RIVISTA ITALIANA DI DIRITTO PUBBLICO COMUNITARIO
ISSN 1121-404X
Anno XXV Fasc. 3-4 - 2015

Serena Crespi

DIRITTI FONDAMENTALI, CORTE DI GIUSTIZIA E RIFORMA DEL SISTEMA UE DI PROTEZIONE DEI DATI

Estratto

MVLTA PAVCIS AG

Milano • Giuffrè Editore

SERENA CRESPI

DIRITTI FONDAMENTALI, CORTE DI GIUSTIZIA E RIFORMA DEL SISTEMA UE DI PROTEZIONE DEI DATI

The protection of personal data is currently at the center of the EU legislative action: identified as a political priority by the Juncker Commission, it is the object of an ongoing comprehensive reform. The article addresses the question of the balancing between, on the one hand, the fundamental right to data protection and, on the other hand, other fundamental rights and public interests, with particular reference to the recent case law of the European Court of Justice. It follows from the most recent jurisprudence (Google Spain, Digital Rights Ireland) that the protection of personal data may prevail over other rights an interests and that any exception to that fundamental right has to be duly justified and subject to a number of clear and specific safeguards. Finally, the article examines the implication of the case law on pending legislative proposals and on international agreements concluded or being negotiated by the European Union.

1. *L'importanza del diritto fondamentale alla protezione dei dati personali nel sistema dell'Unione europea.*

Come è noto, il trattato di Lisbona ha rafforzato la tutela dei diritti fondamentali all'interno del sistema europeo. Ai sensi dell'articolo 6.1 TUE, la Carta UE dei diritti fondamentali e i diritti ivi

menzionati hanno assunto rango primario nel panorama delle fonti europee. Anche per effetto del maggiore valore giuridico attribuito a questi ultimi, a partire dal 1 dicembre 2009 tutte le istituzioni, gli organi e gli organismi UE, nonché gli Stati membri sono ora formalmente obbligati in virtù di una norma di diritto primario a garantire il rispetto dei diritti fondamentali nell'esercizio delle funzioni loro attribuite dai trattati (1). In tale contesto, un ruolo di centrale importanza è svolto dalla Corte di giustizia, prevedendo tra l'altro l'articolo 47 della Carta che ogni persona i cui diritti e le cui libertà essa pretenda essere stati violati ha il diritto a un ricorso effettivo davanti ai giudici anche UE (2). In particolare, nonostante già prima della riforma di Lisbona questi ultimi abbiano garantito una penetrante tutela dei diritti fondamentali dei cittadini europei avverso le iniziative delle istituzioni europee, degli Stati e anche del paese di cittadinanza (3), la nuova architettura UE, sempre più imperniata sulla protezione di tali diritti, ha, in altri termini, assegnato alla Corte il ruolo (e la responsabilità) di giudice dei diritti fondamentali (4), il quale andrà peraltro meglio definito per effetto dell'adesione dell'Unione alla CEDU prevista all'articolo 6.2 TUE e ormai a uno stadio piuttosto avanzato, pur se il recente parere della Corte di giustizia sembra dover indurre a una nuova riflessione in merito (5).

Questa (parzialmente) nuova funzione dei giudici di Lussemburgo, la quale è e sarà esercitata principalmente in giudizi di cui agli articoli 256, 263 e 267 TFUE, richiederà allora ancor di più rispetto al passato la ponderazione dei diversi diritti coinvolti al fine di stabilirne, caso per caso, la prevalenza di uno sull'altro. I diritti

---

(1) Così i rapporti della Commissione europea del 30 marzo 2011 e del 16 aprile 2012 sull'applicazione della Carta, COM(2011)160 e COM(2012) 169.

(2) Per un approfondimento di questi aspetti G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer International Publishing, 2014; S. Carrera, M. De Somer, B. Petkova, *The Court of Justice of the European Union as a Fundamental Rights Tribunal Challenges for the Effective Delivery of Fundamental Rights in the Area of Freedom, Security and Justice*, paper 49, agosto 2012.

(3) In merito diffusamente A. Tizzano, *Qualche riflessione sul contributo della Corte di giustizia allo sviluppo del sistema comunitario*, in S. Bariatti, G. Venturini (a cura di), *Nuovi strumenti di diritto internazionale privato.* Liber *Fausto Pocar*, Milano, 2009, p. 925 ss., spec. p. 940 ss.

(4) Così espressamente H. Labayle, *La Cour de justice et la protection des données: quand le juge européen des droits fondamentaux prend ses responsabilités*, reperibile su www.gdr-elsj.eu del 9 aprile 2014. In tal senso anche J.P. Jacqué, *Protection des données personnelles, Internet et conflits entre droits fondamentaux devant la Cour de justice*, in *Rev. trim. dr. europ*., 2014, p. 283 ss.

