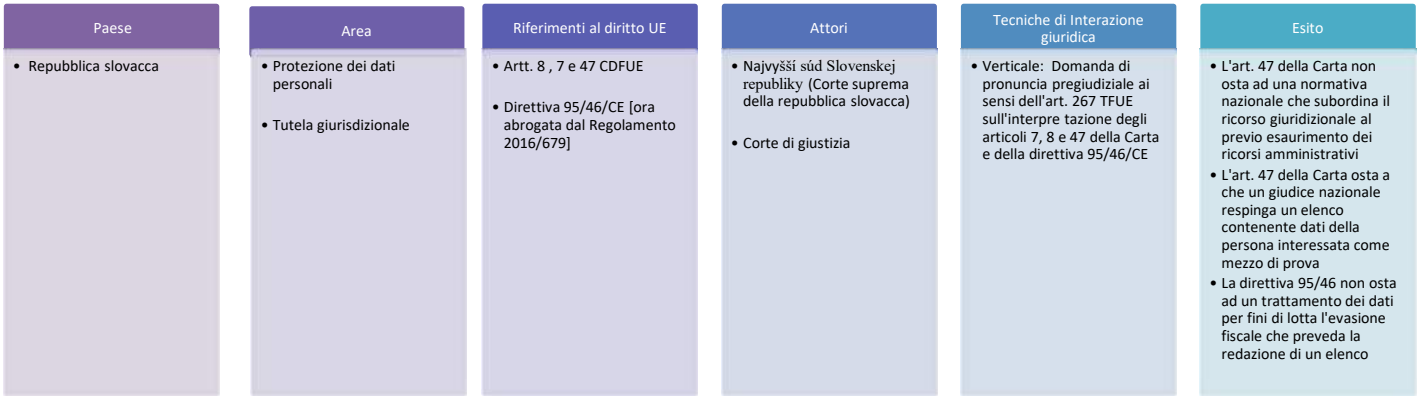
Scheda n. 5 – La tutela dei dati personali nel caso di trattamento ai fini della riscossione delle imposte e della lotta contro la frode fiscale

- Corte di giustizia, sentenza del 27 settembre 2017, *Puškár*, causa C-73/16

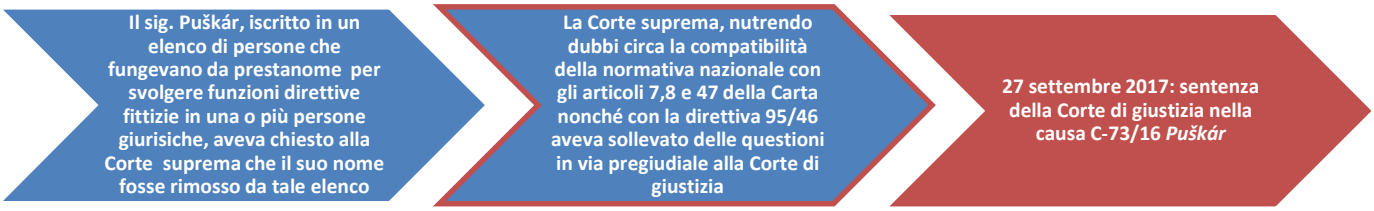
1. Aspetti centrali

L'art. 47 della Carta non osta a una normativa nazionale che subordina la possibilità di esperire un ricorso in via giurisdizionale per la tutela dei dati personali al previo esaurimento dei rimedi disponibili dinanzi alle autorità amministrative nazionali, a condizione che le modalità concrete di esercizio di detti rimedi non pregiudichino eccessivamente il diritto a un ricorso effettivo. In particolare, l'esaurimento dei rimedi amministrativi disponibili non comporti un ritardo sostanziale per la proposizione di un ricorso giurisdizionale, produca la sospensione della prescrizione dei diritti considerati e non provochi costi eccessivi.
L'art. 47 della Carta osta a che un giudice nazionale respinga, quale mezzo di prova di una violazione della tutela dei dati personali, un elenco presentato dalla persona interessata e contenente dati personali di quest'ultima, qualora tale persona si sia procurata l'elenco senza il consenso, previsto dalla legge, del responsabile del trattamento di detti dati, a meno che tale rigetto sia previsto dalla normativa nazionale e rispetti, al tempo stesso, il contenuto essenziale del diritto a un ricorso effettivo e il principio di proporzionalità.
Un trattamento dei dati personali da parte delle autorità di uno Stato membro ai fini della riscossione delle imposte e della lotta alla frode fiscale, come quello a cui si procede con la redazione di un elenco di persone che rivestirebbero ruoli dirigenziali fittizi all'interno di persone giuridiche, senza il consenso delle persone interessate, è compatibile con il diritto dell'Unione, purché siano soddisfatte le seguenti condizioni: alle autorità nazionali sono stati affidati compiti di interesse pubblico dalla normativa nazionale; la redazione di tale elenco e l'iscrizione in quest'ultimo del nome delle persone interessate sono effettivamente idonee e necessarie al raggiungimento degli obiettivi perseguiti; sussistono elementi sufficienti per presumere che le persone interessate figurino a ragione in tale elenco; tutte le condizioni di liceità di tale trattamento dei dati personali imposte dalla direttiva 95/46 sono state soddisfatte.

2. A colpo d'occhio



3. Cronologia



4. Descrizione

a. Fatti

Il sig. Puškár era stato inserito dalla Direzione delle Finanze e l'Ufficio Crimini dell'amministrazione finanziaria della Repubblica Slovacca in un elenco di persone fisiche che fungevano da prestanome per rivestire funzioni direttive fittizie in una o più persone giuridiche. Il sig. Puškár, ritenendosi vittima di una violazione dei propri diritti della personalità a causa dell'inclusione del suo nome nell'elenco, aveva chiesto alla Corte suprema della Repubblica Slovacca che fosse ingiunto alla Direzione delle Finanze e alle altre amministrazioni finanziarie di non iscrivere il suo nome in tale elenco o in ogni altro elenco simile e che fosse cancellata qualsiasi indicazione che lo riguardasse.

La Corte suprema aveva respinto, in quanto infondato, il ricorso proposto dal sig. Puškár per motivi procedurali, in quanto il ricorrente non aveva esaurito i rimedi dinanzi alle autorità amministrative nazionali. Il sig. Puškár aveva quindi proposto ricorso alla Corte costituzionale della Repubblica Slovacca che, in base alla giurisprudenza della Corte europea dei diritti dell'uomo (Corte EDU), aveva ritenuto violati diversi diritti fondamentali del ricorrente, in particolare, il diritto a un equo processo, il diritto alla vita privata, nonché alla protezione dei dati personali. La Corte costituzionale aveva quindi annullato la decisione della Corte suprema e rinviato la causa dinnanzi a tale giudice per una nuova trattazione e una nuova pronuncia nel merito.

La Corte suprema aveva quindi deciso di sospendere il procedimento e di sollevare una questione in via pregiudiziale alla Corte di giustizia.

b. Ragionamento della Corte di giustizia

In via preliminare, la Corte verifica se la questione rientra nell'ambito di applicazione della direttiva 95/46/CE [ora abrogata dal regolamento 2016/679]. Infatti, tale direttiva non si applica al trattamento di dati personali aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato e le attività dello Stato in materia penale. Nel caso di specie, tuttavia, i dati erano stati raccolti e utilizzati ai fini della riscossione delle imposte e della lotta alla frode fiscale e non sono quindi ritenuti dalla Corte oggetto di esclusione.

Tali dati rientrano, secondo la Corte, nella nozione di "dati personali" ai sensi della direttiva 95/46, la quale espressamente prevede che gli Stati membri possano adottare disposizioni legislative intese a limitare la tutela dei dati qualora tale restrizione costituisca una misura necessaria alla salvaguardia di un interesse economico o finanziario di uno Stato membro anche in materia fiscale. Tali misure nazionali, come quelle oggetto del procedimento, rientrano quindi nell'ambito di applicazione della direttiva.

La prima questione affrontata della Corte riguarda l'interpretazione dell'art. 47 della Carta e se esso osti a una normativa nazionale che subordini la possibilità di esperire un ricorso

giurisdizionale, da parte di una persona che afferma sia stato violato il suo diritto alla tutela dei dati personali, al previo esaurimento dei rimedi disponibili dinanzi alle autorità amministrative nazionali.

La direttiva 95/46, pur richiedendo espressamente che gli Stati membri stabiliscano che chiunque possa disporre di un ricorso giurisdizionale, non disciplina le condizioni alle quali tale ricorso può essere proposto e non esclude che il diritto nazionale possa prevedere rimedi anche dinanzi alle autorità amministrative. Nel definire tali modalità procedurali, gli Stati membri devono tuttavia garantire il rispetto del diritto a un ricorso effettivo e a un giudice imparziale, come sancito dall'art. 47 della Carta.

Secondo la Corte, il fatto che una normativa nazionale subordini la ricevibilità di un ricorso giurisdizionale al previo esaurimento dei rimedi amministrativi disponibili introduce un passaggio aggiuntivo per l'accesso al giudice, che può rallentare l'accesso a un ricorso giurisdizionale e può comportare costi aggiuntivi. L'obbligo di esaurire i rimedi amministrativi disponibili integra, pertanto, pertanto una restrizione del diritto a un ricorso effettivo dinanzi a un giudice ai sensi dell'art. 47 della Carta e deve, quindi, rispettare le condizioni previste dall'art. 52, par. 1, della Carta perché possa essere considerato giustificato.

La Corte rileva quindi che tale limite è previsto dalla normativa nazionale e non rimette in questione il contenuto essenziale del diritto sancito dall'art. 47 della Carta. Inoltre, l'obbligo di esaurire i rimedi amministrativi risponde a obiettivi di interesse generale legittimi, in quanto mira ad alleggerire i giudici delle cause che possono essere decise direttamente dall'autorità amministrativa interessata, nonché a migliorare l'efficacia dei procedimenti giurisdizionali per quanto riguarda le controversie ove sia già stato presentato un reclamo. Inoltre, secondo la Corte, non emergono mezzi meno incisivi atti a conseguire altrettanto efficacemente detti obiettivi. Infine, la Corte ritiene che non risulta una sproporzione tra tali obiettivi e gli eventuali inconvenienti causati dall'obbligo di esaurire i rimedi amministrativi disponibili, a condizione tuttavia che le modalità concrete di esercizio di detti rimedi non pregiudichino eccessivamente il diritto a un ricorso effettivo dinanzi a un giudice. In particolare, secondo il giudice dell'Unione, è importante che: l'esaurimento dei rimedi amministrativi disponibili non comporti un ritardo sostanziale per la proposizione di un ricorso giurisdizionale; non produca la sospensione dei diritti considerati; e non provochi costi eccessivi.

In secondo luogo, la Corte valuta se l'art. 47 della Carta debba essere interpretato nel senso che osti a che un giudice nazionale respinga, quale mezzo di prova di una violazione della tutela dei dati personali, un elenco presentato dalla persona interessata e contenente dati personali di quest'ultima, qualora tale persona abbia ottenuto l'elenco senza il consenso, richiesto dalla legge, del responsabile del trattamento di tali dati.

La Corte ritiene innanzitutto ricevibile la questione, in quanto il rigetto da parte del giudice nazionale del mezzo di prova prodotto dal sig. Puškár, ottenuto senza il consenso del responsabile del procedimento, costituirebbe una restrizione del diritto a un ricorso giurisdizionale sancito dalla direttiva 95/46, nonché una restrizione del diritto a un ricorso effettivo ai sensi dell'art. 47 della Carta. Trattandosi di un limite a un diritto fondamentale, è necessario verificare se esso può quindi essere giustificato conformemente all'art. 52, par. 1, della Carta.

