Giusella Finocchiaro

La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain *a* Schrems

Sommario: Introduzione. – 1. Le scelte politiche. – 2. Gli argomenti giuridici. – 2.1. La rilevanza degli artt. 7 e 8 della Carta dei diritti fondamentali. 2.2. L'interpretazione estensiva della nozione di 'stabilimento'. – 3. Ulteriori indicazioni interpretative. – 3.1. La pluralità di leggi nazionali applicabili. – 3.2. Distinzione fra 'dato personale' e 'valutazione'. Definizione di 'trattamento'. – 3.3. Bilanciamento fra il diritto all'accesso ai documenti amministrativi e il diritto alla protezione dei dati personali. – 3.4. Trattamento dei dati personali da parte di un'autorità amministrativa. Obbligo di informativa. – 3.5. Elementi biometrici dei passaporti e dei documenti di viaggio. – Conclusioni

Introduzione

La giurisprudenza della Corte di giustizia europea in materia di dati personali da *Google Spain* a *Schrems* appare piuttosto ricca, a conferma della rilevanza strategica che ha assunto questo tema nell'Unione europea.

Si tratta di una decina di sentenze in meno due anni, elencate in nota[1],

[1*]Il commento rientra nell'ambito del PRIN 2010 - 2011, «La regolamentazione giuridica delle Tecnologie dell'Informazione e della Comunicazione (TIC) quale strumento di potenziamento delle società inclusive, innovative e sicure». Le sentenze della Corte di giustizia europea riguardanti il trattamento di dati personali, che succedono alla sentenza del 13 maggio 2014, *Google Spain, Google Inc. e Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* (causa C-131/12) sono elencate di seguito: Corte di giustizia, sentenza del 17 luglio 2014, cause riunite C-141/12 e C-372/12, *Y.S. e a.*; Corte di giustizia, sentenza del 2 ottobre 2014, causa C-127/13 P, *Strack/Commissione*; Corte di giustizia, sentenza dell'11 dicembre 2014, causa C-212/13, *Ryneš*; Corte di giustizia, sentenza del 16 aprile 2015, cause riunite da C-446/12 a C-449/12, *Willelms e a.*; Corte di giustizia, sentenza del 16 luglio 2015, causa C-615/13 P, *ClientEarth e PAN Europe/EFSA*; Corte di giustizia, sentenza del 16 luglio 2015, causa C-580/13, *Coty Germany;* Corte di giustizia, sentenza del 1° ottobre 2015, causa C-201/14, *Bara e a.*; Corte di giustizia, sentenza del 1° ottobre 2015, causa C-230/14, *Weltimmo*; Corte di giustizia, sentenza del 6 ottobre 2015, causa C-362/14, *Schrems,* cui si aggiunge per rilevanza, come sopra anticipato, Corte di giustizia, sentenza dell'8 aprile 2014, cause

cui si aggiunge per importanza, pur essendo di poco antecedente alla decisione *Google Spain*, la sentenza dell'8 aprile 2014, *Digital Rights Ireland* e *Seitlinger e a.* (cause riunite C-293/12 e C-594/12) [2].

riunite C-293/12 e C-594/12*, Digital Rights Ireland* e *Seitlinger e a.* Le sentenze possono essere tutte reperite all'URL www.curia.europa.eu .

[2] Si fa riferimento alla decisione della Corte di giustizia dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland e Seitlinger e a*. La sentenza ha origine da due distinte domande di pronuncia pregiudiziali riunite, presentate rispettivamente dalla High Court (Irlanda) e dal Verfassungsgerichtshof (Austria). Le domande di pronuncia pregiudiziale vertono sulla validità della 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, che modifica la direttiva 2002/58/CE. La Corte di giustizia dichiara la direttiva 2006/24/CE invalida, rilevando che: data l'estrema diffusione dei mezzi di comunicazione elettronica, la direttiva ha ingerenza sui diritti fondamentali della quasi totalità della popolazione europea; la direttiva riguarda in maniera generale qualsiasi persona e qualsiasi mezzo di comunicazione elettronica nonché l'insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi; la direttiva non prevede alcun criterio oggettivo né le condizioni sostanziali o procedurali che permettano di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore; la direttiva impone un periodo di conservazione dei dati di sei mesi ma non effettua alcuna distinzione tra le categorie di dati a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate e non determina la durata di conservazione in base a criteri obiettivi al fine di garantire che sia limitata allo stretto necessario. La Corte rileva, infine, che dal momento che tale direttiva non impone che i dati siano conservati sul territorio dell'Unione, non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente, esplicitamente richiesto dall'articolo 8, comma 3, della Carta dei diritti fondamentali dell'Unione europea. Conseguentemente la Corte ritiene che il legislatore dell'Unione abbia ecceduto i limiti imposti dal rispetto del principio di proporzionalità alla luce degli articoli 7, 8 e 52, comma 1, della Carta dei diritti fondamentali dell'Unione europea. In particolare sostiene che la direttiva non sia frutto di un corretto bilanciamento tra la necessità di garantire la sicurezza pubblica contro la criminalità grave, attraverso la conservazione dei dati personali nell'ambito delle comunicazioni elettroniche, e il diritto dei cittadini alla protezione dei dati personali, sotto il profilo del diritto fondamentale al rispetto della vita privata.

1. Le scelte politiche

Si leggono alcune tendenze, evidenti nelle due decisioni più note, *Google Spain* e *Schrems* [3], ma presenti anche in altre, di carattere politico[4], anticipatorie rispetto alle scelte ormai quasi compiute nell'emanando regolamento[5].

[3] A differenza di quanto verrà effettuato per le altre decisioni non si ritiene opportuno riassumere il contenuto delle due decisioni, rispettivamente oggetto di un numero monografico di *Dir. Inf.* il n. 4/5 del 2014, nonché di questo *Dir. Inf.* olume. Ci si limita qui a ricordare che i principi di diritto affermati nella decisione *Google Spain* sono tre. In primo luogo, la sentenza afferma che si applica la legge nazionale del Paese nel quale il motore di ricerca opera, esercitando anche altre attività, quali la promozione e la vendita degli spazi pubblicitari. In secondo luogo, che Google, e in generale i motori di ricerca, sono «titolari del trattamento» e pertanto che l'interessato ha il diritto di richiedere che sia rimossa l'indicizzazione direttamente al motore di ricerca, a prescindere da ogni richiesta al gestore del sito *web* che ha pubblicato l'informazione, anche nel caso in cui l'informazione sia stata e sia legittimamente pubblicata sul sito *web*. In terzo luogo, che l'interessato «ha diritto 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 una ricerca effettuata a partire dal suo nome» e che «nel valutare i presupposti di applicazione di tali disposizioni, si deve verificare in particolare se l'interessato abbia diritto a che l'informazione in questione 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, senza per questo che la constatazione di un diritto siffatto presupponga che l'inclusione dell'informazione in questione in tale elenco arrechi un pregiudizio a detto interessato». La recente decisione Schrems della Corte di giustizia europea invalida la decisione della Commissione nota come *Safe Harbour* e afferma che spetta agli Stati nazionali valutare se gli Stati Uniti siano da considerarsi un Paese che, ai sensi della direttiva-madre in materia di protezione dei dati personali, garantisce un livello di tutela adeguato.