(5) Sull'adesione della UE alla CEDU, v. però il parere negativo della Corte di giustizia 2/13 del 18 dicembre 2014, reperibile sul sito curia.europa.eu.

fondamentali UE, al pari peraltro di quelli CEDU, possono in effetti soggiacere a restrizioni, le quali, ai sensi dell'articolo 52.1 della Carta, devono essere previste dalla legge, proporzionate, necessarie, nonché devono rispettare il contenuto essenziale di detti diritti e libertà e rispondere a finalità d'interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. E in effetti l'analisi della giurisprudenza comune anche antecedente il trattato di Lisbona mostra come i giudici di Lussemburgo non abbiano esitato a condizionare l'esercizio anche delle libertà di circolazione, pietra angolare del sistema comune, all'applicazione di altri principi UE fondamentali relativi all'individuo (6).

Un recente esempio di contemperamento tra diritti fondamentali può essere tratto dalla giurisprudenza comune in materia di protezione dei dati personali, la quale ha avuto un notevole impulso nel 2014. Nonostante in effetti non manchino in tale ambito interventi del giudice di Lussemburgo anche risalenti (7), nell'ultimo anno esso è stato ripetutamente chiamato a pronunciarsi sul valore del diritto dei privati alla protezione dei dati personali (sentenze *Google Spagna* (8) e *Digital Rights Irland Ltd* (9)) quando in concorso con altri diritti fondamentali (d'autore, iniziativa economica, libertà d'informazione e d'espressione, pubblica sicurezza), nonché nei rapporti tanto tra persone fisiche e giuridiche quanto tra cittadini e autorità pubbliche. La maggior attenzione del giudice UE alla protezione dei dati è invero comprensibile dato che, da un lato, l'uso sempre più frequente di Internet per comunicare, avere accesso e scambiare informazioni, nonché offrire e acquistare beni o servizi ha esposto la vita privata degli individui a nuovi e maggiori rischi, i quali sono solo accennati nella direttiva 46 risalente al 1995 (10). Dall'altro lato, la protezione dei dati è ora espressamente menzionata nel diritto primario e in particolare nella Carta quale diritto fondamentale (articolo 8.2) peraltro autonomo rispetto al diritto alla vita privata e familiare di cui all'articolo 7. La Carta si differenzia allora dalla CEDU, la quale tutela invece la protezione dei dati come parte

(6) Tra i tanti esempi Corte di giustizia UE 26 giugno 1997, C-368/95, *Vereinigte Familiapres Zeitungsverlags und vertriebs GmbH v Heinrich Bauer Verlag*, punto 18; 12 giugno 2003, C-112/00, *Schmidberger*; 14 ottobre 2004, C-36/02, *Omega*, punto 35; 14 febbraio 2008, C-244/06, *Dynamic Medien Vertriebs GmbH*, punto 42.

(7) Corte di giustizia UE 6 novembre 2003, C-101/01, *Lindqvist*.

(8) Corte di giustizia UE 13 maggio 2014, C-131/12.

(9) Corte di giustizia UE 8 aprile 2014, C-293/12 e C-594/12.

(10) *GUCE* L 281 del 1995.

del più ampio diritto al rispetto della vita privata e familiare (articolo 8).

Inoltre, a differenza di molti altri diritti fondamentali UE di cui alla Carta, la protezione dei dati personali figura anche all'articolo 16 TFUE, il quale attribuisce al legislatore europeo competenza concorrente con gli Stati ad adottare, secondo la procedura ordinaria, le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché quelle connesse alla libera circolazione di tali dati (11). La tutela della protezione dei dati nella UE non è, in altri termini, lasciata alla sola azione di controllo negativo della Corte di giustizia ma anche a quella positiva del legislatore UE, attraverso la costruzione di un quadro normativo di protezione completo e adeguato alle nuove esigenze del sistema internazionale. E in effetti su questa base giuridica l'esecutivo europeo, affermando proprio l'esigenza di modernizzare gli attuali atti in materia alla luce dei rapidi sviluppi tecnologici e della globalizzazione, ha proposto nel 2012 un pacchetto di riforme consistente in una proposta di regolamento sulla protezione dei dati destinata a sostituire la già citata direttiva 95/46 (12), e in una direttiva sulla protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale, la quale sostituirà la decisione quadro 2008/977/GAI (13). Il pacchetto è attualmente al vaglio del Consiglio, mentre il Parlamento europeo ha già nel marzo 2014 adottato in prima lettura, con una larga maggioranza, la sua posizione sulla proposta della Commissione, confermandone i principali elementi. Inoltre il Consiglio europeo ha più volte posto l'accento sull'importanza di assicurare l'adozione della riforma entro il 2015, anche in quanto essa rappresenta un elemento essenziale del mercato unico digitale.