Secondo la Corte, spetta al giudice nazionale verificare se tale restrizione sia prevista dal diritto nazionale, e se incida sul contenuto essenziale del diritto fondamentale in questione. In quest'ultimo caso, il giudice nazionale dovrà verificare se l'esistenza dell'elenco e il fatto che esso contenga dati personali del sig. Puškár siano contestati nell'ambito del procedimento principale e se quest'ultimo

disponga di altri mezzi di prova in tal senso. Infine, il giudice nazionale deve valutare se il rigetto dell'elenco quale mezzo di prova sia necessario e risponda effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. A tale riguardo, la Corte ritiene che l'obiettivo di evitare l'impiego non autorizzato di documenti interni nell'ambito di un procedimento giurisdizionale può costituire un obiettivo di interesse generale legittimo. Inoltre, qualora un elenco debba rimanere riservato e contenga dati personali di altre persone fisiche, occorre tutelare i diritti di tali persone. Spetta tuttavia al giudice nazionale verificare se il diritto sancito dall'art. 47 della Carta non ne risulti eccessivamente pregiudicato. Secondo la Corte, infatti, quanto meno nel caso in cui la persona i cui dati personali figurano nell'elenco abbia diritto di accedere a tali dati, siffatto rigetto risulta eccessivo rispetto agli obiettivi menzionati. Infatti, al fine di valutare la proporzionalità del rigetto dell'elenco quale mezzo di prova, il giudice nazionale deve esaminare se la legislazione nazionale limiti o meno, rispetto ai dati contenuti in tale elenco, i diritti di accesso e informazione previsti dalla direttiva 95/46 e se una tale restrizione sia giustificata. Inoltre, anche ove tale restrizione sia prevista e sussistano elementi per riconoscere un interesse legittimo all'eventuale riservatezza dell'elenco, i giudici nazionali devono verificare se, nel singolo caso, questi prevalgano sull'interesse alla tutela dei diritti del singolo e se siano disponibili altri mezzi per garantire siffatta riservatezza, in particolare per quanto riguarda i dati personali di altre persone fisiche contenuti nell'elenco.

In definitiva, l'art. 47 della Carta deve essere interpretato nel senso che esso osta a che un giudice nazionale respinga, in quanto mezzo di prova di una violazione della tutela dei dati personali, un elenco presentato dalla persona interessata e contenente dati personali di quest'ultima, qualora tale persona si sia procurata l'elenco senza il consenso, richiesto per legge, del responsabile del trattamento dei dati, a meno che tale rigetto sia previsto dalla normativa nazionale e rispetti al tempo stesso il contenuto essenziale del diritto a un ricorso effettivo e il principio di proporzionalità.

In terzo luogo, la Corte valuta se gli artt. 7 e 8 della Carta ostino a un trattamento dei dati personali da parte delle autorità dello Stato membro ai fini della riscossione delle imposte e della lotta alla frode fiscale, come quello a cui si è preceduto con la redazione dell'elenco, senza il consenso delle persone interessate.

Secondo la Corte, la redazione dell'elenco può essere considerata un trattamento dei dati lecito, in quanto la riscossione delle imposte e la lotta alla frode fiscale sono compiti di interesse pubblico, ai sensi dell'art. 7 della direttiva 95/46. Il giudice nazionale dovrà tuttavia verificare se le autorità slovacche che hanno redatto tale elenco, o alle quali quest'ultimo è stato comunicato, siano state investite di tali compiti ai sensi della normativa nazionale e se in particolare, i compiti menzionati ricomprendano l'obiettivo del trattamento dei dati in questione.

Il giudice nazionale dovrà poi verificare se la redazione dell'elenco sia necessaria all'espletamento dei compiti di interesse pubblico, tenendo conto, in particolare, della finalità esatta della redazione dell'elenco, degli effetti giuridici a cui sono sottoposte le persone che vi sono iscritte e del carattere pubblico o meno di tale elenco. È quindi necessario, secondo la Corte, prestare particolare attenzione al rispetto del principio di proporzionalità, in quanto il fatto di essere iscritta nell'elenco può pregiudicare i diritti di una persona, può ledere la sua presunzione di innocenza sancita dall'art. 48 della Carta, nonché la libertà di impresa delle persone giuridiche collegate alle persone fisiche iscritte nell'elenco, ai sensi dell'art. 16 della Carta. Una tale ingerenza potrebbe, quindi, 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. Il giudice

nazionale dovrebbe poi ulteriormente verificare che le altre condizioni di liceità del trattamento dei dati personali imposte dalla direttiva 95/46 siano soddisfatte.

Infine, la Corte è chiamata a valutare se l'art. 47 della Carta debba essere interpretato nel senso che esso osta a che un giudice nazionale privilegi la giurisprudenza della Corte rispetto a quella della Corte EDU nel caso in cui vi sia una divergenza tra le due.

Nel caso di specie, infatti, il giudice del rinvio, a seguito della remissione della questione da parte della Corte costituzionale della Repubblica Slovacca, aveva ritenuto che quest'ultima avesse fatto riferimento alla giurisprudenza della Corte EDU, senza tenere in considerazione la giurisprudenza rilevante della Corte di giustizia relativa all'applicazione del diritto dell'Unione in materia di protezione dei dati personali.

La Corte di giustizia non risponde tuttavia alla questione, in quanto il giudice del rinvio non ha precisato in modo chiaro e concreto in cosa consistano le divergenze menzionate.

c. Esito a livello nazionale

Non disponibile.

5. Analisi

a. Il ruolo della Carta

Nella presente sentenza, la Corte di giustizia si sofferma innanzitutto sulla portata del diritto fondamentale a una tutela giurisdizionale effettiva, sancito dall'art. 47 della Carta, nell'ambito del trattamento dei dati personali. La Corte, dopo aver rilevato che la direttiva 95/46 non contiene alcuna disposizione che disciplini specificamente le condizioni alle quali un ricorso giurisdizionale può essere proposto, rileva che spetta agli Stati membri disciplinare le modalità procedurali volte ad assicurare la salvaguardia dei diritti conferiti da tale direttiva, nel rispetto dell'art. 47 della Carta (c.d. principio di autonomia procedurale).

Partendo da tale presupposto, la Corte valuta quindi il requisito procedurale, posto dalla normativa Slovacca - relativo al previo esperimento dei ricorsi amministrativi interni - in relazione all'art. 47 della Carta. In particolare, la Corte analizza tale requisito come una limitazione al diritto fondamentale a un ricorso effettivo e, quindi, in base ai requisiti previsti dall'art. 52, par. 1, della Carta:

> "*Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, 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*".

Allo stesso modo, la Corte valuta la possibilità di fornire, come mezzo di prova durante il procedimento giurisdizionale, un elenco da parte della persona interessata e contenente dati personali di quest'ultima, ottenuto senza il consenso, previsto dalla legge, del responsabile del trattamento. Anche in questo caso, la Corte ritiene che respingere un tale elenco come mezzo di prova costituisca una limitazione al diritto fondamentale sancito dall'art. 47 della Carta e che, come tale, debba essere giustificata sulla base dei requisiti previsti dall'art. 52, par. 1, della Carta.

Infine, la Corte di giustizia valuta se la redazione di un elenco come quello preso in esame sia conforme al diritto dell'Unione, in particolare agli artt. 7 e 8 della Carta. La Corte procede a un bilanciamento tra le esigenze derivanti dalla riscossione delle imposte e la lotta alla frode fiscale,

riconosciuti come compiti di interesse pubblico, e la tutela del diritto fondamentale al rispetto della vita privata. Restrizioni a tale diritto, secondo la Corte, devono intervenire entro i limiti dello stretto necessario. In particolare, una tale ingerenza potrebbe risultare proporzionata solo ove sussistano elementi sufficienti per presumere che le persone interessate figurino a ragione in un siffatto elenco. Inoltre, il giudice nazionale deve comunque verificare che le altre condizioni di liceità del trattamento dei dati personali previste dal diritto dell'Unione siano soddisfatte.

b. Dialogo giuridico

Interazione verticale tra il giudice nazionale, il *Najvyšší súd Slovenskej republiky* (Corte suprema della Repubblica Slovacca) e la Corte di giustizia attraverso il meccanismo del rinvio pregiudiziale.

c. Impatto della decisione della Corte di giustizia

La sentenza in esame rileva anche in relazione all'interpretazione del regolamento 679/2016, che ha abrogato e sostituito la direttiva 95/46/CE.

In particolare, l'art. 79 del regolamento 679/2016 prevede il diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento. Sebbene il regolamento dedichi maggiore attenzione all'aspetto della tutela giurisdizionale, esso non disciplina le condizioni procedurali attraverso le quali la persona interessata possa esercitare il proprio diritto. Esse dovranno quindi essere definite dagli Stati membri, nel rispetto dell'art. 47 della Carta, come interpretato dalla presente sentenza.

d. Altri casi rilevanti

Sulle limitazioni ai diritti fondamentali (artt. 7 e 8 della Carta) in ambito nazionale:

- Corte di giustizia, sentenza del 21 dicembre 2016, *Tele2 Sverige e Watson e* a., C-203/15 e C-698/15.

Scheda n. 6 – La corresponsabilità dell'amministratore di una pagina in un social network in caso di violazione delle norme relative al trattamento dei dati personali dei visitatori

- Corte di giustizia (Grande sezione), sentenza del 5 giugno 2018, *Wirtschaftsakademie Schleswig-Holstein*, causa C-210/16

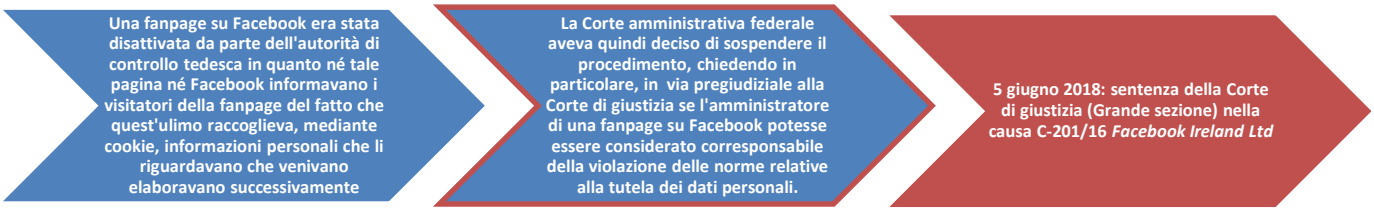
1. Aspetti centrali

L'amministratore di una pagina presente su un *social network* deve essere qualificato come "responsabile del trattamento" ai sensi della direttiva 95/46/CE qualora abbia contribuito, attraverso la propria azione di impostazione dei parametri del suo pubblico destinatario e degli obiettivi di gestione o promozione delle sue attività, alla determinazione delle finalità e degli strumenti del trattamento dei dati personali dei visitatori della pagina.
L'autorità di controllo di uno Stato membro può esercitare le sue funzioni anche rispetto a una filiale situata nello stesso Stato membro, anche se, in base alla ripartizione delle funzioni tra le varie filiali del gruppo societario, essa non è competente alla raccolta e al trattamento dei dati personali.
L'autorità di controllo è competente a esercitare le sue funzioni in piena indipendenza rispetto alle autorità situate negli altri Stati membri, senza previamente richiedere l'intervento dell'autorità di controllo di un altro Stato membro.

2. A colpo d'occhio

Paese	Area	Riferimenti al diritto UE	Attori	Tecniche di Interazione giuridica	Esito
• Germania	• Protezione dei dati personali	• Art. 8 CDFUE • Direttiva 95/46/CE [ora abrogata dal Regolamento 679/2016]	• Bundesverwaltungsgericht (Corte amministrativa federale, Germania) • Corte di giustizia	• Verticale: Domanda di pronuncia pregiudiziale ai sensi dell'art. 267 TFUE sull'interpre tazione della direttiva 95/46/CE	• La Corte riconosce la corresponsabilità dell'amministratore di una fanpage su Facebook in caso di violazione delle norme relative alla tutela dei dati personali. • L'autorità di controllo, in presenza di determinate condizioni, può esercitare le sue funzioni su una fliale situata nel suo Stato membro • Definizione di indipendenza dell'autorità di controllo

3. Cronologia



4. Descrizione

a. Fatti

La società tedesca Wirtschaftakademie, specializzata nel settore della formazione, aveva attivato una *fanpage* su Facebook, attraverso la quale diffondeva la propria offerta sul mercato. Attraverso una funzionalità messa a disposizione gratuitamente da Facebook secondo condizioni d'uso non modificabili, gli amministratori della *fanpage* potevano ottenere dati statistici anonimi riguardanti i visitatori di tali pagine. I dati erano raccolti attraverso *cookie* installati da Facebook sul computer o su qualsiasi altro dispositivo della persona che aveva visitato la *fanpage*, indipendentemente dal fatto che tale persona possedesse o meno un profilo su Facebook.