[4] Evidenziano l'indirizzo politico assunto dalla Corte di giustizia già dal caso *Google*: Pollicino, *Un* digital right to *privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel* reasoning *di* Google Spain, in *Dir. Inf.* 2014, p. 569 ss.; G. Sartor - M. Viola de Azevedo Cunha, *Il caso* Google *e i rapporti regolatori Usa/EU*, in *Dir. Inf.* 2014, p. 657 ss. e A. Mantelero, *Il futuro regolamento EU sui dati personali e la valenza 'politica' del caso* Google*: ricordare e dimenticare nella* digital economy, in *Dir. Inf.* 2014, p. 681 ss. La scelta della Corte di anticipare il contenuto dell'emanando regolamento è sottolineata da: P. Piroddi, *Questioni internazionalprivatistiche sui motori di ricerca*, in *Dir. Inf.* 2014, p. 623 ss. e ancora da O. Pollicino, *op. cit.,* in particolare p. 587 ss., A. Mantelero, *op.cit.*

[5] Si tratta ovviamente della proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), adottata dalla Commissione il 25 gennaio 2012, n. 2012/0011 consultabile all'URL http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52012PC0011.Il 12 marzo 2014 anche il Parlamento europeo ha votato in prima lettura sulla proposta.

In estrema sintesi, la Corte vuole affermare l'applicabilità della normativa europea anche nel caso in cui i titolari di trattamento dei dati personali siano soggetti non europei e i dati vengano trattati prevalentemente fuori dall'Europa. Ribadisce il rango costituzionale del diritto alla protezione dei dati personali secondo la Carta dei diritti fondamentali dell'Unione europea e soprattutto la prevalenza di tale diritto sugli altri diritti, pure costituzionalmente garantiti, affermando così una scelta culturale e di principi[6]. Riafferma il carattere di eccezionalità delle limitazioni al diritto alla protezione dei dati personali. Assume che il livello di protezione dei dati personali adottato in Europa sia più elevato rispetto al livello di protezione dei dati personali adottato altrove nel mondo e si fa promotrice del modello europeo del diritto alla protezione dei dati personali. La Corte europea si riappropria e consolida la posizione volta ad affermare l'applicazione del diritto europeo al trattamento dei dati personali degli europei. Si tratta di indirizzi profondamente politici in cui la Corte orgogliosamente sceglie cultura, principi e diritto europeo, contrapponendosi alla visione e agli interessi, nei casi in esame, statunitensi[7].

La Corte esercita dunque un ruolo di supplenza politica, estendendo l'applicabilità della normativa europea e anticipando nell'interpretazione

Il 15 giugno 2015, dopo un lungo e travagliato iter di approvazione, anche il Consiglio «Giustizia e affari interni» ha raggiunto un accordo generale sulla proposta di regolamento, permettendo così l'apertura dei triloghi con il Parlamento europeo e la Commissione il 24 giugno 2015. A distanza di pochi mesi, in una riunione straordinaria tenutasi il 17 dicembre 2015, la Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo ha espresso la sua posizione sui testi concordati nei negoziati in forma di trilogo tra il Consiglio, il Parlamento europeo e la Commissione. Il 18 dicembre 2015 il Comitato dei rappresentanti permanenti (Coreper) ha approvato il testo di compromesso. I testi saranno ora presentati, ai fini dell'adozione di un accordo politico, in una prossima sessione del Consiglio. Dopo l'adozione della posizione del Consiglio in prima lettura, i testi saranno trasmessi al Parlamento per l'approvazione. Si prevede che il regolamento e la direttiva entreranno in vigore nella primavera del 2016 e saranno applicabili a partire dalla primavera del 2018. L'evoluzione dell'iter di approvazione del «pacchetto protezione dati» è consultabile nei seguenti siti, dai quali sono state tratte le informazioni sopra riassunte: http://eur-lex.europa.eu/legal-content/IT/HIS/?uri=CELEX:52012PC0011 - http://www.consilium.europa.eu/it/policies/data-protection-reform/ - http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4443361

[6] Su questo punto, v. O. Pollicino, *op. cit.* che fra l'altro sottolinea il 'capovolgimento temporale' (*sic* p. 576) operato dalla Corte, secondo la quale sono gli artt. 7 e 8 della Carta a ricevere attuazione da parte di disposizioni di diritto derivato di cinque anni precedenti.

[7] Sul punto, v. G. Sartor - M. Viola de Azevedo Cunha, *op. cit.*, con ampia bibliografia.

della direttiva-madre l'emanando regolamento europeo sulla protezione dei dati personali.

Il fenomeno appare immediatamente leggibile nelle decisioni *Google Spain* e *Schrems* ma gli argomenti giuridici sono altresì ampiamente elaborati in *Digital Rights Ireland* e in *Weltimmo*[8].

2. Gli argomenti giuridici

I macroargomenti giuridici elaborati dalla Corte sono due. Innanzitutto la rilevanza degli artt. 7 e 8 della Carta dei diritti fondamentali e la prevalenza del diritto alla protezione dei dati personali e alla vita privata (prevalentemente intesi come un'endiadi) sugli altri diritti. In secondo luogo, l'interpretazione estensiva dell'art. 4 della direttiva sull'applicabilità territoriale della stessa e, in particolare, della nozione di 'stabilimento'.

2.1 La rilevanza degli artt. 7 e 8 della Carta dei diritti fondamentali

La Corte conferma ed enfatizza non solo la rilevanza costituzionale, ma anche la supremazia valoriale degli artt. 7 e 8 della Carta dei diritti

[8] La domanda di pronuncia pregiudiziale verte sull'interpretazione degli articoli 4, paragrafo 1, lettera a), e 28, paragrafi 1, 3 e 6, della direttiva 95/46/CE. Nel caso di specie la Weltimmo, società registrata in Slovacchia, gestiva un sito Internet di annunci immobiliari riguardanti beni situati in Ungheria. Nell'ambito di tale attività, essa trattava i dati personali degli inserzionisti. A seguito di un'ipotesi di trattamento illecito dei dati, gli inserzionisti presentavano reclamo all'autorità ungherese preposta alla tutela dei dati personali, che comminava alla Weltimmo un'ammenda per aver violato la legge ungherese di attuazione della direttiva 95/46/CE. La Weltimmo contestava la decisione dell'autorità di controllo ungherese adducendo che non avrebbe potuto irrogare l'ammenda non avendo titolo per applicare la legge del proprio paese, adottata sulla base della direttiva 95/46/CE. Chiamata a dirimere la controversia, la Corte suprema adiva la Corte di giustizia per chiarire se, nel caso di specie, la direttiva consentisse all'autorità ungherese di controllo di applicare la legge ungherese adottata sulla base della direttiva e di imporre l'ammenda prevista da tale legge. Secondo la Corte di giustizia, come si avrà modo di illustrare nel corso di questo lavoro, l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46/CE, deve essere interpretato nel senso che esso consente l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile del trattamento di tali dati è registrato, purché il medesimo svolga, tramite un'organizzazione stabile nel territorio di tale Stato membro, un'attività effettiva e reale, anche minima, nel contesto della quale si svolge tale trattamento.

fondamentali dell'Unione europea[9] che si riferiscono rispettivamente al rispetto della vita privata e della vita familiare e alla protezione dei dati di carattere personale e che costituiscono, come la Corte ribadisce, la base per l'interpretazione della direttiva 95/46/CE[10].