L'importanza ormai incontestabile del diritto di tutela dei dati personali nel sistema dell'Unione, testimoniata anche dal fatto che la riforma del quadro legislativo è stata posta tra le priorità della nuova

---

(11) In generale su tali aspetti B. Cortese, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Dir. Un. eur.*, 2013, n. 2.

(12) COM(2012)11 del 25 gennaio 2012. In merito, v. anche la Comunicazione della Commissione europea COM(2010)609.

(13) COM(2012)10 del 25 gennaio 2012. La decisione quadro 2008/977/GAI del 27 novembre 2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale è pubblicata in *GUUE* L 350 del 30 dicembre 2008.

Commissione europea presieduta da Juncker (14), nonché le nuove sfide di contemperarlo con altri diritti parimenti rilevanti rende allora necessaria l'analisi della più recente giurisprudenza UE in materia al fine di valutarne i risultati interpretativi e il loro impatto non solo sulla riforma del sistema comune in materia di protezione dei dati personali, ma anche sulla questione, divenuta particolarmente sensibile a seguito del c.d. *datagate*, degli scambi internazionali di dati personali (segnatamente con gli Stati Uniti).

2. *La sentenza* Google Spagna *e la tutela dei dati personali nei rapporti orizzontali.*

Nella sentenza *Google Spagna* la Corte è stata chiamata innanzitutto a contemperare il diritto dei cittadini UE alla protezione della vita privata con l'interesse economico sotteso all'attività di *Google*, nonché con la libertà d'ottenere o di comunicare informazioni in particolare sulla rete (15). La questione, posta prima davanti all'autorità spagnola della protezione dei dati, poi all'*Audienca National* e in ultimo alla Corte UE in via pregiudiziale, era quella di stabilire se un individuo potesse invocare il diritto alla protezione dei dati per ottenere la soppressione da internet d'informazioni relative alla propria persona, peraltro veritiere e legittimamente pubblicate molti anni prima da terzi su un quotidiano, in quanto ne ritenesse la diffusione pregiudizievole. In effetti, allorché un utente di internet introduceva il nome del sig. Gonzalez, cittadino spagnolo residente in Spagna, nel motore di ricerca *Google Search*, otteneva dei *link* verso alcune pagine dell'archivio *on line* del quotidiano spagnolo *La Vanguardia* sulle quali figurava un annuncio di vendita all'asta di alcuni immobili del ricorrente, risalente a sedici anni prima, connessa al pignoramento degli stessi effettuato per la riscossione coattiva di alcuni crediti. Come rilevato dal ricorrente, questo pignoramento era stato interamente definito da svariati anni e la menzione dello stesso,

---

(14) V. J.C. Juncker, *Orientamenti Politici per la prossima Commissione Europea*, 15 luglio 2014 (http://ec.europa.eu/priorities/docs/pg_it.pdf).

(15) Sulla sentenza *Google Spagna* e in particolare sull'equilibrio tra diritto alla protezione dei dati e diritto d'informazione, D. Erdos, *From the Scylla of Restriciton to the Charybdis of License? Exploring the Scope of the "Special Purpose" Freedom of Expression Shield in European Data Protection*, in *Comm. Market Law Rev.*, 2015, p. 119 ss.; R. Wacks, *Privacy: a very short introduction*, Oxford University Press, 2015, cap. 4.; G. Busseuil, *Arrêt Google: du droit à l'oubli de la neutralité du moteur de recherche*, in *Semaine juridique entreprise et affaires*, 2014, n. 24, 12 giugno, pp. 51-54.

gravemente pregiudizievole della sua vita privata, era ormai priva di qualsiasi rilevanza per il pubblico.

Ora, mentre per tutte le autorità amministrative e giudiziarie coinvolte nella controversia anche a livello nazionale il diritto alla protezione dei dati non avrebbe legittimato la soppressione dell'informazione di base in quanto la pubblicazione sul *La Vanguardia* era veritiera, legittima e aveva avuto luogo su ordine del Ministero del lavoro al fine di conferire il massimo della pubblicità alla vendita pubblica e raccogliere il maggior numero possibile di partecipanti all'asta, tale diritto fondamentale ben avrebbe potuto limitarne la diffusione su internet attraverso motori di ricerca come *Google Search*. La divulgazione d'informazioni sensibili relative a un individuo è in effetti differente a seconda che avvenga a mezzo stampa o attraverso l'uso delle moderne tecnologie. Come rilevato dalla Corte (punto 80), non può essere ignorato che l'esistenza di un legame tra l'archivio *on line* di un quotidiano e internet attraverso i motori di ricerca conferisce all'informazione una diffusione universale in grado d'incidere significatamene sui diritti al rispetto alla vita e alla protezione dei dati personali di un individuo. Tale trattamento consente, infatti, a qualsiasi utente di internet d'ottenere, mediante l'elenco dei risultati partendo dal mero nome di una persona fisica, una visione complessiva delle informazioni relative alla stessa e in particolare a una moltitudine d'aspetti della sua vita privata, i quali non sarebbero stati tra loro connessi o lo sarebbero stati con difficoltà senza l'ausilio di *Google Search*.