L'autorità tedesca di vigilanza per la protezione dei dati personali aveva ordinato alla Wirtschaftakademie la disattivazione della *fanpage*, prevedendo una penalità in caso di mancato adempimento, in quanto né la società tedesca né Facebook avevano informato i visitatori della *fanpage* del fatto che quest'ultimo raccoglieva, mediante *cookie*, informazioni personali che li riguardavano e che venivano successivamente elaborate. In particolare, l'autorità garante riconosceva la corresponsabilità della società tedesca che, avendo creato la *fanpage*, aveva fornito un contributo attivo e volontario alla raccolta, da parte di Facebook, di dati personali riguardanti i visitatori della pagina, dati di cui essa beneficiava tramite le statistiche messe a sua volta a disposizione dal *social network*.

Avverso tale decisione, la società tedesca aveva proposto ricorso, sostenendo di non poter essere ritenuta responsabile del trattamento dei dati realizzato da Facebook e negando di aver incaricato quest'ultimo di effettuare un trattamento dei dati soggetto al suo controllo o rientrante nella sua sfera di influenza, in quanto effettuato in base a condizioni d'uso non modificabili. Il tribunale annullava quindi la decisione dell'autorità garante, sostenendo che l'amministratore della pagina Facebook non potesse essere considerato come il responsabile del trattamento. In appello, la sentenza di primo grado veniva confermata, a motivo che solo Facebook avrebbe potuto essere considerato il responsabile del trattamento dei dati, mentre la Wirtschaftakademie avrebbe ricevuto solo informazioni statistiche rese anonime.

L'autorità garante proponeva quindi ricorso per cassazione dinanzi al *Bundesverwaltungsgericht* (Corte amministrativa federale), il quale decideva di sospendere il procedimento e di rinviare in via pregiudiziale la questione alla Corte di giustizia.

b. Ragionamento della Corte di giustizia

In primo luogo, la Corte di giustizia affronta la questione se l'amministratore di una *fanpage* presente su un *social network* possa essere considerato responsabile della violazione delle norme relative alla tutela dei dati personali, a motivo della scelta di essersi avvalso di tale *social network* per diffondere la propria offerta di informazioni.

La Corte innanzitutto sottolinea che la nozione di "responsabile di trattamento" deve essere intesa in modo ampio, al fine di garantire una tutela efficace e completa degli interessati. Inoltre, tale nozione non rinvia necessariamente a un unico organismo e può riguardare vari attori che partecipano a tale trattamento, ciascuno dei quali sarà quindi soggetto alle disposizioni applicabili in materia di protezione dei dati. Quindi, se da un lato *Facebook Inc*. e, per quanto riguarda l'Unione europea, *Facebok Ireland*, devono essere considerate senza dubbio "responsabili del trattamento" ai sensi della direttiva 95/46/CE, la questione riguarda se e in che misura l'amministratore di una pagina Facebook possa contribuire, insieme a *Facebook Inc*. e *Facebook Ireland*, a determinare le finalità e gli strumenti del trattamento dei dati personali dei visitatori della pagina e possa quindi essere considerato quale "responsabile del trattamento".

Secondo la Corte, qualsiasi persona che desideri aprire una pagina su Facebook stipula con *Facebook Ireland* un contratto specifico riguardante la sua apertura e aderisce, a tale titolo, alle relative condizioni di utilizzo, compresa la politica in materia di *cookie*. In particolare, il giudice dell'Unione specifica che se da un lato, il mero fatto di utilizzare Facebook non rende un utilizzatore corresponsabile del trattamento dei dati personali effettuato da tale network, dall'altro lato, l'amministratore di una pagina presente sul *social network*, mediante la creazione di tale pagina, permette a Facebook di posizionare *cookie* sul computer o su qualsiasi altro dispositivo di una persona che ha visitato la sua *fanpage*, a prescindere che essa abbia o meno un profilo Facebook. Inoltre, la creazione di una pagina su Facebook implica, da parte del suo amministratore, un'azione di impostazione dei parametri in base, segnatamente, al suo pubblico destinatario, nonché agli obiettivi di gestione o di promozione delle sue attività, che influisce sul trattamento di dati personali ai fini della creazione di statistiche stabilite a partire dalle visite sulla *fanpage.* Inoltre, tale amministratore può, tramite filtri messi a disposizione da Facebook, definire i criteri a partire dai quali si devono stabilire tali statistiche e designare perfino le categorie di persone i cui dati personali saranno oggetto di utilizzo da parte di Facebook.

Inoltre, il fatto che le statistiche elaborate da Facebook siano trasmesse all'amministratore della pagina in forma anonima, non toglie, secondo la Corte, che la realizzazione di tali statistiche si fondi sulla raccolta preliminare, mediante *cookie* installati da Facebook, e sul trattamento dei dati personali dei visitatori delle pagine a siffatti fini statistici. Inoltre, in base alla direttiva 95/46, non è un requisito per ritenere corresponsabile l'amministratore, che egli abbia accesso ai dati delle persone interessate.

In base a tali considerazioni, la Corte conclude, quindi, ritenendo che l'amministratore di una *fanpage* presente su Facebook partecipi, attraverso la propria azione d'impostazione dei parametri, in funzione 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 *fanpage*. Pertanto, tale amministratore deve essere qualificato, all'interno dell'Unione, come responsabile del trattamento dei dati personali, insieme a *Facebook Ireland*. Tuttavia, secondo la Corte, l'esistenza di una corresponsabilità non si deve tradurre necessariamente in una responsabilità equivalente dei diversi operatori nell'ambito di un trattamento di dati personali; al contrario, il grado di responsabilità di ciascuno di essi deve essere valutato tenendo conto delle circostanze rilevanti del caso di specie.

In secondo luogo, la Corte affronta la questione se l'autorità di controllo possa esercitare i suoi poteri nei confronti di una filiale situata nel territorio dello Stato membro cui essa appartiene, anche se, in base alle ripartizioni delle funzioni all'interno del gruppo societario, tale filiale non è competente per la raccolta e il trattamento dei dati personali, funzioni che gravano per intero su una filiale stabilita in un altro Stato membro.

Secondo la Corte, per determinare se un'autorità di controllo sia autorizzata ad esercitare i poteri che le sono conferiti dal diritto nazionale nei confronti di uno stabilimento situato sul territorio dello Stato membro cui essa appartiene, è necessario verificare se le due condizioni poste dalla direttiva 95/46 siano soddisfatte, ossia, da un lato, che si tratti di uno "stabilimento del responsabile del trattamento" e, dall'altro, che il trattamento in parola sia effettuato nel contesto delle attività di tale stabilimento. Per quanto riguarda il primo requisito, secondo cui il responsabile del trattamento deve disporre di uno stabilimento nel territorio dello Stato membro dell'autorità di controllo interessata, la Corte rileva che *Facebook Inc*. e *Facebook Ireland* dispongono di una filiale stabilita in Germania. Riguardo al secondo requisito, la Corte ritiene che l'espressione "nel contesto delle attività di uno stabilimento" non possa essere interpretato restrittivamente. La Corte rileva che la filiale stabilita in Germania è destinata a garantire, in tale Stato membro, la

promozione e la vendita di spazi pubblicitari che servono a rendere redditizi i servizi offerti da Facebook, il quale raccoglie i dati personali mediate *cookie* proprio al fine di migliorare il proprio sistema pubblicitario e individuare meglio le comunicazioni che esso diffonde. Pertanto, le attività di tale filiale devono essere ritenute inscindibilmente connesse al trattamento di dati personali di cui la *Facebook Inc*. è responsabile insieme alla *Facebook Ireland*. Di conseguenza, secondo la Corte, un siffatto trattamento deve essere considerato come effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento.

Infine, la Corte di giustizia è chiamata a valutare se, nel caso in cui un'autorità di controllo di uno Stato membro intenda esercitare i poteri d'intervento nei confronti di un organismo situato nel medesimo Stato membro a motivo di violazioni commesse da un terzo responsabile del trattamento di dati, stabilito nel territorio di un altro Stato membro, essa possa esercitarle in modo autonomo rispetto all'autorità di controllo dello Stato membro ove il responsabile del trattamento ha sede.

Secondo la Corte, le autorità di controllo sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite, come risulta dall'art. 8, par. 3, della Carta e dall'art. 16, par. 2, del TFUE. Inoltre, sebbene le autorità debbano coordinarsi tra loro nella misura necessaria all'esercizio delle loro funzioni, non vi è nessun criterio di priorità che disciplini l'intervento delle autorità di controllo le une rispetto alle altre e non sussiste l'obbligo, a carico delle autorità di uno Stato membro di conformarsi alla posizione espressa da un'autorità di un altro Stato membro.

Nel caso di specie, pertanto, l'autorità tedesca era competente a valutare in maniera autonoma la liceità del trattamento dei dati rispetto alle valutazioni eventualmente espresse dall'autorità di vigilanza dell'Irlanda, sede di *Facebook Ireland*.

c. Esito a livello nazionale

Non disponibile.

5. Analisi

e. Il ruolo della Carta

La questione sottoposta alla Corte di giustizia riguarda l'interpretazione della direttiva 95/46/CE, e la sua attuazione a livello nazionale. Pertanto, la Carta è applicabile al caso di specie, in base all'art. 51, par. 1, della Carta e la relativa giurisprudenza.

Tuttavia, il solo riferimento espresso alla Carta, in particolare al suo art. 8, relativo alla protezione dei dati, è rinvenibile in relazione al carattere indipendente dell'autorità di controllo incaricata di sorvegliare l'applicazione delle disposizioni adottate da uno Stato membro in attuazione della direttiva 1995/46/CE (ora abrogata dal Regolamento 2016/679/UE). Secondo la Corte, tale indipendenza deve essere interpretata nel senso che ogni autorità è tenuta a verificare che siano rispettati gli obblighi discendenti dal diritto dell'Unione nel territorio dello Stato membro cui essa appartiene, senza che vi sia nessun criterio di priorità nell'intervento delle autorità di controllo appartenenti a Stati membri diversi e senza che un'autorità debba conformarsi o far propria la soluzione adottata dall'autorità di un altro Stato membro.

f. Dialogo giuridico

Interazione verticale tra il giudice nazionale, il *Bundesverwaltungsgericht* (Corte amministrativa federale della Germania) e la Corte di giustizia attraverso il meccanismo del rinvio pregiudiziale.

g. Impatto della decisione della Corte di giustizia

Con l'entrata in vigore del regolamento 2016/679/UE (c.d. GDPR), la sentenza in oggetto, in particolare nella parte in cui individua come responsabile del trattamento dei dati personali anche l'amministratore di una *fanpage* presente su un *social network*, può ingenerare dubbi circa la terminologia utilizzata.

Infatti il regolamento GDPR ha distinto la nozione di "titolare del trattamento" e di "responsabile del trattamento", definendo il primo 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 di dati personali" (art. 4, par. 7). È invece definito "responsabile del trattamento": "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" (art. 4, par. 8). Nel caso di specie, l'amministratore della pagina Facebook dovrebbe quindi essere definito "titolare del trattamento" ai sensi del suddetto regolamento.

Ciò che rimane incerto è se quest'ultimo possa essere considerato come "contitolare del trattamento" insieme a Facebook ai sensi dell'art. 26 del regolamento, in base al quale "[a]llorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento". Questo comporta che, ai sensi dell'art. 82, par. 4, "qualora più titolari del trattamento (…) siano coinvolti nello stesso trattamento e siano (…) responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato". Tuttavia, nella sentenza la Corte ha riconosciuto che: "l'esistenza di una corresponsabilità non si traduce necessariamente in una responsabilità equivalente dei diversi operatori nell'ambito di un trattamento di dati personali. Al contrario, tali operatori possono essere coinvolti in fasi diverse di tale trattamento e a diversi livelli, di modo che il grado di responsabilità di ciascuno di essi deve essere valutato tenendo conto di tutte le circostanze rilevanti del caso di specie" (par. 43).

h. Altri casi rilevanti

Sull'indipendenza delle autorità nazionali di controllo:

- Corte di giustizia (Grande sezione), sentenza dell'8 aprile 2014, *Commissione c. Ungheria*, causa C-288712;
- Corte di giustizia (Grande sezione), sentenza del 9 marzo 2010, *Commissione c. Germania*, causa C-518/07;
- Corte di giustizia (Grande sezione), sentenza del 16 ottobre 2012, *Commissione c. Austria*, causa C-614/10.