Come è noto, l'art. 8 della Carta, significativamente fra i diritti di libertà, afferma il diritto alla protezione dei dati personali, e precisamente che ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Afferma, inoltre, che i dati personali devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o ad un altro fondamento legittimo previsto dalla legge e che ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Sempre nell'art. 8 si afferma che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente[11].

Tale diritto è distinto dal diritto alla protezione della vita privata, altra formulazione del diritto alla riservatezza, riconosciuto dall'art. 7 della Carta, ove si afferma il diritto al rispetto della vita privata e della vita familiare: ogni individuo, dispone la norma, ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

Il diritto alla protezione dei dati personali ha un oggetto estremamente vasto, che è conseguenza della stessa definizione di dato personale. Muovendo, infatti, dall'ampia definizione di dato personale, il diritto alla protezione dei dati personali si configura come il diritto di un soggetto di controllare l'insieme delle informazioni che al medesimo si riferiscono e che quindi costituiscono il suo riflesso e delineano lo stesso suo essere nella società dell'informazione.

Il diritto alla protezione dei dati personali è anche noto come «information privacy», «informational privacy», «data privacy», tutte espressioni nelle quali si evidenzia che l'oggetto del diritto è l'informazione o il dato, benché a rigore dato e informazione siano termini non coincidenti.

Il diritto alla protezione dei dati personali deve essere considerato distinto dalla libertà negativa di non subire interferenze nella propria vita privata, al cuore del diritto alla riservatezza, costituendo invece il fondamento della libertà positiva di esercitare un controllo sul flusso delle proprie informazioni. Per questa ragione è frequente che il diritto alla protezione dei dati

[9] In tal senso, *ex multis, Digital Rights Ireland*, punto 53; *Google Spain*, punti 53, 66 e 74 nonché Schrems, punto 39.
[10] Così *Google Spain* punto 68; *Ryneš*, punto 29 e *Schrems*, punto 38.
[11] Per approfondimenti si rinvia a G. Finocchiaro, *Privacy e protezione dei dati personali*, Zanichelli, Bologna, 2012.

personali sia inteso come diritto all'autodeterminazione informativa, cioè alla scelta di ogni soggetto di autodefinirsi e determinarsi.

Il necessario carattere di eccezionalità delle deroghe al diritto fondamentale alla tutela dei dati personali è sancito nella decisione *Digital Rights Ireland* ove si afferma che la direttiva 2006/24/CE (annullata dalla medesima decisione) non prevedendo «norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta, comporta un'ingerenza nei suddetti diritti fondamentali 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»[12]. Nella stessa decisione si afferma inoltre il ruolo essenziale dell'autorità di controllo da parte di un'autorità indipendente che «costituisce un elemento essenziale del rispetto della tutela delle persone riguardo al trattamento dei dati personali (v., in tal senso, sentenza Commissione/Austria, C-614/10, EU:C:2012:631, punto 37)»[13].

L'obiettivo della protezione dei dati personali dei cittadini europei che comporta un'estensione dell'ambito di applicazione della direttiva conduce addirittura a formulare l'ulteriore requisito che i dati siano conservati nel territorio europeo. Questa materializzazione della protezione è formulata nella sentenza *Digital Rights Ireland*, ove si afferma che dal momento che la direttiva 2006/24/CE (come si è detto, annullata nella medesima decisione) non impone che i dati di cui trattasi siano conservati sul territorio dell'Unione, non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente, esplicitamente richiesto dall'articolo 8, paragrafo 3, della Carta dei diritti fondamentali [14].

I medesimi argomenti sono più ampiamente sviluppati nel caso *Schrems* ove si afferma che una normativa europea «che comporta un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta deve prevedere, secondo la giurisprudenza costante della Corte, regole chiare e precise che disciplinino la portata e l'applicazione della misura *de qua* e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati».

E nella stessa decisione, riferendosi evidentemente al trattamento

[12] Punto 65 della decisione *Digital Rights Ireland*.
[13] Punto 68 della decisione *Digital Rights Ireland*.
[14] Così il punto 68 della sentenza *Digital Rights Ireland*. V. in senso critico O. Pollicino, *op. cit.*, in particolare p. 587.

attraverso i *social network*, si precisa altresì che tali garanzie acquisiscono maggiore importanza «allorché i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi (sentenza Digital Rights Ireland e a., C293/12 e C594/12, EU:C:2014:238, punti 54 e 55, nonché la giurisprudenza ivi citata)» [15].

Nella medesima decisione si richiama il principio che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario [16]. Ciò conduce la Corte a ritenere che non sia conforme al citato principio una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione 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 ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta e che una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta [17].

La Corte sottolinea la necessità della previsione per il singolo di potersi avvalere di rimedi giuridici per esercitare il proprio diritto al controllo sui suoi dati personali, controllo che costituisce l'essenza del diritto stesso alla protezione dei dati personali, e ribadisce che «l'esigenza 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 (v., in tal senso, sentenze Les Verts/Parlamento, 294/83, EU:C:1986:166, punto 23; Johnston, 222/84, EU:C:1986:206, punti 18 e 19; Heylens e a., 222/86, EU:C:1987:442, punto 14, nonché, UGTRioja e a., da C428/06 a C434/06, EU:C:2008:488, punto 80)»[18] .

L'eccezionalità delle deroghe al diritto alla protezione dei dati personali è richiamata anche dalla sentenza dell'11 dicembre 2014, causa C-212/13, *Ryneš*[19]. In questa decisione la Corte ribadisce l'eccezionalità dell'esclu-

[15] Così il punto 91 della sentenza *Schrems*.
[16] Così il punto 92 della sentenza *Schrems*.
[17] Così i punti 93 e 94 della sentenza *Schrems*.
[18] Così il punto 95 della sentenza *Schrems*.
[19] Nel caso di specie viene contestato al sig. Ryneš un illecito trattamento dei dati personali avvenuto attraverso l'installazione di un sistema di videosorveglianza all'esterno dell'abitazione personale, senza informare e richiedere il consenso dei passanti 'videore-

sione prevista dall'art. 3 della direttiva per il trattamento effettuato per ragioni personali o familiari [20].

2.2 L'interpretazione estensiva della nozione di 'stabilimento'

Nelle decisioni in esame la Corte estende l'ambito di applicazione della direttiva. In particolare, l'*iter* argomentativo utilizzato muove dall'interpretazione estensiva dell'art. 4 e della nozione di 'stabilimento', che conduce ad anticipare l'applicazione dell'art. 3 dell'emanando regolamento [21].