Il rischio di serie interferenze nella vita privata della persone fisiche è poi ancor maggiore considerato che motori di ricerca come quello in esame costituiscono ormai il principale strumento di ricerca d'informazioni usato nella società moderna. La Corte sembra così confermare le preoccupazioni dell'esecutivo europeo quanto alla necessità d'introdurre, modificando la direttiva 95/45, specifiche regole in grado di rispondere alle nuove sfide cui la moderna tecnologia ha sottoposto il diritto alla protezione dei dati.

Queste considerazioni sono state sufficienti per i giudici UE per escludere che l'interesse di *Google Search* allo svolgimento della sua attività economica potesse prevalere sulla protezione della vita privata (articolo 7) e dei dati personali (articolo 8) degli individui (punto 81). Più difficile è stato invece contemperare tali diritti con quello d'informazione. La soppressione di notizie anche solo dall'elenco dei risultati di un motore di ricerca produce, infatti, riper-

cussioni sul legittimo interesse degli internauti ad essere informati e a reperire informazioni su una certa persona fisica.

Ora, nel contemperare tali diritti, la Corte sembra aver ripreso, pur senza citarne precedenti giurisprudenziali, lo stesso metodo di valutazione della Corte EDU quanto alla ponderazione degli articoli 8 (diritto al rispetto della vita famigliare) e 10 (libertà d'espressione) CEDU (16). L'equilibrio tra i due diritti coinvolti deve in effetti essere valutato in funzione di vari elementi, da valutarsi caso per caso, quali la natura dell'informazione, il carattere sensibile della stessa per la vita privata della persona interessata, l'interesse del pubblico a disporre dell'informazione e il ruolo nella vita pubblica della persona oggetto dell'informazione (punto 81). Inoltre, interpretando estensivamente l'articolo 6 della direttiva 95/46 in base al quale una persona fisica ha diritto a vedere cancellate o rettificate le informazioni pubblicate se *non esatte o aggiornate*, la Corte di giustizia ha dedotto da tale norma anche l'obbligo del motore di ricerca a controllare che le informazioni pubblicate siano *adeguate, pertinenti e non eccedenti* rispetto alle finalità per le quali vengono rilevate, nonché siano conservate in modo tale da consentire l'identificazione delle persone interessate per un *arco di tempo non superiore a quello necessario*. Anche un trattamento dei dati inizialmente lecito, perché veritiero, esatto e aggiornato, può, in altri termini, diventare successivamente illecito ai sensi dell'articolo 6 della direttiva 95/46 così come interpretato dai giudici di Lussemburgo quando tali dati non siano più necessari in rapporto alle finalità per le quali sono stati inizialmente resi pubblici (punto 93), il che accade quando sia trascorso molto tempo dal momento della prima pubblicazione. Aggiungendo condizioni ulteriori a quelle previste dall'articolo 6 della direttiva 95/46, i giudici comuni ammettono dunque che i cittadini UE possano ricorrere ai rimedi di cui a quest'ultima norma, ossia la cancellazione dell'informazione, quando la pubblicazione delle stesse, ancorché veritiere e esatte, non sia più necessaria e sia quindi sproporzionata.

---

(16) Per un'analisi di questi aspetti UE-CEDU, v. il *Manuale sul diritto europeo in materia di protezione dei dati* pubblicato nel 2014 sul sito dell'Agenzia UE per i diritti fondamentali (FRA) e in particolare la sentenza *Axel Springer AG c. Germania* ove la Corte EDU ha precisato che, al fine di contemperare il diritto all'informazione di cui all'articolo 10 e quello alla tutela della vita privata di cui all'articolo 8, è necessario valutare (i) se il fatto pubblicato dall'articolo in questione rivesta un interesse generale; (ii) se l'interessato sia un personaggio pubblico; (iii) in che modo l'informazione sia stata ottenuta e se sia affidabile.

Alla luce di tutti questi elementi e posto che, secondo la Corte, (i) il sig. Gonzalez non ricopriva alcun ruolo pubblico; (ii) l'informazione in discussione, ossia il pignoramento e la vendita all'asta d'immobili di proprietà del ricorrente nella causa principale, non possedeva una particolare rilevanza per il pubblico ma aveva invece carattere sensibile per la vita privata dell'interessato; e (iii) la pubblicazione iniziale dell'informazione era stata effettuata ben sedici anni prima, i giudici UE hanno concluso ritenendo la prevalenza dell'esigenza del singor Gonzalez alla protezione dei dati rispetto a quella pubblica di fruire dell'informazione. Al fine di tutelare questo diritto fondamentale, *Google Search* era allora obbligato a sopprimere dall'elenco di risultati ottenuti a seguito di una ricerca effettuata a partire dal nome di una persona i *link* verso pagine *web* pubblicate da terzi e contenenti informazioni relative a questa persona, e ciò anche quando tali notizie non fossero state previamente o simultaneamente cancellate dalle pagine *web* di cui trattasi ed eventualmente anche quando la loro pubblicazione su queste ultime fosse di per sé lecita (punto 88).