Scheda n. 7 – Il bilanciamento tra libertà religiosa e protezione dei dati

- Corte di giustizia (Grande sezione), sentenza del 10 luglio 2018, *Tietosuojavaltuutettu*, causa C-25/17

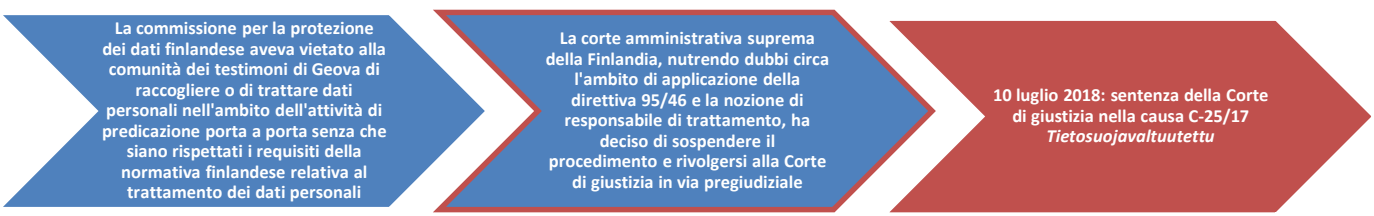
1. Aspetti centrali

La raccolta di dati personali da parte dei membri di una comunità religiosa nell'ambito di un'attività di predicazione porta a porta e i trattamenti successivi di tali dati rientrano nella sfera di applicazione della direttiva 95/46. Tali attività non possono essere equiparate ad attività proprie delle autorità statali; inoltre, non si tratta di attività a carattere esclusivamente personale o domestico, in quanto l'attività di predicazione va oltre la sfera privata di un membro predicatore di una comunità religiosa.
La nozione di "archivio" ai sensi della direttiva 95/46 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 siano 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.
Una comunità religiosa è responsabile, congiuntamente ai suoi membri predicatori, 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 essa abbia accesso a tali dati o che debba dimostrare di aver fornito ai propri membri istruzioni scritte o incarichi relativamente a tali trattamenti.

2. A colpo d'occhio

Paese	Area	Riferimenti al diritto UE	Attori	Tecniche di Interazione giuridica	Esito
• Finlandia	• Protezione dei dati personali	• Art. 10 CDFUE • Direttiva 95/46/CE [ora abrogata dal Regolamento 2016/679]	• Korkein hallinto-oikeus (Corte amministrativa suprema, Finlandia) • Corte di giustizia	• Verticale: Domanda di pronuncia pregiudiziale ai sensi dell'art. 267 TFUE sull'interpre tazione della direttiva 95/46/CE, letta alla luce dell'art. 10 della Carta	• La direttiva si applica anche nel caso di attività di membri predicatori di una comunità religiosa • la nozione di archivio comprende anche i dati raccolti porta a porta • la comunità religiosa può essere ritenuta coresponsabile del trattamento dei dati personali, insieme ai membri predicatori incaricati di raccogliere i dati

3. Cronologia



4. Descrizione

d. Fatti

La commissione per la protezione dei dati finlandese 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 soddisfatti i requisiti legali per il trattamento dei dati personali. La comunità aveva quindi presentato ricorso avanti al tribunale amministrativo, che annullava la decisione della commissione a motivo che la comunità dei testimoni di Geova non era responsabile del trattamento di dati personali e che l'attività di quest'ultima non costituiva un trattamento illecito di tali dati.

La commissione aveva quindi impugnato la sentenza davanti alla Corte amministrativa suprema della Finlandia. Secondo quanto constatato da tale giudice, i membri della comunità dei testimoni di Geova, nell'ambito della loro attività di predicazione porta a porta, prendevano appunti sulle visite effettuate a persone che essi stessi o detta comunità non conoscevano. I dati raccolti potevano, tra l'altro, comprendere il nome e l'indirizzo delle persone contattate porta a porta e informazioni sul loro credo religioso e sulla loro situazione familiare. Tali dati venivano raccolti a titolo di promemoria, per poter essere consultati per un'eventuale visita successiva, senza che le persone interessate vi avessero acconsentito o ne fossero state informate. Inoltre, secondo il giudice del rinvio, la comunità dei testimoni di Geova aveva fornito ai suoi membri istruzioni in ordine alla redazione di tali appunti. Infatti, tale comunità e le relative congregazioni organizzavano e coordinavano l'attività di predicazione porta a porta dei loro membri e, in particolare, gestivano un elenco di persone che avevano espresso la volontà di non ricevere più visite da parte dei predicatori, consultabile dai membri stessi della comunità.

La Corte suprema aveva quindi deciso di sospendere il procedimento e di adire la Corte di giustizia in via pregiudiziale, al fine di appurare se l'attività di predicazione porta a porta praticata dai membri di una comunità religiosa ricadesse nell'ambito di applicazione della direttiva 95/46 e, nel caso, se l'insieme dei dati raccolti e trattati in maniera non automatizzata, potessero essere considerati un archivio ai sensi di tale normativa. In caso affermativo, il giudice del rinvio poneva, quindi, la questione se la comunità dei testimoni di Geova potesse essere considerata responsabile di tale trattamento.

e. Ragionamento della Corte di giustizia

Innanzitutto, la Corte affronta la questione se la raccolta dei dati personali da parte dei membri di una comunità religiosa nell'ambito di un'attività di predicazione porta a porta e i trattamenti successivi dei dati possano rientrare in una delle ipotesi di esclusione di applicazione della direttiva 95/46.

In primo luogo, il giudice dell'Unione verifica la prima eccezione all'ambito di applicazione della direttiva, ovvero se le attività in questione possano essere considerate attività proprie dello Stato o delle autorità statali, estranee alle attività dei singoli. Secondo la Corte, la raccolta di dati personali da parte dei membri della comunità dei testimoni di Geova, nell'ambito di un'attività di predicazione porta a porta, rientra esclusivamente nell'ambito di un'iniziativa religiosa di singoli. Ne consegue che una tale attività non costituisce un'attività propria delle autorità statali e che, pertanto, non può essere equiparata a quelle escluse dall'ambito di applicazione della direttiva 95/46.

In secondo luogo, la direttiva esclude dal suo ambito di applicazione il trattamento dei dati effettuato per l'esercizio di attività "esclusivamente" personali o domestiche e, in base alla giurisprudenza della Corte, esse devono essere intese come riguardanti unicamente le attività che rientrano nell'ambito della vita privata o familiare dei singoli. A tale riguardo, un'attività non può essere considerata a carattere esclusivamente personale o domestico, ai sensi di tale disposizione, se il suo scopo è quello di rendere i dati personali accessibili a un numero indefinito di persone, ovvero se tale attività 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. Nel caso di specie, l'attività di predicazione porta a porta, nel cui ambito i membri della comunità dei testimoni di Geova raccolgono dati personali, ha, per sua stessa natura, la finalità di diffondere il credo della comunità dei testimoni di Geova presso persone che non appartengono al nucleo familiare dei membri predicatori. Tale attività è diretta quindi verso l'esterno della sfera privata dei membri predicatori. Inoltre, alcuni dei dati raccolti dai membri predicatori sono trasmessi alle congregazioni di tale comunità, le quali conservano elenchi, compilati in base a questi dati, di persone che non desiderano più ricevere visite. Nell'ambito della loro attività di predicazione, questi ultimi pertanto rendono, quanto meno alcuni dei dati rilevati, accessibili a un numero potenzialmente illimitato di persone.

Inoltre, il fatto che il trattamento dei dati personali avvenga nell'ambito di un'attività relativa a una pratica religiosa non conferisce di per sé un carattere esclusivamente personale o domestico all'attività di predicazione porta a porta. Infatti, l'art. 10, par. 1, della Carta implica la libertà di ciascuno di manifestare la propria religione o la propria convinzione, individualmente o collettivamente, in pubblico o in privato, mediante il culto, l'insegnamento, le pratiche e l'osservanza dei riti. La nozione di religione contenuta in tale disposizione può comprendere sia il *forum internum*, ossia il fatto di avere convinzioni, sia il *forum externum*, ossia la manifestazione pubblica di una fede religiosa. Inoltre, la libertà di manifestare la propria religione individualmente o collettivamente, in pubblico o in privato, include anche il diritto di cercare di convincere altre persone, ad esempio attraverso una predicazione. Nel caso di specie, sebbene l'attività di predicazione porta a porta dei membri di una comunità religiosa sia tutelata dall'art. 10, par. 1, della Carta, in quanto espressione della fede dei predicatori, tale circostanza non ha l'effetto di conferire alla suddetta attività un carattere esclusivamente personale o domestico, in quanto l'attività di predicazione va oltre la sfera privata di un membro predicatore di una comunità religiosa.

La Corte si sofferma poi sulla nozione di "archivio" ai sensi della direttiva 95/46. Infatti, se i dati sono trattati in modo non automatizzato, la direttiva si applica solo se i dati trattati sono contenuti o destinati a figurare in un archivio. Ai sensi della direttiva, la nozione di "archivio" comprende "qualsiasi insieme strutturato di dati personali accessibili, secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico" (art. 2 della direttiva 95/46). In particolare, il requisito secondo cui l'insieme dei dati personali deve avere un carattere strutturato secondo criteri specifici, secondo la Corte, mira unicamente a consentire che i dati relativi a una persona possano essere individuati facilmente. A parte tale requisito, la direttiva non prescrive né le modalità secondo le quali un archivio deve essere strutturato né la forma che esso deve presentare. Nel caso di specie, nell'ambito dell'attività di predicazione, i dati venivano raccolti a titolo di promemoria per agevolare l'organizzazione di visite successive a persone già contattate porta a porta. Essi comprendevano non solo informazioni sul contenuto delle conversazioni riguardanti le convinzioni personali della persona visitata, ma anche il nome e l'indirizzo. Inoltre, tali informazioni, almeno alcune di esse, erano utilizzate per elaborare elenchi gestiti dalle congregazioni della comunità dei testimoni di Geova, riguardanti le persone che non desideravano più ricevere visite da parte di predicatori membri di tale comunità. Pertanto, secondo la Corte, 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.

Infine, la Corte è chiamata a pronunciarsi sulla circostanza se una comunità religiosa come quella dei testimoni di Geova possa essere considerata, congiuntamente con i suoi membri predicatori, responsabile dei trattamenti di dati personali effettuati da questi ultimi nell'ambito di un'attività di predicazione porta a porta organizzata, coordinata e sostenuta da tale comunità, e se, a tal fine, sia necessario che detta comunità abbia accesso a tali dati o si dimostri che essa ha fornito ai propri membri istruzioni scritte o incarichi relativamente a tali trattamenti.

A tale proposito, la Corte afferma che la nozione di "responsabile del trattamento" deve essere interpretata in maniera ampia, al fine di garantire una tutela efficace e completa delle persone interessate. Se più soggetti partecipano al trattamento, ciascuno di essi deve essere assoggettato alle disposizioni applicabili in materia di protezione di dati personali; questo tuttavia non vuol dire che una responsabilità congiunta implichi necessariamente una responsabilità equivalente dei diversi soggetti che partecipano al trattamento dei dati personali. Secondo la Corte, può essere considerata responsabile del trattamento una persona fisica o giuridica che, a scopi che le sono propri, influisca sul trattamento dei dati personali e partecipi, pertanto, alla determinazione delle finalità e dei mezzi di tale trattamento, senza che tale determinazione debba essere effettuata necessariamente mediante istruzioni scritte o incarichi da parte del responsabile. Inoltre, una responsabilità congiunta non presuppone che ciascuno di essi abbia accesso ai dati personali trattati.