Infatti, secondo l'art. 4, comma 1, della direttiva, «Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali:

a) effettuato nel contesto delle attività di uno stabilimento del responsabile[22] del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati

gistrati'. Il sig. Ryneš adduceva che il sistema di videosorveglianza era stato installato per tutelare la vita sua e dei propri familiari, in quanto diritto fondamentale e inviolabile, e che il trattamento dei dati in questione rientrava nell'«esercizio di attività a carattere esclusivamente personale o domestico», escludendo l'applicabilità della direttiva 95/46/CE e dei conseguenti obblighi informativi e di raccolta del consenso per il trattamento.

[20] Così *Ryneš*, punto 28.

[21] Sulla nozione di stabilimento v. G. Caggiano, *L'interpretazione del «contesto delle attività di stabilimento» dei responsabili del trattamento dei dati personali, in Dir. Inf.* 2014, p. 605 ss.

[22] Si ricorda che la definizione di 'responsabile' di trattamento fornita dalla direttiva all'art. 2, comma 1, lett. d) è la seguente: «la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario". Essa dunque corrisponde alla definizione di 'titolare' del trattamento dei dati personali nel diritto italiano, che si legge all'art. 4, comma 1, lett. f) del decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, che definisce 'titolare', «la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza».Una figura analoga a quella del responsabile del trattamento prevista dal Codice in materia di protezione dei dati personali italiano non è invece contemplata dalla direttiva, la quale prevede due sole figure: il responsabile ('titolare' nell'attuazione italiana della direttiva) e l'incaricato (definito 'incaricato' anche nel Codice italiano).

membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile; […]» [23].

Cruciale diviene quindi l'interpretazione della nozione di 'stabilimento', che viene dilatata fino a divenire «nel contesto delle attività di uno stabilimento», contrapponendo così l'attività di trattamento 'nel contesto' e l'attività di trattamento 'in senso proprio', come si legge nelle conclusioni dell'avvocato generale nel caso *Weltimmo*. Ivi si legge altresì che l'articolo 4, paragrafo 1, lettera a), svolge una duplice funzione, consentendo da un lato, l'applicazione del diritto dell'Unione attraverso il diritto di uno dei suoi Stati membri quando il trattamento dei dati abbia luogo esclusivamente 'nel contesto' delle attività di uno stabilimento situato nel loro territorio, e ciò anche se il trattamento dei dati 'in senso proprio' viene effettuato in un terzo Stato (come accadeva nella causa *Google Spain* e *Google*) e consentendo dall'altro, di determinare la legge applicabile in quanto norma di conflitto tra le leggi dei diversi Stati membri (come appunto nel caso *Weltimmo*) [24].

Nel caso *Google Spain* è esplicito il tentativo della Corte di ampliare l'ambito di applicazione territoriale della direttiva 95/46/CE, attraverso un'interpretazione estensiva dell'art. 4, per assicurare ai dati di cittadini europei, trattati fuori dai confini dell'Unione, le medesime garanzie assicurate ai trattamenti dei dati effettuati all'interno dell'Unione. In particolare nell'individuare il luogo al quale collegare l'applicazione

[23] Sui criteri di applicabilità della direttiva 95/46/CE e sulla qualificazione dei medesimi sotto il profilo del diritto internazionale, molto è stato scritto. Si rinvia a C. Kuner, *European Data Protection Law-Corporate Compliance and Regulation*, 3rd ed., Oxford, 2007 e in particolare al capitolo terzo per un ampio e approfondito inquadramento del tema, a P. Piroddi, *op. cit.,* la quale evidenzia i vizi argomentativi della decisione *Google*, nonché a L. Moerel, *Back to basics: when does EU data protection law apply?* in *International Data Privacy Law,* 2011, Vol. 1, No. 2, pp. 92-110 e Id., *The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?* in *International Data Privacy Law*, 2011, Vol. 1, No. 1, pp. 28-46. In particolare Moerel ricostruisce la storia dell'art. 4 della direttiva e il passaggio dal criterio del paese di origine, che l'A. ritiene essere quello più efficace, chiaramente originariamente formulato, a criteri che conducono ad una pluralità di leggi nazionali applicabili. Si v. anche L.Colonna, *Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?* in *International Data Privacy Law*, 2014, Vol. 4, No. 3, pp. 203-22, fortemente critica sull'attuale art. 4 della direttiva, del quale fornisce una chiara illustrazione, ricordando i tre differenti approcci cui è riconducibile l'art. 4, rispettivamente basati sulla territorialità, sugli effetti e sulla protezione dei cittadini europei.

[24] Conclusioni dell'avvocato Generale in *Weltimmo*, punto 23.

della direttiva, la Corte ritiene rilevante non tanto il luogo in cui il trattamento dei dati viene fisicamente effettuato, quanto il luogo in cui la società che opera il trattamento esercita la propria attività, basata sul trattamento. Nel caso di specie la Corte osserva che Google Spain (con sede legale a Madrid) costituisce una filiale di Google Inc. (con sede legale negli Stati Uniti) nel territorio spagnolo e, pertanto, uno 'stabilimento' ai sensi della direttiva.

La Corte respinge l'argomento secondo cui il trattamento di dati personali da parte di Google Search non viene effettuato nel contesto delle attività di tale stabilimento in Spagna. La Corte considera al riguardo che, quando i dati vengono trattati per le esigenze di un motore di ricerca gestito da un'impresa che, sebbene situata in uno Stato terzo, dispone di uno stabilimento in uno Stato membro, il trattamento viene effettuato «nel contesto delle attività» di tale stabilimento, qualora quest'ultimo sia destinato ad assicurare, nello Stato membro in questione, la promozione e la vendita degli spazi pubblicitari proposti sul motore di ricerca al fine di rendere redditizio il servizio offerto da quest'ultimo[25].

Sui criteri per determinare il diritto applicabile e l'autorità competente di cui all'articolo 4 della direttiva 95/46/CE, dunque la Corte ripropone l'orientamento evidenziato in *Google Spain* nella recente sentenza *Weltimmo.* Pur essendo diverso il contesto in cui si inseriscono le due sentenze (mentre in *Google Spain* si discuteva sull'applicabilità o meno della direttiva a trattamenti di dati avvenuti fuori dai confini europei, in *Weltimmo* la controversia ha ad oggetto la determinazione di quale tra due legislazioni di Stati membri sia applicabile, in base allo Stato in cui il trattamento è avvenuto), in entrambe è centrale l'interpretazione del concetto di 'stabilimento' e di 'contesto delle attività'. Anche in *Weltimmo*, come in *Google Spain*, la Corte sottolinea come «l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 non esige che il trattamento di dati personali in questione venga effettuato 'dallo' stesso stabilimento interessato, bensì soltanto che venga effettuato 'nel contesto delle attività' di quest'ultimo"[26] e quindi che consenta «l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile del trattamento di tali dati è registrato, purché il medesimo svolga, tramite un'organizzazione stabile nel territorio di tale Stato membro, un'attività effettiva e reale, anche minima, nel contesto della quale si

[25] P. Piroddi, op. cit., p. 647, evidenzia che la Corte inverte totalmente i termini della questione. È l'attività commerciale di vendita di pubblicità che è effettuata nel cotesto delle attività del motore di ricerca e non viceversa.
[26] Così il punto 52 della sentenza *Google Spain*.

svolge tale trattamento».