Tale conclusione dei giudici UE ha suscitato varie critiche da parte della dottrina quanto in particolare al pregiudizio al diritto all'informazione (17). In realtà, l'analisi della pronuncia dimostra come i giudici di Lussemburgo non abbiano escluso la possibilità di una prevalenza di quest'ultimo diritto su quello alla tutela dei dati personali, il quale, al pari peraltro di ogni diritto anche fondamentale, non è assoluto. Anzi, proprio subordinandone la prevalenza a certe condizioni — il ruolo privato del soggetto o quando sia trascorso un lasso di tempo piuttosto lungo e rilevante — la Corte ne conferma la cedevolezza a favore del diritto d'informazione qualora *a contrario* la persona fisica interessata abbia un ruolo pubblico o, anche in assenza di quest'ultimo elemento, quando il tempo trascorso tra gli eventi oggetto della notizia e la pubblicazione della stessa sia ridotto o irrilevante. L'importanza del diritto d'informazione è peraltro testimoniata anche nella proposta di regolamento della Commissione europea, prevedendo il considerando 121 e l'articolo 80 la deroga al regime generale di tutela dei dati personali

(17) In tal senso, Foo Yung Chee, *Europe's Top Court: People have Right to Be Forgotten on Internet*, 13 maggio 2014 reperibile sul sito www.reuters.com. Sul diritto all'oblio, H. Kranenborg, *Google and the Right to Be Forgotten*, in *Protection Law Review*, vol. 1, 2015, p. 1-23; G. Busseuil, *Arrêt Google* cit.

proprio nel caso d'uso degli stessi per fini giornalistici (18) o d'espressione artistica o letteraria.

Né invero i giudici UE hanno creato per via giurisprudenziale un generale diritto all'oblio di ogni notizia, anche solo scomoda, pubblicata su internet, il quale sarebbe invocabile *a posteriori* e s'aggiungerebbe così al diritto d'opposizione *a priori* di cui all'articolo 14 della direttiva 95/46. La Corte non ha, infatti, riconosciuto al sig. Gonzalez il diritto a eliminare l'informazione né dal quotidiano spagnolo *La Vanguardia* o dal suo archivio *on line* né da internet, ma solo quello di cancellare l'informazione dalla lista di risultati ottenuti tramite un motore di ricerca esclusivamente *partendo dal proprio nome* (punto 100). L'informazione rimane in altri termini reperibile — e il diritto alla cancellazione non sussiste — anche *on line*, nonché attraverso i motori di ricerca ma solo partendo *da dati di ricerca differenti dal mero nome di una persona fisica*. I giudici UE sembrano così supportare la Commissione europea nel difficile compito di stabilire, approfondendo il diritto alla cancellazione di cui all'articolo 12.*b* della direttiva 95/46, i confini del diritto all'oblio (*right to be forgotten*) di cui all'articolo 17 della proposta di regolamento, il quale permetterebbe d'ottenere la cancellazione d'informazioni anche vere e corrette quando, ad esempio, i dati immessi non siano più necessari rispetto alle finalità per le quali sono stati raccolti o trattati (articolo 17.1.*a* della proposta di regolamento).

L'esigenza di circoscrivere la diffusione dei dati attraverso la rete e i motori di ricerca è emersa peraltro anche in sistemi diversi dall'Unione europea, quali il Giappone (19), il Messico (20) e il

---

(18) Il considerando 121, riprendendo principi già espressi dalla Corte UE nella sentenza *Satamedia* (16 dicembre 2008, C-73/07, punto 61), precisa al riguardo che rientrano nelle attività giornalistiche anche quelle finalizzate alla diffusione del pubblico di informazioni, pareri o idee, indipendentemente dal canale utilizzato per la loro trasmissione, senza limitarle alle imprese operanti nel settore dei media ma includendovi anche le attività intraprese con o *senza scopo di lucro* (e quindi ad esempio quelle dei *bloggers* su internet). Sulla sentenza UE *Satamedia*, D. Erdos, *From the Scylla of Restriciton* cit.; S. Vousden, Satamedia *and the Single European audiovisual area*, in *European Intellectual Property Review*, 2009, p. 533 ss.