Nel caso di specie, la Corte rileva che la raccolta dei dati personali avviene nell'ambito dell'esercizio dell'attività di predicazione porta a porta, con la quale i membri predicatori della comunità dei testimoni di Geova diffondono il credo della loro comunità. Tale attività di predicazione costituisce una forma di azione essenziale di tale comunità, azione che è organizzata, coordinata e sostenuta dalla comunità stessa. Pertanto, la raccolta di dati personali relativi alle persone contattate porta a porta e il loro trattamento ulteriore sono strumentali al perseguimento dell'obiettivo della comunità dei testimoni di Geova, consistente nel diffondere il credo di quest'ultima e sono perciò effettuati dai suoi membri predicatori a fini propri di detta comunità. Inoltre, non solo la comunità dei testimoni di Geova ha, in generale, conoscenza del fatto che tali trattamenti hanno luogo ai fini della diffusione del proprio credo, ma essa organizza e coordina l'attività di predicazione dei suoi membri, in particolare ripartendo i settori di attività dei diversi predicatori.

Secondo la Corte, tali circostanze consentono di ritenere che la comunità dei testimoni di Geova, organizzando, coordinando e promuovendo l'attività di predicazione dei suoi membri volta alla diffusione del suo credo, partecipa, insieme ai suoi membri predicatori, a determinare le finalità e mezzi dei trattamenti di dati personali delle persone che sono contattate porta a porta. Tale constatazione, peraltro, non può essere rimessa in discussione dal principio dell'autonomia organizzativa delle comunità religiose, derivante dall'art. 17 TFUE. Infatti, l'obbligo di ogni persona di conformarsi alle norme del diritto dell'Unione relative alla protezione dei dati personali non può essere ritenuta un'ingerenza nell'autonomia organizzativa di dette comunità.

f. Esito a livello nazionale

Non disponibile.

5. Analisi

a. Il ruolo della Carta

Nella sentenza oggetto della presente scheda, la Corte è stata chiamata a pronunciarsi su alcuni aspetti della direttiva 95/46 alla luce dell'art. 10 della Carta, relativo alla libertà di religione.

In primo luogo, la Corte ha ritenuto che l'attività di predicazione porta a porta dei membri della comunità dei testimoni di Geova nell'ambito della quale viene effettuato un trattamento dei dati personali, pur essendo tutelata dall'art. 10, par. 1, della Carta in quanto espressione della fede dei predicatori, non esclude l'applicazione delle garanzie previste dalla direttiva 95/46. Essa infatti non può essere considerata un'attività a carattere prevalentemente personale o domestico, in quanto l'attività di predicazione va oltre la sfera privata del membro predicatore della comunità religiosa.

Inoltre, la Corte fornisce una interpretazione ampia della nozione di "archivio" - che include l'insieme di dati personali raccolti nell'ambito di un'attività di predicazione porta a porta, allorché tali dati sono strutturati secondo criteri specifici che consentono, in pratica, di recuperarli facilmente per un successivo impiego – e di responsabile del trattamento. In particolare, la Corte ritiene che una comunità religiosa possa essere considerata responsabile del trattamento congiuntamente ai suoi predicatori, senza che l'autonomia organizzativa delle comunità religiose, tutelata dall'art. 17 TFUE, possa rimettere in discussione l'applicazione della normativa dell'Unione in materia di dati personali. In definitiva, la Corte, operando un bilanciamento tra l'autonomia organizzativa delle comunità religiose e la tutela dei dati personali, ritiene prevalente quest'ultima esigenza in quanto, solo mediante un'ampia definizione della nozione di responsabile, può essere garantita una tutela efficace e completa delle persone interessate (par. 66).

b. Dialogo giuridico

Interazione verticale tra il giudice nazionale, il Najvyšší Korkein hallinto-oikeus (Corte amministrativa suprema, Finlandia) e la Corte di giustizia attraverso il meccanismo del rinvio pregiudiziale.

c. Impatto della decisione della Corte di giustizia

La Corte riprende la sua precedente giurisprudenza, in particolare la sentenza *Wirtschaftakademie* di pochi mesi precedente, per chiarire che una comunità religiosa, congiuntamente ai suoi predicatori, può essere considerata responsabile del trattamento dei 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.

Con l'entrata in vigore del regolamento 679/16, deve essere operata una distinzione tra il "titolare del trattamento" e il "responsabile del trattamento". Infatti, in base alle definizioni fornite dall'art. 2 del regolamento, il primo è "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 di dati personal(...)"; mentre il secondo è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

Nella presente sentenza, la comunità religiosa e i membri predicatori devono essere considerati entrambi titolari del trattamento in quanto entrambi partecipano alla determinazione delle finalità e dei mezzi di tale trattamento.

A questo proposito, la Corte rileva che la responsabilità che ne discende non deve tuttavia necessariamente essere considerata equivalente tra i due titolari: al contrario, i soggetti possono essere coinvolti in fasi diverse del trattamento e a diversi livelli, di modo che il grado di responsabilità di ciascuno di essi deve essere valutato tenuto conto di tutte le circostanze rilevanti del caso di specie (par. 66).

d. Altri casi rilevanti

Sulle eccezioni all'ambito di applicazione della direttiva:

- Corte di giustizia, sentenza del 27 settembre 2017, *Puškár*, causa C-73/16

Sulla nozione di coresponsabile del trattamento:

- Corte di giustizia (Grande sezione), sentenza del 5 giugno 208, *Wirtschaftakademie*, causa C-210/16

Sull'autonomia organizzativa delle comunità religiose:

- Corte di giustizia (Grande sezione), sentenza del 17 aprile 2018, *Egenberger*, causa C-414/16

Scheda n. 8 – Il bilanciamento tra la necessità di sicurezza pubblica e la tutela della vita privata nei servizi di comunicazione elettronica

- Corte di giustizia (Grande sezione), sentenza del 2 ottobre 2018, *Ministerio Fiscal*, causa C-207/16

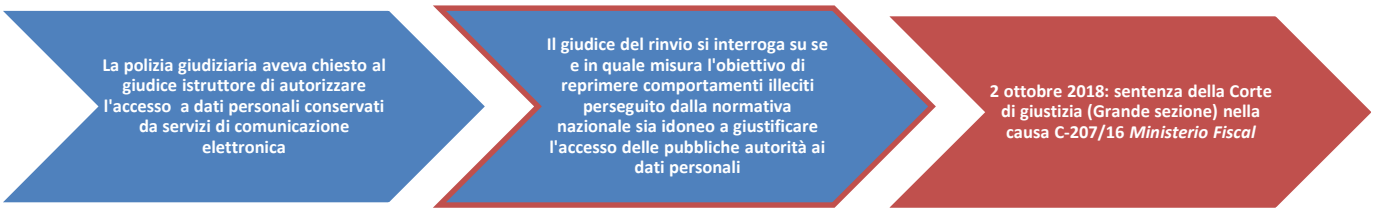
1. Aspetti centrali

Rientra nell'ambito di applicazione della direttiva 2002/58 non solo una misura legislativa che impone ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi al traffico e i dati relativi all'ubicazione, ma anche una misura legislativa riguardante l'accesso delle autorità nazionali ai dati conservati da questi fornitori.
L'accesso delle autorità pubbliche ai dati che mirano all'identificazione dei titolari di carte SIM attivate con un telefono cellulare rubato, come il cognome, il nome e, se del caso, l'indirizzo di tali titolari, comporta un'ingerenza nei diritti fondamentali di questi ultimi, sanciti dagli artt. 7 e 8 della Carta, che 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.

2. A colpo d'occhio

Paese	Area	Riferimenti al diritto UE	Attori	Tecniche di Interazione giuridica	Esito
• Spagna	• Protezione dei dati personali • Servizi di comunicazione elettronica	• Artt. 7, 8 CDFUE • Direttiva 2002/58/CE	• Audiencia Provincial de Terragona (Spagna) • Corte di giustizia	• Verticale: Domanda di pronuncia pregiudiziale ai sensi dell'art. 267 TFUE sull'interpretazione della direttiva 2002/58/CE letta alla luce degli articoli 7, 8 della Carta	• La Corte ritiene che l'accesso ai dati da parte delle autorità pubbliche comporta un'ingerenza nei diritti fondamentali che non presenta una gravità tale da dover essere limitata alla lotta contro la criminalità grave.

3. Cronologia



4. Descrizione

a. Fatti

A seguito di una rapina, ove erano stati rubati portafoglio e cellulare, e al fine di individuarne gli autori, la polizia giudiziaria chiedeva al giudice istruttore di ordinare ai fornitori di servizi di comunicazione elettronica la trasmissione dei numeri di telefono con il codice relativo

all'identificatore internazionale apparecchiature mobili (codice IMEI) del telefono cellulare rubato e i dati personali relativi all'identità civile dei titolari o utenti dei numeri di telefono corrispondenti alle carte SIM attivate con detto codice, quali il loro cognome, nome e, se del caso, indirizzo.

Il giudice istruttore respingeva tali domande, in quanto, da una parte, la misura richiesta non era utile per identificare gli autori del reato e, dall'altro lato, la legge spagnola applicabile limitava tale accesso solo a reati di una particolare gravità.

Il pubblico ministero appellava tale ordinanza dinanzi all'*Audiencia provincial di Terragona*, giudice del rinvio, il quale, ritenendo che l'interesse dello Stato a reprimere i comportamenti penalmente illeciti non potesse giustificare ingerenze sproporzionate nei diritti fondamentali previsti alla Carta, sospendeva il procedimento e adiva la Corte di giustizia in via pregiudiziale.

b. Ragionamento della Corte di giustizia

In via preliminare, la Corte verifica la sua competenza a pronunciarsi sulla questione, in quanto quest'ultima riguarderebbe un'attività dello Stato in materia di diritto penale e non rientrerebbe nell'ambito di applicazione del diritto dell'Unione e, quindi, della Carta, ai sensi del suo art. 51. La direttiva 2002/58 esclude infatti dal proprio ambito di applicazione le "attività dello Stato" , tra i quali figurano le attività dello Stato in settori del diritto penale e quelle riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato, compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza.

La Corte, richiamando la sua precedente sentenza *Tele2 Sverige*, ribadisce che rientra nell'ambito di applicazione di tale direttiva non solo una misura legislativa che impone ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi al traffico e i dati relativi all'ubicazione, ma anche una misura legislativa riguardante l'accesso delle autorità nazionali ai dati conservati da questi fornitori. Infatti, la tutela della riservatezza delle comunicazioni elettroniche e dei dati relativi al traffico afferenti alle stesse si applica alle misure adottate da tutti i soggetti diversi dagli utenti, indipendentemente dal fatto che si tratti di persone o di enti privati oppure di enti statali. Inoltre, misure legislative nazionali che impongano ai fornitori di servizi di comunicazione elettronica di conservare i dati personali, o di accordare alle autorità nazionali competenti l'accesso a tali dati, implicano necessariamente un trattamento, da parte dei fornitori suddetti, di questi dati. Quindi, tali misure, nei limiti in cui disciplinano le attività dei fornitori, non possono essere considerate come attività proprie degli Stati.

Nel caso di specie, la normativa nazionale in questione permetteva alla polizia giudiziaria, in caso di concessione dell'autorizzazione giudiziaria, di imporre ai fornitori di servizi di comunicazione elettronica di rendere disponibili dati personali e permetteva, in tal modo, che essi procedessero a un trattamento di tali dati. Secondo la Corte, la normativa nazionale in questione disciplina le attività dei fornitori di servizi di comunicazione elettronica e rientra, di conseguenza, nell'ambito di applicazione della direttiva 2002/58.

La Corte esamina quindi, nel merito, la domanda del giudice spagnolo che verte, sostanzialmente, sulla questione se, e in quale misura, l'obiettivo perseguito dalla normativa nazionale sia idoneo a giustificare l'accesso delle pubbliche autorità, come la polizia giudiziaria, a dati personali. In particolare, tale giudice si interroga sugli elementi da prendere in considerazione al fine di determinare se i reati con riferimento ai quali le autorità di polizia possono essere autorizzate, a fini di indagine, ad accedere a dati personali conservati dai fornitori di servizi di comunicazioni elettroniche, siano tanto gravi da giustificare l'ingerenza che un tale accesso comporta nei diritti fondamentali garantiti dagli artt. 7 e 8 della Carta, come interpretati dalla Corte nelle sue sentenze dell'8 aprile 2014, *Digital Rights Ireland e a*. e *Tele2 Sverige e Watson e a*.