In *Weltimmo* la sentenza *Google Spain* è espressamente richiamata, affermandosi che «l'espressione 'nel contesto delle attività di uno stabilimento' non può ricevere un'interpretazione restrittiva» e che «il legislatore dell'Unione ha quindi previsto un ambito di applicazione territoriale della direttiva 95/46 particolarmente esteso, che ha inserito all'articolo 4 della stessa» [27].

Un espresso invito all'interpretazione flessibile della nozione di stabilimento è formulato dall'avvocato generale in *Weltimmo* [28] e ripreso dalla Corte che si pronuncia per «una concezione flessibile della nozione di stabilimento, che si discosta dall'impostazione formalistica secondo cui un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata. Infatti, per determinare se una società, responsabile di un trattamento dei dati, dispone di uno stabilimento, ai sensi della direttiva 95/46, in uno Stato membro diverso dallo Stato membro o dal paese terzo in cui è registrata, occorre valutare sia il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività in tale altro Stato membro, prendendo in considerazione la natura specifica delle attività economiche e delle prestazioni di servizi in questione. Ciò vale soprattutto per imprese che offrono servizi esclusivamente tramite Internet.

A questo proposito, occorre segnatamente considerare, alla luce dell'obiettivo perseguito da tale direttiva, consistente nel garantire una tutela efficace e completa del diritto alla vita privata e nell'evitare che le disposizioni vengano eluse, che la presenza di un unico rappresentante, in talune circostanze, può essere sufficiente a costituire un'organizzazione stabile se il medesimo opera con un grado di stabilità sufficiente con l'ausilio dei mezzi necessari per la fornitura dei servizi concreti di cui trattasi nello Stato membro in questione.

[27] Così i punti 25 e 27 della sentenza *Weltimmo.*

[28] Così nel punto 28 delle conclusioni: «Ciò detto, occorre fare riferimento al considerando 19 della direttiva 95/46, che costituisce un elemento di interpretazione fondamentale per determinare il contenuto della nozione di stabilimento ai sensi della medesima direttiva. Detto considerando suggerisce una concezione flessibile della nozione in parola, che si discosta dall'impostazione formalistica secondo cui un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata. Infatti, in primo luogo, detto considerando comprende un criterio di effettività e un elemento di stabilità laddove enuncia che "lo stabilimento nel territorio di uno Stato membro implica l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile […]". In secondo luogo, esso offre una notevole flessibilità disponendo che 'la forma giuridica di siffatto stabilimento, si tratti di una semplice succursale o di una filiale dotata di personalità giuridica, non è il fattore determinante a questo riguardo».

Inoltre, per realizzare detto obiettivo, occorre considerare che la nozione di 'stabilimento', ai sensi della direttiva 95/46, si estende a qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione stabile» [29]. E l'avvocato generale giunge a sostenere che sia sufficiente «un operatore con una presenza duratura, dotato di poco più di un computer portatile» [30]. Richiama, quindi, le interpretazioni della nozione di stabilimento formulate in altri settori del diritto europeo[31] e sottolinea, come già nelle conclusioni dell'avvocato generale nel caso *Google*, la necessità di valutare la particolarità delle attività economiche esercitate tramite Internet[32]. Come argomenta l'avvocato generale, questa valutazione è stata già effettuata nella direttiva sul commercio elettronico ove si enuncia al considerando 19 che «[…] [i]l luogo di stabilimento, per le società che forniscono servizi tramite siti Internet, non è là dove si trova la tecnologia di supporto del sito né là dove esso è accessibile, bensì il luogo in cui tali società esercitano la loro attività economica» e tale definizione è stata ritenuta pertinente dal Gruppo articolo 29[33] al fine di interpretare l'articolo 4 della direttiva 95/46/CE[34].

In questo stesso senso, occorre ricordare, si esprime anche il *Model*

[29] Punti 29, 30 e 31 della sentenza Weltimmo.

[30] Punto 34 delle conclusioni dell'avvocato generale nella sentenza *Weltimmo*.

[31] Punto 29. Siffatta concezione della nozione di stabilimento è in linea con l'interpretazione che tale nozione ha ricevuto nella giurisprudenza della Corte in altri settori del diritto dell'Unione. In particolare, secondo costante giurisprudenza, «la nozione di stabilimento di cui alle disposizioni del Trattato relative alla libertà di stabilimento implica l'esercizio effettivo di un'attività economica per una durata di tempo indeterminata, mercé l'insediamento in pianta stabile in un altro Stato membro», il che «presuppone […] un insediamento effettivo della società interessata nello Stato membro ospite e l'esercizio quivi di un'attività economica reale». Punto 30. Inoltre, il parere n. 8/2010 del Gruppo articolo 29 fa riferimento all'interpretazione della nozione di stabilimento in quanto criterio di collegamento ai fini fiscali in materia di IVA. La giurisprudenza della Corte in tale materia risulta particolarmente interessante – giacché la nozione di stabilimento opera come criterio di collegamento per determinare l'assoggettamento a una normativa tributaria nazionale – e approfondisce la nozione di stabile organizzazione, che «[…] dev'essere caratterizzata da un sufficiente grado di permanenza e da una struttura adeguata, in termini di risorse umane e tecniche, che le consentano di ricevere ed utilizzare i servizi fornitile per le specifiche esigenze delle organizzazioni medesime». Inoltre, la nozione di stabilimento presente sia nell'ambito della Convenzione di Roma che in quello della Convenzione di Bruxelles milita parimenti a favore di una concezione non formalistica.

[32] Punto 34 delle conclusioni dell'avvocato generale nella sentenza Weltimmo.

[33] Gruppo art. 29, Parere n. 8/2010 sul diritto applicabile, adottato il 16 dicembre 2010, 0836-02/10/IT, WP 179.

[34] Punto 35 delle conclusioni dell'avvocato generale nella sentenza Weltimmo.

Law sul commercio elettronico dell'Uncitral[35].

La Corte ritiene, invece, inconferente la questione della cittadinanza delle persone interessate da tale trattamento, così come il luogo in cui sono stati caricati i dati, lo Stato membro al quale sono rivolti i servizi, la nazionalità degli interessati o il luogo in cui risiedono i titolari dell'impresa[36] .

In tal senso si pronuncia anche il Gruppo articolo 29, secondo cui «[n]on sono decisivi [al fine di determinare il diritto applicabile] la cittadinanza o il luogo di residenza abituale dell'interessato né l'ubicazione fisica dei dati personali»[37].

In *Google Spain* si evidenzia specificamente la connessione fra attività di soggetti differenti volte al perseguimento di un unico scopo e quindi funzionali, «inscindibilmente connesse» secondo la Corte ad individuare un'unica nozione di 'contesto'. Afferma la Corte: «le attività del gestore del motore di ricerca e quelle del suo stabilimento situato nello Stato membro interessato sono inscindibilmente connesse, dal momento che le attività relative agli spazi pubblicitari costituiscono il mezzo per rendere il motore di ricerca in questione economicamente redditizio e che tale motore è, al tempo stesso, lo strumento che consente lo svolgimento di dette attività»[38].