(19) Il diritto all'oblio è stato di recente riconosciuto anche dalla giurisprudenza giapponese. Il 10 ottobre 2014 il tribunale di Tokio ha imposto a *Google Search* di cancellare dall'elenco dei risultati ottenuti partendo dal nome di una persona fisica il *link* ad alcune pagine del quotidiano *Kyodo News* risalenti a dieci anni prima ove il nome del soggetto in esame figurava tra quelli sospettati di un certo crimine, reato per il quale quest'ultimo era stato poi dichiarato innocente. In merito, www.japantimes.co.jp/news/2014/10/10/national/crime-legal/tokyo-court-orders-google-remove-search-results-man/#.VDzqlecRG2we.

(20) Il 26 gennaio 2015 l'autorità garante dei dati messicana ha deciso di aprire una procedura contro *Google Mexico* a seguito di una richiesta da parte di un cittadino messicano

Canada (21). Un recente studio mostra poi come la maggior parte dei cittadini nord americani sia favorevole all'introduzione di un diritto all'oblio anche negli USA (22), ossia in un sistema che, forse anche perché il diritto alla protezione dei dati personali non è riconosciuto a livello costituzionale, tende per lo più a privilegiarvi il diritto all'informazione. E in effetti dal 1º gennaio 2015 in California gli internauti minori di diciotto anni possono chiedere di cancellare o rimuovere notizie precedentemente messe *on line* e godono quindi di un vero e proprio *right to be forgotten* (23).

3. Segue. *L'applicazione della direttiva 95/46 all'attività di motori di ricerca anche localizzati in Paesi terzi.*

Al fine di giungere a tali conclusioni, la Corte di giustizia ha peraltro dovuto superare due questioni giuridiche preliminari. La prevalenza del diritto alla protezione dei dati nel caso di specie è in effetti stata possibile solo presupponendo che (i) l'attività di un motore di ricerca, quale è quella di *Google Search* (ma anche *Bing*, *Yahoo* etc.) d'indicizzare i dati personali pubblicati da terzi su alcune pagine *web*, costituisca un trattamento di dati rilevante ai sensi dell'articolo 2.*b* della direttiva 95/46 e che (ii) il gestore di detto motore sia responsabile del suddetto trattamento ai sensi dell'articolo 2.*d* del medesimo atto (24).

Quanto in particolare al primo profilo, la Corte, nella misura in cui ha considerato l'indicizzazione dei dati di cui a *Google Search* come trattamento rilevante, ha così ampliato le previgenti indicazioni di cui alla sentenza *Lindqvist*, la quale aveva già qualificato come trattamento ai sensi della direttiva 95/46 il mero fatto di far figurare i dati personali di un soggetto su una pagina *web* (punto 25). L'attività dei motori di ricerca non sarebbe allora meramente « neu-

---

di cancellazione di dati personali visibili con *Google Search*. In merito, http://aristeguinoticias.com/2701/mexico/inicia-ifai-procedimiento-para-sancionar-a-google-mexico/.

(21) In merito, www.cbc.ca/news/technology/right-to-be-forgotten-how-canada-could-adopt-similar-law-for-online-privacy-1.2676880.

(22) Così, www.softwareadvice.com/security/industryview/right-to-be-forgotten-2014.

(23) Sul diritto all'oblio negli USA e la possibilità di creare sul punto una convergenza, S.C. Bennett, *The Right to Be Forgotten: Reconciling EU and US Perspectives*, in *Berkley J. IntL Law* 161, 2012; M.L. Ambrose Jones, J. Ausloos, *The Right to be Forgotten Across the Pond*, in *Journal of Information Policy*, 2012.

(24) Per l'analisi di tali aspetti, C. Kuner, *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenger*, settembre 2014.

tra » — perché, come sostenuto da *Google*, non sarebbe in grado di modificare le notizie già pubblicate da terzi su internet e applicherebbe solo algoritmi matematici — ma è invece attiva, provvedendo il gestore all'estrazione, alla registrazione, all'organizzazione e alla comunicazione di dati personali agli utenti di internet sotto forma d'elenchi di risultati (punto 28), ossia ad attività che anche nella proposta di regolamento (articolo 4.5) rientrano nella nozione di « trattamento » dei dati. Né invero ogni notizia relativa a una certo soggetto è ricavabile attraverso i motori di ricerca, ben potendo certe notizie essere escluse attraverso l'uso di cosiddetti protocolli d'esclusione come « *robot.txt* » o di codici come « *noindex* » o « *noarchive* ». Si tratterebbe allora d'utilizzare queste tecniche, già applicate per escludere informazioni ritenute dagli editori delle pagine *web* non rilevanti o perché in violazione del diritto d'autore, anche per tutelare i dati personali dei cittadini UE.