La Corte rileva innanzitutto che l'accesso delle autorità pubbliche a tali dati costituisce un'ingerenza nel diritto fondamentale al rispetto della vita privata sancito dall'art. 7 della Carta e nel diritto alla protezione dei dati personali garantito dall'art. 8 della Carta, poiché costituisce un trattamento di dati personali.

Per quanto riguarda gli obiettivi idonei a giustificare la normativa nazionale che disciplina l'accesso delle autorità pubbliche ai dati conservati dai fornitori di servizi di comunicazioni elettroniche e che derogano, pertanto, al principio della riservatezza delle comunicazioni elettroniche, la Corte rileva che tale accesso deve rispondere in modo effettivo e rigoroso a uno degli obiettivi elencati in maniera tassativa dalla direttiva 2002/58, tra cui compare anche l'obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati. Tale obiettivo, peraltro, non implica una lotta contro i soli reati gravi, ma si riferisce ai reati in generale.

La Corte inoltre precisa che, in conformità al principio di proporzionalità, una grave ingerenza può essere giustificata, in materia di prevenzione, ricerca, accertamento e perseguimento di un reato, solo da un obiettivo di lotta contro la criminalità che deve essere qualificata come "grave". Al contrario, qualora l'ingerenza che comporta tale accesso non sia grave, detto accesso può essere giustificato da un obiettivo di prevenzione, ricerca, accertamento e perseguimento di un reato in generale.

Pertanto, la Corte si interroga se, nel caso di specie, l'ingerenza nei diritti fondamentali sanciti agli artt. 7 e 8 della Carta, che un accesso della polizia giudiziaria ai dati di cui trattasi nel procedimento principale comporterebbe, debba essere considerata come "grave". Secondo la Corte, tale accesso ha il solo scopo di identificare i titolari delle carte SIM attivate, per un periodo di dodici giorni, con il codice IMEI del cellulare rubato. Senza una verifica incrociata dei dati relativi alle comunicazioni effettuate con tali schede SIM e dei dati relativi all'ubicazione, questi dati non permettono di conoscere né la data, né l'ora, né la durata, né i destinatari delle comunicazioni effettuate con la, o le, carte SIM in questione, né i luoghi in cui dette comunicazioni sono avvenute o la frequenza di esse con talune persone nel corso di un determinato periodo. Pertanto, i dati a cui l'autorità giudiziaria chiede di avere accesso non permettono di trarre conclusioni precise sulla vita privata delle persone i cui dati sono oggetto di attenzione.

In tali circostanze, l'accesso solo a tali dati non può essere qualificato come un'ingerenza "grave" nei diritti fondamentali delle persone i cui dati sono oggetto di attenzione. L'ingerenza che un accesso a tali dati comporta può quindi essere giustificata dall'obiettivo di prevenzione, ricerca, accertamento e perseguimento di "reati" in generale, senza che sia necessario che tali reati siano qualificati come "gravi".

In definitiva, quindi, l'accesso delle autorità pubbliche ai dati che mirano all'identificazione dei titolari di carte SIM attivate con un telefono cellulare rubato, come il cognome, il nome e, se del caso, l'indirizzo di tali titolari, comporta un'ingerenza nei diritti fondamentali di questi ultimi, sanciti dagli artt. 7 e 8 della Carta dei diritti fondamentali, che 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.

c. Esito a livello nazionale

Non disponibile.

5. Analisi

e. Il ruolo della Carta

Nella presente sentenza, la Corte è chiamata a valutare se un'ingerenza nei diritti fondamentali di cui agli artt. 7 e 8 possa essere giustificata alla luce dell'obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati da parte delle autorità pubbliche.

In particolare, richiamando numerosi passaggi delle sentenze *Digital Rights Ireland* e *Tele2 Swerige*, la Corte parte dalla premessa che l'accesso delle autorità pubbliche a dati personali, come nel caso di specie, costituisce un'ingerenza nei diritti fondamentali di cui agli artt. 7 e 8 della Carta e, pertanto, deve essere giustificata. Tuttavia, la Corte si sofferma solo su due aspetti relativi, rispettivamente, all'obiettivo legittimo perseguito dalla normativa in questione e al rispetto del principio di proporzionalità.

In relazione a quest'ultimo aspetto, la Corte precisa, avuto riguardo in particolare alla sua precedente sentenza *Tele2 Swerige*, che qualora l'ingerenza sia qualificata come grave, essa può essere giustificata in materia di prevenzione, ricerca, accertamento e perseguimento di un reato, solo da un obiettivo di lotta contro la criminalità che deve essere qualificata come "grave". Al contrario, qualora l'ingerenza che comporta tale accesso ai diritti fondamentali non sia grave, detto accesso può essere giustificato da un obiettivo di prevenzione, ricerca, accertamento e perseguimento di un reato in generale.

Nel caso di specie, i dati oggetto del trattamento non permettevano di trarre conclusioni precise sulla vita privata delle persone i cui dati erano oggetto di attenzione. Pertanto, l'ingerenza non era stata qualificata dalla Corte come grave.

Secondo la Corte "l'accesso delle autorità pubbliche ai dati che mirano all'identificazione dei titolari di carte SIM attivate con un telefono cellulare rubato, come il cognome, il nome e, se del caso, l'indirizzo di tali titolari, comporta un'ingerenza nei diritti fondamentali di questi ultimi, sanciti dai suddetti articoli della Carta dei diritti fondamentali, che 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" (par. 63).

f. Dialogo giuridico

Interazione verticale tra il giudice nazionale, l'*Audiencia Provincial de Terragona* (Corte provinciale di Terragona, Spagna) e la Corte di giustizia attraverso il meccanismo del rinvio pregiudiziale.

g. Impatto della decisione della Corte di giustizia

La sentenza *Ministerio Fiscal* aggiunge un ulteriore elemento a quanto già statuito dalla Corte nelle sentenze *Digital Rights Ireland* e *Tele2 Swerige*.

Essa infatti si sofferma sull'esame della proporzionalità dell'ingerenza nei diritti fondamentali di cui agli artt. 7 e 8 della Carta, rispetto all'obiettivo perseguito. Nella sentenza *Tele2 Swerige* la Corte aveva affermato che, in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, soltanto la lotta contro la criminalità grave era idonea a giustificare un accesso delle autorità pubbliche a dati personali conservati dai fornitori di servizi di comunicazione che, considerati nel loro insieme, consentivano di trarre conclusioni precise sulla vita privata delle persone i cui dati erano oggetto di attenzione. Nella presente sentenza, la Corte precisa tuttavia che "in conformità al principio di proporzionalità, una grave ingerenza può essere giustificata, in materia di prevenzione, ricerca, accertamento e perseguimento di un reato, solo da un obiettivo di lotta contro la criminalità che deve essere qualificata come «grave». Al contrario, qualora l'ingerenza che comporta tale accesso non sia grave, detto accesso può essere giustificato da un obiettivo di prevenzione, ricerca, accertamento e perseguimento di un «reato» in generale" (par. 56 e 57).

Tuttavia, la Corte non chiarisce cosa debba intendersi, nel diritto dell'Unione, con reato grave, lasciando tale qualificazione alla normativa nazionale

h. Altri casi rilevanti

Sulle limitazioni ai diritti fondamentali (artt. 7 e 8 della Carta):

- Corte di giustizia (Grande sezione), sentenza dell'8 aprile 2014, *Digital Rights Ireland*, cause riunite C-293/12 e C-594/12;
- Corte di giustizia, sentenza del 21 dicembre 2016, *Tele2 Sverige e Watson e* a., C-203/15 e C-698/15.

Scheda n. 9 – Il rapporto tra libertà di espressione e protezione dei dati

- Corte di giustizia, sentenza del 14 febbraio 2019, *Buivids*, causa C-345/17

1. Aspetti centrali

La registrazione video di taluni agenti di polizia all'interno di un commissariato, durante la raccolta di una deposizione, e la pubblicazione del video così registrato su un sito Internet dove gli utenti possono inviare, visionare e condividere contenuti video, rientra nell'ambito di applicazione della direttiva 95/46/CE. Tale registrazione video e pubblicazione su un sito Internet possono costituire un trattamento di dati personali esclusivamente a scopi giornalistici, sempre che dal video risulti che detta registrazione e detta pubblicazione abbiano quale unica finalità la divulgazione al pubblico di informazioni, opinioni e idee.
Qualora emerga che la registrazione e pubblicazione abbiano come unica finalità la divulgazione al pubblico di informazioni, opinioni o idee, il giudice nazionale dovrà verificare se le esenzioni e le deroghe previste dalla direttiva 95/46 risultino necessarie per conciliare il diritto alla vita privata con le norme che disciplinano la libertà di espressione, e se tali esenzioni e deroghe operino nei limiti dello stretto indispensabile.

2. A colpo d'occhio

Paese	Area	Riferimenti al diritto UE	Attori	Tecniche di Interazione giuridica	Esito
• Lettonia	• Protezione dei dati personali	• Direttiva 95/46/CE [ora abrogata dal Regolamento 2016/679]	• Augstākā tiesa (Corte suprema, Lettonia) • Corte di giustizia	• Verticale: Domanda di pronuncia pregiudiziale ai sensi dell'art. 267 TFUE sull'interpre tazione della direttiva 95/46/CE • Orizzontale: la CG richiama la giurisprudenza della Corte EDU in materia di libertà di espressione	• La CG riconosce l'applicabilità della direttiva e che la registrazione di un video e la sua pubblicazione su un sito Internet accessibile a un numero indefinito di persone può costituire, a determinate condizioni, un trattamento di dati personali esclusivamente a scopi giornalistici

3. Cronologia

Mentre si trovava presso i locali di un commissariato della polizia nazionale, il sig. Buivids aveva filmato le operazioni di raccolta della sua deposizione nell'ambito di un procedimento per illecito amministrativo. Il sig. Buivids ha quindi pubblicato il video sul sito www.youtube.com.

La Corte suprema lettone, nutrendo dei dubbi circa l'ambito di applicazione della direttiva 95/46/CE e la sua interpretazione ha deciso di sospendere il procedimento e sollevare due questioni pregiudiziali

14 febbraio 2019: sentenza della Corte di giustizia nella causa C-345/17 *Buivids*

4. Descrizione

a. Fatti

Mentre si trovava presso i locali di un commissariato della polizia nazionale, il sig. Buivids aveva filmato le operazioni di raccolta della sua deposizione nell'ambito di un procedimento per illecito amministrativo. Il sig. Buivids aveva quindi pubblicato il video così registrato – che

mostrava alcuni agenti di polizia e le attività da essi esercitate all'interno del commissariato, compreso udire le loro conversazioni – sul sito www.youtube.com.

L'Agenzia nazionale per la protezione dei dati aveva ritenuto che il video violasse la disciplina sulla protezione dei dati, in quanto il sig. Buivids non aveva comunicato agli agenti di polizia, nella loro qualità di interessati, le informazioni relative alla finalità del trattamento dei dati personali. Inoltre, il sig. Buivids non aveva neppure comunicato all'Agenzia le informazioni relative alla finalità della registrazione in questione e della sua pubblicazione. L'Agenzia aveva quindi chiesto al sig. Buivids di rimuovere il video dai siti Internet in cui era stato caricato.

Il sig. Buivids aveva adito il tribunale amministrativo competente per ottenere la declaratoria di illegittimità di tale decisione, nonché il risarcimento dei danni asseritamente subiti, sostenendo che la pubblicazione del video avesse come scopo di attirare l'attenzione sulla condotta, a suo avviso illecita, delle forze di polizia. Il tribunale aveva tuttavia respinto il ricorso. Allo stesso modo, anche l'impugnazione del sig. Buivids avverso la pronuncia di primo grado era stata respinta, in quanto egli non aveva indicato quale fosse la finalità della pubblicazione del video in questione.