La Corte può così concludere che «l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 deve essere interpretato nel senso che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai sensi della disposizione suddetta, 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».

Non diversamente su questo punto aveva argomentato l'avvocato generale, sottolineando come fosse necessario muovere dalla considerazione del modello economico dei fornitori di servizi di motore di ricerca su Internet[39].

[35] Così anche l'*UNCITRAL Model Law on Electronic Commerce*, art. 15 e il commento nella *Guide to Enactment*, par. 105 ss. In argomento v. L.G. Castellani, *I testi dell'Uncitral in materia di diritto del commercio elettronico*, in G. Finocchiaro-F. Delfini, *Diritto dell'informatica*, Utet, 2014, p. 43 ss. e G. Finocchiaro, *Il ruolo dell'Uncitral nello sviluppo della disciplina sul commercio elettronico*, *ibidem*, p. 63 ss.

[36] Così il punto 37 delle conclusioni dell'avvocato generale in *Weltimmo*.

[37] Parere n. 8/2010, pag. 10. V. anche le conclusioni dell'avvocato generale Jääskinen nella causa *Google Spain.*

[38] Così il punto 56 della sentenza Google Spain.

[39] Punto 64 e ss. delle conclusioni dell'avvocato generale. In particolare al punto 65:

L'interpretazione della Corte anticipa, quanto agli effetti, l'emanando regolamento europeo[40]. Secondo il testo della proposta di regolamento emendato attualmente disponibile, reso dal Consiglio dell'Unione Europea l'11 giugno 2015 (9565/15), il controverso art. 3 intitolato «Campo di applicazione territoriale» nella versione odierna dispone come segue: «Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o di un incaricato del trattamento nell'Unione.

Il presente regolamento si applica al trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

a) l'offerta di beni o la prestazione di servizi ai suddetti residenti nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure

b) il controllo del loro comportamento, quest'ultimo inteso all'interno dell'Unione europea. […]»[41].

«dev'essere tenuto in considerazione il modello economico di un fornitore di servizi di motore di ricerca su Internet nel senso che il suo stabilimento ha un ruolo significativo nel trattamento dei dati personali se è collegato ad un servizio implicato nella vendita di pubblicità mirata agli abitanti di tale Stato membro». E al punto 67: «il trattamento di dati personali avviene nell'ambito di uno stabilimento del responsabile del trattamento se tale stabilimento funge da collegamento per il servizio di posizionamento per il mercato pubblicitario di tale Stato membro, anche se le operazioni tecniche di trattamento dei dati hanno luogo in altri Stati membri o in paesi terzi».

[40] In particolare sull'art. 3 della proposta di regolamento v. W. Kotschy, The proposal for a new General Data Protection Regulation—problems solved?, in International Data Privacy Law 2014, Vol. 4, No. 4, pp. 274-281.

[41] I considerando 20 e 21 aggiungono sul punto quanto segue.«20) Onde evitare che una persona fisica venga privata della tutela cui ha diritto in base al presente regolamento, è necessario che questo disciplini anche il trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento non stabilito nell'Unione, quando le attività di trattamento sono legate all'offerta di beni o servizi a dette persone indipendentemente dal fatto che vi sia un pagamento o no all'interno dell'Unione. Per determinare se tale responsabile del trattamento stia offrendo beni o servizi a dette persone nell'Unione, occorre verificare se risulta che il responsabile del trattamento intenda concludere affari con residenti in uno o più Stati membri dell'Unione. Se la semplice accessibilità del sito Internet del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica, di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il responsabile del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, e/o la menzione di clienti o utenti residenti nell'Unione, possono evidenziare l'intenzione del responsabile del trattamento volta all'offerta di beni o servizi a dette persone nell'Unione. 21) È opportuno che anche il trattamento dei

Nell'art. 3 dell'emanando regolamento si accentua la tendenza espansiva del diritto dell'Unione passando per l'individuazione di molteplici criteri di collegamento: quello territoriale (il luogo in cui viene effettuato il trattamento), ma assai estensivamente e poco chiaramente dilatato fino a comprendere l'ambiguo riferimento all'ambito delle attività' addirittura 'dell'incaricato'; quello teleologico (protezione dei residenti europei); quello che ha riguardo all'oggetto (fornitura dei servizi resi anche gratuitamente, così da ricomprendere, fra l'altro, i motori di ricerca); quello che ha riguardo agli effetti del trattamento (controllo del comportamento). Una pluralità di criteri, disomogenei e non chiaramente formulati, così da attrarre in ogni caso nell'ambito di applicazione della normativa europea i trattamenti anche all'estero effettuati.

3. Ulteriori indicazioni interpretative

Le decisioni della Corte passate in rassegna consentono di trarre alcune ulteriori indicazioni interpretative emergenti e inducono a riflettere su alcune conseguenze.

3.1 La pluralità di leggi nazionali applicabili

Nelle more dell'approvazione e dell'entrata in vigore del regolamento europeo, le decisioni della Corte conducono all'applicazione di una pluralità di leggi nazionali[42], conseguenza che si sarebbe voluta scongiurare nella prima versione della direttiva[43].

Addirittura si considera 'elusivo' il comportamento volto ad applicare la legislazione di un solo Stato membro, ovviamente attuativa della diretti-

dati personali di residenti nell'Unione ad opera di un responsabile del trattamento non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al controllo del loro comportamento all'interno dell'Unione. Per stabilire se un'attività di trattamento sia assimilabile al 'controllo del comportamento' dell'interessato, occorre verificare se le operazioni che questi esegue su Internet sono sottoposte a tecniche di trattamento dei dati volte alla profilazione dell'utente, in particolare per prendere decisioni che li riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali».

[42] Lo ricorda l'avvocato generale nelle conclusioni relative al caso *Weltimmo*, punto 63, evidenziando una distanza considerevole fra le legislazioni degli Stati membri con riguardo alla regolamentazione e ai poteri sanzionatori delle autorità di controllo.

[43] Così ricorda L. Moerel, *Back to basics: when does EU data protection law apply?,* cit.

va[44]. Questo argomento è supportato dal considerando 19 della direttiva, il quale dispone che «quando un unico responsabile del trattamento è stabilito nel territorio di diversi Stati membri, in particolare per mezzo di filiali, esso deve assicurare, segnatamente per evitare che le disposizioni vengano eluse, che ognuno degli stabilimenti adempia gli obblighi previsti dalla legge nazionale applicabile alle attività di ciascuno di essi», dimostrando così palesemente quanta scarsa fiducia il legislatore europeo riponga in se stesso.

L'azione della Corte di giustizia rende più forte il diritto nazionale, in taluni casi a scapito della Commissione, come risulta evidente in *Schrems*, ove la Corte decide che spetti all'autorità irlandese decidere se occorre sospendere il trasferimento dei dati degli iscritti a Facebook verso gli Stati Uniti, sulla base dell'interpretazione dell'art. 8 della Carta dei diritti fondamentali ove è esplicito il riferimento all'autorità nazionale di controllo, ritenendo che le autorità nazionali di controllo possano *effettuare le proprie valutazioni anche quando vi sia già una decisione della Commissione.*

3.2 Distinzione fra 'dato personale' e 'valutazione'. Definizione di 'trattamento'

Ulteriori indicazioni interpretative vengono dalle decisioni in rassegna. In primo luogo, ancora alcuni chiarimenti sulla nozione di 'dato personale'.