Google Search è stato inoltre ritenuto dalla Corte responsabile del predetto trattamento dei dati, in modo autonomo peraltro rispetto all'editore della pagina *web*. Quanto a tale aspetto, i giudici di Lussemburgo sembrano così rovesciare il principio della neutralità degli intermediari applicato in passato con riferimento all'attività a pagamento di *Google Francia* attraverso il sistema *adwords* (25), nonché alla base della direttiva 2000/31 sul commercio elettronico (articoli 12-15), la quale è peraltro applicabile anche nel regime previsto dalla proposta di regolamento (articolo 2.3) (26). La lettura combinata di queste due pronunce sembra allora creare un paradosso: un motore di ricerca mentre è responsabile quanto alla sua attività di ricerca gratuita (sentenza *Google Spagna*) non lo è quando agisca nell'ambito della sua attività a pagamento (pronuncia *Google Francia* e direttiva sul commercio elettronico).

Il fatto poi che la Corte (punti 48-60) abbia ritenuto applicabile la direttiva 95/46 a un'attività realizzata di fatto da una società USA, ossia *Google Inc*., svolgendo *Google Spagna* per lo più attività di mera promozione e vendita di spazi pubblicitari, sul presupposto che *Google Inc*. possedeva uno stabilimento all'interno dell'UE (Spagna) e che il trattamento dei dati personali dei cittadini europei

(25) Corte di giustizia UE 23 marzo 2010, C-238/08, *Google France*, punti 117 ss.

(26) La direttiva è pubblicata in *GUCE* L 178 del 17 luglio 2000. Sul principio di neutralità degli intermediari, E. Derieux, *Neutralité et responsabilité des intermédiaires d'internet. Mythe ou réalité du principe de neutralité?*, in A. Strowel (a cura di), *La neutralité d'internet en Europe*, Bruxelles, 2013, p. 141 ss.

avvenisse in ogni caso « *nel contesto delle attività* » di *Google Spagna* di cui all'articolo 4.1.*a* della direttiva 95/46, conferma l'applicazione extraterritoriale del diritto UE alla protezione dei dati, già alla base della direttiva 95/46 (considerando 18 e 20, nonché articolo 4 della stessa) (27). Peraltro la proposta di regolamento — se, come lascia supporre il parere del Parlamento europeo del 21 ottobre 2013, sarà mantenuta anche nella versione definitiva dell'atto — amplia ulteriormente l'applicazione territoriale della disciplina comune inerente la protezione dei dati personali, prevedendo adesso chiaramente l'articolo 3.2 che le imprese anche non stabilite nell'Unione europea devono applicare la normativa UE *quando offrano beni e servizi ai consumatori europei o ne controllano il comportamento*. Come rilevato dalla Commissione europea nella sua comunicazione del 27 novembre 2013, il riferimento all'offerta di beni e servizi quale elemento in funzione del quale determinare l'applicazione della normativa europea, e non più solo « nel contesto delle attività di uno stabilimento » UE, garantirà, ancor di più rispetto al passato, il rispetto del diritto fondamentale alla protezione dei dati indipendentemente dall'ubicazione geografica di un'impresa o delle sue strutture di trattamento, le quali ben potranno essere localizzate anche interamente al di fuori dell'Unione.

4. *La sentenza* Digital Rights Irland Ltd *e la tutela dei dati personali nei rapporti verticali.*

L'importanza assegnata dalla Corte alla tutela dei dati personali nel sistema UE non si è tuttavia limitata ai soli trattamenti tra privati ma ha riguardato anche quelli tra cittadini e autorità pubbliche. In particolare, nella causa *Digital Rights Ireland Ltd* di poco precedente la sentenza *Google Spagna* (28), i giudici UE hanno affrontato le questioni giuridiche inerenti la raccolta, la conservazione e l'utilizzo dei dati di una persona fisica residente nell'Unione europea me-

---

(27) Sull'importanza della direttiva 95/46 anche oltre i confini UE, M. Birnhack, *The EU Data Protection Directive: An Engine of A Global Regime*, in *Computer Law & Security Repo*rt, 2008, p. 1 ss.

(28) Sulla pronuncia UE *Digital Rights Ireland Ltd*, T. Wisman, *Privacy: Alive and Kicking (The Digital Rights Ireland Jusgment)*, in *Protection Law Review*, vol. 1, 2015; E. Guild, S. Carrera, *The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive*, CEOS paper 65/2014; O. Lynskey, *The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland*, in *Common Market Law Review*, 2014, pp. 1789-1812.

diante comunicazioni telefoniche o elettroniche da parte di un'autorità pubblica di uno degli Stati membri, le quali erano regolate dalla direttiva 2006/24 (29). Al fine di prevenire, indagare e accertare reati gravi legati alla criminalità organizzata e al terrorismo (30), l'articolo 5 di tale atto, forse anche perché adottato all'indomani degli attentati terroristici di Madrid e Londra, imponeva in particolare ai fornitori di servizi di comunicazione elettronica o di una rete pubblica di comunicazione di conservare per un periodo di tempo significativo (fino a ventiquattro mesi) alcune categorie di dati personali inerenti gli utilizzatori — quelli per identificare la fonte dell'informazione e il destinatario, nonché la data, l'ora, la frequenza e la durata di una certa comunicazione telefonica o elettronica — in grado di consentire di trarre conclusioni molto precise sulla vita degli utenti, così da renderli accessibili alle autorità nazionali competenti.