Il sig. Buivids aveva pertanto presentato ricorso per cassazione dinnanzi all'*Augustākā tiesa* (Corte suprema della Lettonia), facendo valere il suo diritto alla libertà di espressione. Nutrendo dei dubbi circa l'ambito di applicazione della direttiva 95/46 e sulla sua interpretazione, la Corte suprema aveva quindi deciso di sospendere il procedimento e di rivolgersi alla Corte di giustizia in via pregiudiziale.

b. Ragionamento della Corte di giustizia

In primo luogo, la Corte è chiamata a valutare se la registrazione video di taluni agenti di polizia all'interno di un commissariato, durante la raccolta di una deposizione, e la pubblicazione del video così registrato su un sito Internet, rientrano nell'ambito di applicazione della direttiva 95/46/CE.

Richiamando la sua precedente giurisprudenza, la Corte afferma che l'immagine di una persona registrata da una telecamera costituisce un dato personale ai sensi della direttiva, e che pertanto, dato che nel video è possibile vedere e ascoltare gli agenti di polizia, le immagini delle persone in tal modo registrate costituiscono altrettanti dati personali. Inoltre, una registrazione video delle persone immagazzinata in un dispositivo di registrazione continua, ossia una memoria di una fotocamera, costituisce un trattamento di dati personali automatizzato. Così come è da qualificarsi come trattamento di dati, almeno in parte automatizzato, l'operazione consistente nel far comparire su una pagina Internet dati personali. Pertanto, secondo la Corte, la pubblicazione – su un sito Internet dove gli utenti possono inviare, visionare e condividere contenuti video – di una registrazione video, come quella in questione, nella quale appaiono dati personali, costituisce un trattamento interamente o parzialmente automatizzato.

La Corte prende poi in esame i casi in esclusione dell'applicazione della direttiva: in primo luogo, al trattamento dei dati personali relativo ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione e, comunque, ai trattamenti aventi ad oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato e le attività dello Stato in materia di diritto penale; in secondo luogo, ai trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico. Secondo la Corte, la registrazione e la pubblicazione del video da parte del sig. Buivids non rientra in nessuna delle ipotesi contemplate, perché non è assimilabile ad attività proprie degli Stati o delle autorità statali. Inoltre, il trattamento non può essere definito domestico o personale, in quanto la pubblicazione del video è avvenuta su

un sito Internet, senza alcuna restrizione di accesso, dove gli utenti possono inviare, visionare e condividere contenuti video, rendendo così accessibili i dati personali a un numero indefinito di persone. Pertanto, secondo la Corte, il trattamento dei dati in oggetto rientra nell'ambito di applicazione della direttiva.

In secondo luogo, la Corte prende in esame il rapporto tra il diritto fondamentale alla vita privata, ai sensi dell'art. 7 della Carta, e quello alla libertà di espressione e di informazione, di cui all'art. 11 della Carta. In particolare, la Corte è chiamata a pronunciarsi circa la possibilità che una registrazione video di taluni agenti di polizia all'interno di un commissariato, durante la raccolta di una deposizione, e la pubblicazione del video così registrato su un sito Internet accessibile a un numero indefinito di persone, possa costituire un trattamento di dati a scopi giornalistici ai sensi della direttiva 95/46/CE. Infatti, qualora tale trattamento sia stato effettuato esclusivamente a scopi giornalistici, ciò comporterebbe l'applicazione di determinate esenzioni e deroghe, ai sensi di tale direttiva.

La Corte, innanzitutto, ricorda l'importanza della libertà di espressione in ogni società democratica e della necessità di interpretare in senso ampio le nozioni ad essa correlate, tra cui quella di giornalismo. Infatti, le deroghe ed esenzioni non solo si applicano alle imprese operanti nei media, ma anche a chiunque svolga attività giornalistica. Tale attività è definita dalla Corte come quella diretta a divulgare al pubblico informazioni, opinioni o idee, indipendentemente dal mezzo di trasmissione utilizzato.

Nel caso di specie, il fatto che il sig. Buivids non sia un giornalista professionista non esclude, secondo la Corte, che la registrazione e la pubblicazione del video possano rientrare nell'ambito di applicazione di tali esenzioni e deroghe. In particolare, il fatto che il fatto che il video sia stato caricato su un sito Internet come Youtube, non può, di per sé, privare tale trattamento dei dati personali della qualità di essere effettuato esclusivamente a scopi giornalistici. In tal senso, la Corte dà atto dell'evolversi e del moltiplicarsi dei mezzi di comunicazione e di diffusione di informazioni e che il supporto mediante il quale vengono trasmessi i dati oggetto di trattamento non è determinante per valutare se si tratti di un'attività esclusivamente a scopi giornalistici.

Tuttavia, non tutte le informazioni pubblicate su Internet che riguardino dati personali rientrano nella nozione di attività giornalistiche. Secondo la Corte, spetta al giudice nazionale stabilire se la registrazione e la pubblicazione del video abbiano quale unica finalità la divulgazione al pubblico di informazioni, opinioni o idee. A tale scopo, il giudice nazionale potrà, in particolare, prendere in considerazione il fatto che, secondo il sig. Buivids, il video in questione è stato pubblicato su un sito Internet per richiamare l'attenzione della società su condotte, a suo avviso irregolari, tenute dalla polizia durante la raccolta della sua deposizione. Al contrario, qualora risultasse che la registrazione e la pubblicazione di detto video non abbiano quale unica finalità la divulgazione al pubblico di informazioni, opinioni o idee, non si potrà dichiarare che il trattamento dei dati personali sia stato effettuato esclusivamente a scopi giornalistici.

Tuttavia, le esenzioni e deroghe devono essere applicate solo nella misura in cui siano necessarie per conciliare due diritti fondamentali, vale a dire il diritto alla protezione della vita privata e alla libertà di espressione. In particolare, per ottenere un equilibrato contemperamento di questi due diritti fondamentali, la tutela del diritto alla vita privata richiede che le deroghe e le limitazioni alla protezione dei dati operino entro i limiti dello stretto necessario. A tale proposito, la Corte ricorda che l'art. 7 della Carta ha lo stesso significato e portata dell'art. 8 della CEDU e, pertanto, in base all'art. 52, par. 3, della Carta, il significato e la portata degli stessi sono almeno uguali a quelli conferiti dalla suddetta Convenzione e dall'interpretazione fornita dalla Corte EDU. Lo stesso vale per l'art. 11 della Carta e l'art. 10 della CEDU.

A tale proposito, la Corte di giustizia richiama la giurisprudenza della Corte EDU, dalla quale emergono una serie di criteri rilevanti che devono essere presi in considerazione per effettuare la ponderazione tra i due diritti fondamentali; segnatamente, il contributo a un dibattito di interesse generale, la notorietà dell'interessato, l'oggetto del *reportage*, la condotta anteriore dell'interessato, il contenuto, la forma e le conseguenze della pubblicazione, le modalità e le circostanze in cui le informazioni sono state ottenute, nonché la loro veridicità. Allo stesso modo, deve essere presa in considerazione la possibilità per il responsabile del trattamento di adottare misure atte a ridurre l'entità dell'interferenza con il diritto alla vita privata.

Nel caso di specie, la Corte rileva che non si può escludere che la registrazione e la pubblicazione del video da parte del sig. Buivids costituiscano un'ingerenza nel diritto fondamentale al rispetto della vita privata degli agenti di polizia che appaiono nel video. Qualora emerga che la registrazione e pubblicazione abbiano come unica finalità, la divulgazione al pubblico di informazioni, opinioni o idee, il giudice nazionale dovrà comunque verificare se le esenzioni e le deroghe previste dalla direttiva risultino necessarie per conciliare il diritto alla vita privata con le norme che disciplinano la libertà di espressione, e se tali esenzioni e deroghe operino nei limiti dello stretto indispensabile.

In definitiva, secondo la Corte, la registrazione video di taluni agenti di polizia all'interno di un commissariato, durante la raccolta di una deposizione, e la pubblicazione del video così registrato su un sito Internet dove gli utenti possono inviare, visionare e condividere contenuti video, possono costituire un trattamento di dati personali esclusivamente a scopi giornalistici, sempre che da tale video risulti che detta registrazione e detta pubblicazione abbiano quale unica finalità la divulgazione al pubblico di informazioni, opinioni e idee.

c. Esito a livello nazionale

Non disponibile.

5. Analisi

i. Il ruolo della Carta

La sentenza *Buivids* appare particolarmente importante sotto il profilo del bilanciamento tra due diritti fondamentali: il diritto alla protezione della vita privata, sancito dall'art. 7 della Carta, e il diritto alla libertà di espressione, di cui all'art. 11 della Carta.

Sia l'art. 7 sia l'art. 11 della Carta trovano un corrispettivo nella Convenzione EDU, rispettivamente gli artt. 8, par. 1, e 11 della Convenzione. Ciò rileva, in particolare per quanto riguarda l'interpretazione e la portata dei diritti sanciti nella Carta, che, in base all'art. 52, par. 3, devono essere almeno uguali a quelle dei diritti sanciti nella Convenzione, come interpretati dalla Corte EDU.

Nella sentenza, la Corte, pur riconoscendo che la registrazione e pubblicazione di video su Internet possano costituire un'ingerenza nel diritto fondamentale al rispetto della vita privata, rimette esclusivamente al giudice nazionale la verifica se tali attività possano beneficiare di esenzioni o deroghe, in quanto necessarie a conciliare il diritto alla vita privata con le norme che disciplinano la libertà di espressione. Inoltre, la Corte ritiene che deve essere sempre il giudice nazionale a procedere alla verifica che tali esenzioni e deroghe operino "nei limiti dello stretto indispensabile", senza tuttavia fornire alcuna indicazione in tal senso.

j. Dialogo giuridico

Interazione verticale tra il giudice nazionale, l'*Augustākā tiesa* (Corte suprema, Lettonia) e la Corte di giustizia, attraverso il meccanismo del rinvio pregiudiziale.

Interazione orizzontale: la Corte di giustizia richiama la giurisprudenza della Corte EDU in materia di ponderazione dei diritti fondamentali alla protezione della vita privata e alla libertà di espressione (sentenza Corte EDU, 27 giugno 2017, *Satakunnan Markkinapörsse Oy* e *Satamedia Oy* c. *Finlandia*, ricorso n. 931/13).

k. Impatto della decisione della Corte di giustizia

In primo luogo, la sentenza in oggetto, rileva in quanto precisa l'ambito di applicazione della direttiva 95/46 e, in particolare, delle sue eccezioni: la direttiva non si applica per l'esercizio di attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, nonché riguardo a trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

Con l'entrata in vigore del regolamento 16/679, l'art. 2, rubricato "Ambito di applicazione materiale", riprende in gran parte i casi in cui anche la direttiva non poteva trovare applicazione. In riferimento alle attività a carattere esclusivamente personale o domestico, il regolamento fornisce tuttavia una precisazione, in quanto il considerando n. 18 prevede che "il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei *social network* e attività online intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico".

In secondo luogo, la Corte analizza la questione del bilanciamento tra due diritti fondamentali, la protezione della vita privata e la libertà di espressione. Nella direttiva 95/46 tale questione era disciplinata dall'art. 9 "Trattamento dei dati e libertà di espressione", il quale prevedeva l'applicazione di alcune deroghe ed esenzioni nel caso il trattamento dei dati fosse ad esclusivi fini giornalistici o di espressione artistica o letteraria. Con l'entrata in vigore del regolamento 16/679, l'art. 85 riprende il contenuto dell'art. 9 della direttiva, omettendo tuttavia il riferimento al "trattamento esclusivo" e prevedendo l'applicazione di esenzioni e deroghe non solo ai fini del trattamento effettuato a scopi giornalistici, di espressione artistica o letteraria, ma anche "di espressione accademica". Anche il considerando n.153 del regolamento, pur riprendendo anch'esso in gran parte il contenuto del considerando n. 37 della direttiva dedicato al bilanciamento tra i due diritti fondamentali, aggiunge che: "per tenere conto dell'importanza del diritto alla libertà di espressione in tutte le società democratiche è necessario interpretare in modo esteso i concetti relativi a detta libertà, quali la nozione di giornalismo". Tale precisazione sembra quindi codificare (anche se in maniera molto generale) la giurisprudenza della Corte di giustizia sul punto.

l. Altri casi rilevanti

Sulla pubblicazione di dati personali su Internet e il bilanciamento con la libertà di espressione:

- Corte di giustizia, sentenza del 6 novembre 2003, *Lindqvist*, causa C-101/01;
- Corte di giustizia (Grande sezione), sentenza del 16 dicembre 2008, *Satamedia*, C-73/07.