La decisione del 17 luglio 2014, causa C-141/12, *Y.S. e a.* ha ad oggetto l'interpretazione degli articoli 2, lettera a), 12, lettera a), e 13, paragrafo 1, lettere d), f) e g), della direttiva 95/46/CE nonché degli articoli 8, paragrafo 2, e 41, paragrafo 2, lettera b), della Carta dei diritti fondamentali dell'Unione europea. Tale sentenza ha origine da due distinte domande pregiudiziali, poi riunite. In entrambi i casi, i cittadini di un paese terzo che hanno presentato una domanda di permesso di soggiorno temporaneo nei Paesi Bassi, contestano il rifiuto da parte del Ministero di trasmettere a detti cittadini copia di un documento amministrativo concernente le loro domande di permesso di soggiorno.

La Corte distingue fra dati personali e valutazioni effettuate nell'ambito di un procedimento amministrativo, in relazione alle quali non possono essere esercitati i diritti di accesso, rettifica e controllo previsti dalla direttiva sulla protezione dei dati personali. In particolare, stabilisce che l'articolo 2, lettera a), della direttiva 95/46/CE, dev'essere interpretato nel senso che i dati relativi al richiedente un titolo di soggiorno che compaio-

[44] Così la decisione *Weltimmo*, punti 28 e 30.

no in un documento amministrativo in cui viene esposta la motivazione addotta dal funzionario a sostegno della bozza di decisione che egli è incaricato di redigere nell'ambito del procedimento precedente all'adozione di una decisione relativa alla domanda e, eventualmente, i dati che figurano nell'analisi giuridica contenuta nel documento medesimo costituiscono dati personali ai sensi di tale disposizione, mentre detta analisi non può invece ricevere, di per sé, la stessa qualificazione. Infatti, l'analisi giuridica costituisce non già un'informazione riguardante il richiedente il titolo di soggiorno, ma tutt'al più, un'informazione riguardante la valutazione e l'applicazione, da parte dell'autorità competente, di tale diritto alla situazione del richiedente. Di conseguenza, contrariamente ai dati relativi al richiedente il titolo di soggiorno, l'analisi non può, di per sé, formare oggetto di una verifica della sua esattezza da parte di detto richiedente né di una rettifica ai sensi dell'articolo 12, lettera b), della direttiva 95/46/CE. Ciò considerato, il fatto di estendere il diritto di accesso del richiedente il titolo di soggiorno a detta analisi giuridica asseconderebbe, in realtà, non già l'obiettivo di tale direttiva consistente nel garantire la tutela del diritto alla vita privata del richiedente con riferimento al trattamento dei dati che lo riguardano, bensì quello di garantirgli un diritto di accesso ai documenti amministrativi, diritto che non forma tuttavia oggetto della direttiva 95/46/CE.

Si ribadisce, inoltre, una interpretazione estensiva della nozione di 'trattamento' in *Weltimmo,* confermando che va considerata 'trattamento'l'operazione consistente nel far comparire su una pagina Internet dati personali, come già in precedenza affermato dalla Corte di giustizia, *in primis* nel caso *Lindqvist* [45].

3.3 Bilanciamento fra il diritto all'accesso ai documenti amministrativi e il diritto alla protezione dei dati personali

Un'ulteriore tematica affrontata dalla Corte di giustizia in due delle sentenze sopra riportate (*Strack / Commissione* e *ClientEarth e PAN Europe / EFSA)*, concerne in particolare il bilanciamento fra il diritto all'accesso ai documenti amministrativi e il diritto alla protezione dei dati personali.

Costituiscono, infatti, oggetto della decisione le condizioni per il trasferimento di dati personali a norma dell'art. 8 del 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

[45] Così il punto 37 della sentenza *Weltimmo*.

dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati.

In questi casi, l'accesso ai documenti era stato accordato, ma oscurando alcuni dati personali. In particolare, nella seconda delle decisioni citate, erano stati oscurati i nominativi degli esperti che avevano formulato alcune osservazioni.

La Corte, in entrambe le sentenze, ricorda che ai sensi dell'articolo 8, lettera b), del regolamento n. 45/2001/CE, i dati personali possono, di norma, essere trasferiti soltanto se il destinatario dimostra la necessità della loro trasmissione e se non sussistono ragioni per presumere che possano subire pregiudizio interessi legittimi degli interessati.

Dalla stessa formulazione di tale disposizione emerge che essa subordina il trasferimento di dati personali al ricorrere di due condizioni cumulative. In tale contesto, incombe anzitutto a colui che chiede il trasferimento dimostrarne la necessità. Se la dimostra, spetta allora all'istituzione interessata verificare se non sussistano ragioni per presumere che il trasferimento in questione possa pregiudicare gli interessi legittimi dell'interessato. In assenza di ragioni di tale sorta, occorre procedere al trasferimento richiesto, mentre, nel caso contrario, l'istituzione interessata deve effettuare un bilanciamento tra i diversi interessi in gioco per pronunciarsi sulla domanda di accesso.

Tuttavia non può, in generale, riconoscersi alcuna automatica prevalenza dell'obiettivo di trasparenza sul diritto alla protezione dei dati personali. Rimane in capo alle parti richiedenti il trasferimento di dati personali l'onere di provare puntualmente e concretamente tale necessità. Allo stesso modo l'autorità interessata è tenuta a valutare se la divulgazione richiesta possa ledere concretamente ed effettivamente l'interesse protetto.

Ogni valutazione deve essere quindi effettuata caso per caso.

Sul bilanciamento fra diritti contrapposti si segnala anche la decisione del 16 luglio 2015, causa C-580/13, *Coty Germany*.

La domanda di pronuncia pregiudiziale verte sull'interpretazione dell'articolo 8, paragrafo 3, lettera e), della direttiva 2004/48/CE del Parlamento europeo e del Consiglio, del 29 aprile 2004, sul rispetto dei diritti di proprietà intellettuale.

La domanda è stata presentata nell'ambito di una controversia tra la Coty Germany GmbH (in prosieguo: la «Coty Germany»), una società titolare di diritti di proprietà intellettuale, e la Stadtsparkasse Magdeburg, un istituto di credito, in merito al rifiuto di quest'ultima di fornire alla Coty Germany informazioni relative ad un conto bancario.

La Corte rileva che una disposizione del diritto nazionale che consenta un rifiuto di fornire dati personali in maniera illimitata, non contemplando alcuna condizione né precisazione è idonea a violare il diritto fondamentale di proprietà intellettuale e non rispetta, pertanto, l'esigenza di assicurare un giusto equilibrio tra i diversi diritti fondamentali controbilanciati dall'articolo 8 della direttiva 2004/48/CE, cioè diritto di proprietà intellettuale, da un lato, e diritto alla tutela dei dati personali, dall'altro.