Sulla nozione di "esercizio di attività a carattere esclusivamente personale o domestico":

- Corte di giustizia, sentenza dell'11 dicembre 2014, *František Ryneš*, causa C-212/13.

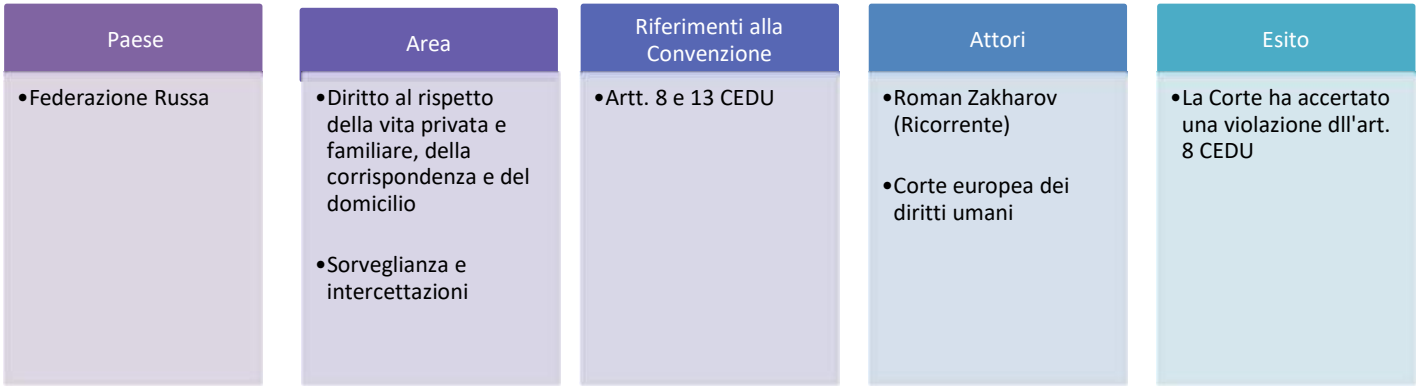
Scheda 10 – Il bilanciamento tra esigenze di sicurezza nazionale e tutela della vita privata secondo la Corte EDU

- Corte europea dei diritti umani (Grande Camera), *Roman Zakharov c. Federazione Russa*, ricorso n. 47143/06, sentenza del 4 dicembre 2015.

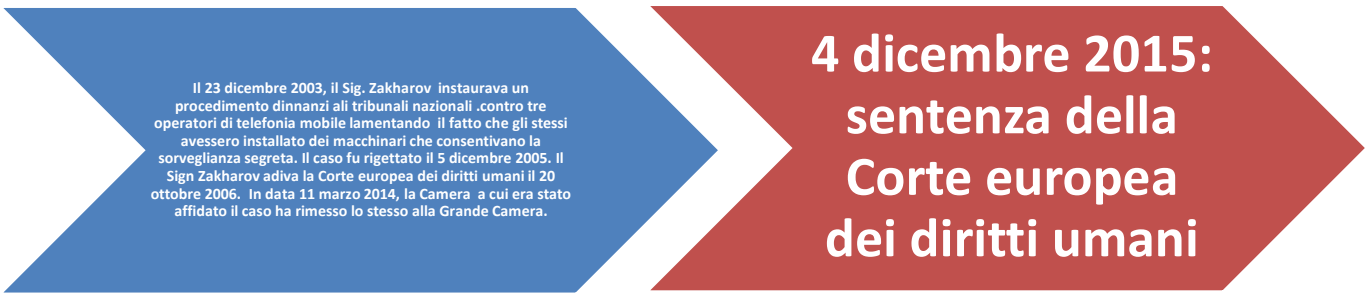
6. Aspetti centrali

L'intercettazione di comunicazioni telefoniche ai fini di sorveglianza è ammissibile qualora sia motivata, tra l'altro, da ragioni di sicurezza nazionale o prevenzione del crimine.
Tuttavia, il rischio che caratterizza ogni attività di sorveglianza segreta, ossia la possibilità che la stessa sia usata per danneggiare, o finanche distruggere, l'ordinamento democratico, impone che siano prestate garanzie adeguate ed efficaci per prevenire forme di abuso. Tali garanzie possono includere: il monitoraggio dell'attività di sorveglianza; la durata ridotta della stessa; l'esistenza di una procedura di autorizzazione per la sorveglianza e la detenzione dei dati oggetto di intercettazione; la previsione di rimedi disponibili all'individuo per contestare l'intercettazione.

7. A colpo d'occhio



8. Cronologia



9. Descrizione

d. Fatti

Il sig. Zakharov, nato nel 1977 e residente a San Pietroburgo, era caporedattore di una rivista in materia di aviazione e presidente della sezione di San Pietroburgo di un'organizzazione non governativa (*Glasnots Defence Foundation*) impegnata nel monitoraggio della libertà di stampa e nella promozione dell'indipendenza dei mezzi di comunicazione di massa nella Federazione Russa. Il Sig. Zakharov era cliente di numerosi operatori di telefonia mobile.

Nel 2006, il Sig. Zakharov instaurava un procedimento davanti ai tribunali nazionali contro tre operatori di telefonia mobile, lamentando un'interferenza nel proprio diritto al rispetto della vita privata e familiare. Ciò in quanto gli operatori telefonici convenuti, in conformità a un provvedimento adottato dal Ministero delle comunicazioni, mai reso pubblico, avrebbero installato delle apparecchiature in grado di permettere ai servizi di sorveglianza di intercettare tutte le comunicazioni telefoniche senza bisogno di una preventiva autorizzazione da parte del giudice. Il Sig. Zakharov chiedeva, pertanto, ai tribunali aditi di ordinare agli operatori di telefonia la rimozione delle suddette apparecchiature.

A seguito del rigetto del ricorso da parte del tribunale di prima istanza e della corte di appello, motivato sulla base dell'assenza di prove circa l'effettiva intercettazione delle comunicazioni del Sig. Zakharov, quest'ultimo adiva la Corte EDU, lamentando la violazione da parte dello Stato russo degli artt. 8 (diritto al rispetto della vita privata e familiare) e 13 (diritto a un rimedio effettivo) della CEDU.

e. Ragionamento della Corte europea dei diritti umani

In primo luogo, la Corte EDU affronta la questione della ricevibilità del ricorso. Lo Stato convenuto aveva, infatti, eccepito il mancato esaurimento delle vie di ricorso interne, nonché l'impossibilità di considerare il Sig. Zakhorov vittima di una violazione della Convenzione. La Corte rigetta entrambe le eccezioni. Con particolare riferimento all'assenza della qualità di vittima, la Corte nota come la mera esistenza di una legge che autorizza le intercettazioni segrete delle comunicazioni telefoniche e il conseguente rischio che le proprie comunicazioni siano intercettate sono elementi sufficienti affinché un individuo possa considerarsi vittima di una violazione dell'art. 8 della Convenzione, a patto che alcune condizioni siano soddisfatte. Non è invece necessario che l'individuo dimostri l'effettiva intercettazione delle proprie comunicazioni. Le condizioni richieste sono: il fatto che l'individuo sia tra coloro potenzialmente colpiti dall'attività di sorveglianza, in quanto membro di un gruppo al quale l'attività di sorveglianza si rivolge o poiché la misura prevista è di carattere generale; l'assenza di un rimedio effettivo a fronte di possibili abusi. Nel caso di specie, la Corte ravvisa entrambe le condizioni: la misura prevista dal provvedimento russo ha carattere generale e non sono previsti rimedi effettivi per coloro che subiscono l'attività di sorveglianza. Conseguentemente, la Corte riconosce la qualità di vittima del Sig. Zakharov, nonostante egli non sia in grado di provare l'avvenuta intercettazione delle proprie comunicazioni telefoniche.

In secondo luogo, la Corte esamina se l'interferenza statale nel godimento del diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, sancito all'art. 8 della CEDU, sia giustificata. La Corte, in particolare, si concentra sull'assenza di prevedibilità e necessità della misura legislativa che istituisce il sistema di sorveglianza. La Corte ravvisa criticità nelle disposizioni concernenti, tra l'altro, le modalità con cui le autorità pubbliche possono ricorrere ad attività di sorveglianza; la durata di tali misure; la detenzione e la distruzione dei dati raccolti (stante la mancanza di chiarezza); il monitoraggio dell'attività di sorveglianza (in quanto non conforme ai requisiti di indipendenza e competenza); la portata limitata dei rimedi previsti.

Conseguentemente, la Corte stabilisce che il sistema di sorveglianza previsto per legge in Russia non fornisce garanzie adeguate ed effettive a fronte di possibili abusi e, pertanto, non ritiene soddisfatti i requisiti di "qualità della norma" e di "necessità in una società democratica".

La Corte riconosce l'intervenuta violazione dell'art. 8 della CEDU da parte della Federazione Russa.

Alla luce di quanto affermato con riferimento all'art. 8, la Corte non ritiene necessario esaminare separatamente l'asserita violazione dell'art. 13 della stessa Convenzione.

f. Esito a livello nazionale

Non disponibile.

10. Analisi

l. Considerazioni generali

Con la presente sentenza, la Corte ha confermato i suoi precedenti orientamenti giurisprudenziali in materia di intercettazioni e sorveglianza. Tuttavia, la Corte ha applicato la sua giurisprudenza all'analisi di un intero sistema di sorveglianza, così individuando i criteri ai quali anche altri sistemi di sorveglianza dovranno adeguarsi per non interferire con il godimento del diritto al rispetto della vita privata e familiare. Più in generale, la Corte ha ribadito la pericolosità dei programmi di sorveglianza per il mantenimento dell'ordine democratico e la necessità di sottoporre tali pratiche a un attento scrutinio.

Preme rilevare, inoltre, come la Corte, nel valutare la compatibilità della legislazione russa con la Convenzione, non si sia limitata al dato letterale, ma abbia intrapreso un'analisi accurata dell'applicazione pratica delle disposizioni.

Tale sentenza è stata emessa dopo le decisioni della Corte di giustizia nei casi *Digital Rights* e *Schrems* (v. *supra* schede 2 e 4) e alla prima delle due sentenze la Corte rinvia esplicitamente nell'identificare il diritto applicabile al caso in esame.

m. Altri casi rilevanti

Sull'intercettazione di comunicazioni nello svolgimento di attività di sorveglianza e la possibile interferenza nel godimento del diritto al rispetto della vita privata e familiare di cui all'art. 8 della CEDU si vedano anche:

- Corte europea dei diritti umani, *Szabó and Vissy c. Ungheria*, ricorso n. 37138/14, sentenza del 12 gennaio 2016;
- Corte europea dei diritti umani, *Mustafa Sezqin Tanrikulu c. Turchia*, ricorso n. 27473/06, sentenza del 18 luglio 2017;
- Corte europea dei diritti umani, *Big Brother Watch and Others c. Regno Unito*, ricorsi n. 58170/13 62322/14 24960/15, sentenza del 13 settembre 2018 (rinviato alla Grande Camera).

Bibliografia essenziale sull'applicazione della Carta dei diritti fondamentali nell'ambito della protezione dei dati (in italiano)

BESTAGNO, *Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali*, in *Il diritto dell'Unione europea*, 2015, p. 25 ss.

CAGGIANO, *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in *Studi sull'integrazione europea*, 2018, p. 9 ss.

CAMPIGLIO, *Articolo 7*, in POCAR e BARUFFI (a cura di), *Commentario breve ai Trattati dell'Unione europea*, Milano, 2014, p. 1678 ss.

PIRODDI, *Articolo 8*, in POCAR e BARUFFI (a cura di), *Commentario breve ai Trattati dell'Unione europea*, Milano, 2014, p.1682 ss.