Ne consegue che l'articolo 8, paragrafo 3, lettera e), della direttiva 2004/48/CE del Parlamento europeo e del Consiglio, del 29 aprile 2004, sul rispetto dei diritti di proprietà intellettuale, deve essere interpretato nel senso che esso osta ad una disposizione nazionale che consenta, in maniera illimitata ed incondizionata, ad un istituto bancario di opporre il segreto bancario per rifiutarsi di fornire, nell'ambito dell'articolo 8, paragrafo 1, lettera c), della medesima direttiva, informazioni relative al nome e all'indirizzo del titolare di un conto.

3.4 Trattamento dei dati personali da parte di un'autorità amministrativa. Obbligo di informativa

La decisione del 1° ottobre 2015, causa C-201/14, *Bara e a.*, concerne ancora il trattamento dei dati personali da parte di un'autorità amministrativa. Ivi si precisa che anche nel caso di comunicazione dei dati personali da un'amministrazione pubblica ad un'altra amministrazione pubblica, l'interessato deve essere informato. In particolare, gli articoli 10, 11 e 13 della direttiva 95/46/CE devono essere interpretati nel senso che essi ostano a misure nazionali che consentono a un'amministrazione pubblica di uno Stato membro di trasmettere dati personali a un'altra amministrazione pubblica, a fini di trattamento, senza che le persone interessate siano state informate né di tale trasmissione né del successivo trattamento.

3.5 Elementi biometrici dei passaporti e dei documenti di viaggio

Infine, nella decisione della Corte di giustizia del 16 aprile 2015, cause riunite da C-446/12 a C-449/12, *Willelms e a.*, le domande di pronuncia pregiudiziale vertono sull'interpretazione degli articoli 1, paragrafo 3, e 4, paragrafo 3, del 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, come modificato dal regolamento (CE) n. 444/2009 del Parlamento europeo e del Consiglio, del 6 maggio 2009, in particolare in merito al rifiuto da parte della amministrazione olandese di rilasciare ai ricorrenti un passaporto (C-446/12, C-448/12 e C-449/12) e una carta d'identità (C-447/12) se non sono rilevati contestualmente i loro dati biometrici.

In materia di trattamento dei dati biometrici dei passaporti e dei documenti di viaggio, nella sentenza *Schwarz* (C-291/12, EU:C:2013:670) la Corte aveva già dichiarato che l'uso e la conservazione dei dati biometrici ai fini precisati all'articolo 4, paragrafo 3, del regolamento (CE) n. 2252/2004 sono conformi ai requisiti di cui agli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

Nel caso di specie la Corte chiarisce che suddetto regolamento non è applicabile alle carte d'identità rilasciate da uno Stato membro ai propri cittadini, come le carte d'identità dei Paesi Bassi, e ciò indipendentemente tanto dalla durata della loro validità quanto dalla possibilità di utilizzarle nel corso di viaggi effettuati al di fuori di tale Stato.

Conclusioni

Come si è anticipato, nelle decisioni della Corte di giustizia da *Google* a *Schrems* si legge chiaramente l'importanza strategica della protezione dei dati personali e la volontà di affermare la competenza della Corte ed il modello europeo. Questo fenomeno non sorprende ed anzi è nella natura delle cose che ogni giudice tenda ad affermare la propria competenza. Il tema che si affronta è cruciale anche con riguardo alla legge applicabile e alla giurisdizione su Internet più in generale, ancora non risolto, non essendo individuabile un soggetto politico legittimato a emanare le regole a livello globale[46].

L'attenzione della Corte è concentrata proprio sul diritto alla protezione dei dati personali su Internet e il diritto alla protezione della vita privata appare quasi una citazione di stile, l'inevitabile elemento di un'endiadi che tuttavia non suscita una particolare autonoma attenzione.

Non appare tanto la vita privata il bene che si vuole proteggere, quanto piuttosto le informazioni, e più o meno consapevolmente, il valore

[46] Sull'argomento si rinvia U. Draetta, *Internet nel diritto internazionale*, in G. Finocchiaro-F. Delfini, *op.cit.,* p. 3 ss. e a G. Finocchiaro, *Lex mercatoria e commercio elettronico*, in *Diritto di internet*, Zanichelli, 2008, p. 1.

economico ad esse connesso. Il diritto alla protezione dei dati personali è talmente pervasivo da superare agevolmente i confini della vita privata in senso stretto e da approdare nel minaccioso territorio della diffusione delle informazioni su Internet.

In effetti, la partita realmente aperta è proprio quella sulla *governance* di Internet[47].

L'azione politica della Corte di giustizia potrà forse condurre all'affermazione del modello europeo sulla protezione dei dati personali, ma ciò dovrebbe indurre ad una seria riflessione proprio su questo modello.

Esso, infatti, non soddisfa sotto molti aspetti e necessiterebbe di una revisione radicale, ben più ampia di quella contenuta nella proposta di regolamento. Tale modello attualmente si presta, infatti, ad un'applicazione meramente formalistica e poco sostanziale che facilmente si riduce ad un modulo di informativa e alla prestazione di un consenso vuoto e ineffettivo. Manca un'adeguata attenzione sulla sicurezza dei dati, incentrata sui dati e non sull'interessato, il quale spesso è debole sotto ogni profilo: culturale, economico, tecnologico e soprattutto di consapevolezza. Manca un'analisi di tipo economico sul modello che si adotta: non soltanto dal punto di vista del titolare del trattamento ma anche dal punto di vista del mercato europeo. Mentre imprese come Google o Facebook potranno facilmente adattarsi ad un più severo (e costoso) diritto europeo, non è chiaro quanto questo graverà sulle imprese europee.

Troppo poco spazio è lasciato al bilanciamento del diritto alla protezione dei dati personali con altri diritti pure costituzionalmente garantiti, quali il diritto alla libertà di espressione, il diritto di accesso ad Internet e la libertà di impresa. Mentre affermare il diritto alla protezione della vita privata può corrispondere ai valori e alla cultura europei, così come affermare il diritto all'identità personale, il diritto alla protezione dei dati personali in sé considerato (e privato del collegamento spesso solo retoricamente operato con la protezione della vita privata) è talmente ampio e pervasivo da rischiare di divenire poco comprensibile.

Ergere un muro intorno all'Europa, poi, può significare proteggerla, ma anche isolarla dal resto del mondo con l'effetto, già descritto da molti, della balcanizzazione di Internet.

Sono temi politici, appunto, che richiederebbero un altro e diverso tavolo di discussione.

[47] Su questo punto, in maniera chiara ed incisiva, F. Pizzetti, *Le Autorità Garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain. È tempo di far cadere il 'velo di Maya'*, in *Dir. Inf.* 2014, p. 805 ss.

Abstract

The paper summarizes the ECJs decisions on personal data protection, from Google Spain to Schrems.

It points out the main issues touched by these decisions focusing in particular, on the relevance of the rights to privacy and to protection of personal data as fundamental rights and on the applicable law.

What emerges from the analysis of the argumentative path followed by the Court on these issues is the intention to extend the scope of the European data protection law beyond European borders.

The paper draws a special attention to the political role assumed by the ECJ in this context in promoting the European model.