Ora, pur se, come più volte rilevato dalla giurisprudenza UE e CEDU, la lotta alla criminalità grave e al terrorismo finalizzata al mantenimento della pace e della sicurezza costituisce un obiettivo generale dell'Unione europea, la cui efficacia dipende in larga misura dall'uso di moderne tecniche d'indagine quali sono per l'appunto le intercettazioni telefoniche e elettroniche oggetto della direttiva 2006/24, la Corte di giustizia ha concluso nel caso di specie considerando le interferenze nella vita privata dei cittadini UE di cui alla direttiva in esame, pur in principio ammesse, non proporzionate all'obiettivo di garantire la sicurezza pubblica. La direttiva permetteva, infatti, di conservare i dati di *qualsiasi* persona che facesse uso di *ogni* mezzo di comunicazione anche in assenza d'indizi tali da far credere che il loro comportamento potesse avere un nesso, ancorché indiretto o lontano, con reati gravi, nonché anche relativamente a persone soggette alla normativa sul segreto professionale. In altri termini, al fine di lottare contro la criminalità grave e il terrorismo e quindi contro l'iniziativa di gruppi circoscritti, la direttiva autorizzava a tracciare in maniera generale tutte le comunicazioni dell'insieme delle persone che facessero uso di telefonia fissa e mobile, accesso a internet, posta elettronica e telefonia su internet e quindi di

---

(29) *GUUE* L 105 del 13 aprile 2006.

(30) Nonostante la connessione con le materie di cui all'ex terzo pilastro, la direttiva 2006/24 trovava la propria base giuridica nell'articolo 95 TCE, inerente l'armonizzazione per la creazione del mercato interno, e non nel terzo pilastro. Sull'adeguatezza dell'articolo 95 TCE come base giuridica, la quale era stata messa in discussione già all'indomani dell'adozione della direttiva dall'Irlanda e dalla Slovacchia, Corte di giustizia UE 26 giugno 2006, C-301/04, *Irlanda c. Consiglio e Parlamento*.

tutti gli abbonati e gli utenti registrati senza imporre alcuna relazione tra soggetti controllati/dati conservati e una minaccia reale per la sicurezza pubblica.

La direttiva 2006/24 non stabiliva neppure regole chiare, limiti o eccezioni all'accesso e all'uso dei dati personali da parte delle autorità nazionali in grado di ridurre il rischio d'abusi o usi illeciti dei dati raccolti e conservati da parte delle stesse. Tale atto comune non circoscriveva, ad esempio, il numero di persone che disponessero di un'autorizzazione d'accesso e d'uso dei dati conservati, né subordinava tali attività ad alcun criterio oggettivo (ad esempio, per indagini penali riguardanti reati gravi da definirsi con precisione) o al controllo di un giudice o di un'entità amministrativa indipendente in grado di delimitare l'accesso e l'uso dei dati personali a quanto necessario per perseguire l'obiettivo generale perseguito della lotta alla criminalità. Infine, la direttiva non introduceva neppure criteri obiettivi (sul tipo dei dati raccolti o sui soggetti tracciati) che permettessero di determinare, tra i due estremi temporali indicati all'articolo 6 (da sei mesi a due anni), l'effettiva durata della conservazione dei dati, la quale avrebbe invece dovuto essere parimenti circoscritta a quanto strettamente necessario. Né invero la direttiva prevedeva un obbligo preciso degli Stati a stabilire simili limitazioni.

Ciò posto, come espressamente rilevato dalla Corte di giustizia (punto 37) e anche dall'avvocato generale (punti 77 e 80 delle conclusioni), l'ingerenza della direttiva 2006/24 sui diritti fondamentali sanciti dagli articoli 7 e 8 della Carta era allora particolarmente grave in quanto di vasta portata. Nonostante dunque il considerando 22 dichiarasse espressamente che la direttiva 2006/24 « rispetta i diritti fondamentali », quest'ultima, secondo la Corte, violava in modo non proporzionato i diritti di cui agli articoli 7 e 8 della Carta aventi rango primario (e probabilmente anche l'articolo 8 CEDU) ed era allora invalida.

Tale decisione si pone così in linea non solo con la giurisprudenza della Corte di Strasburgo relativa all'applicazione dell'articolo 8 CEDU a casi di raccolta, conservazione e utilizzo dei dati sensibili di una persona fisica (31), ma anche con le sentenze di alcune alte

---

(31) Così, Corte EDU 4 dicembre 2008, *S. e Marper c. Regno Unito*, 30562/04 e 30566/04 relativamente alla compatibilità con l'articolo 8 CEDU (vita privata e tutela dei dati personali) del sistema di raccolta, conservazione e utilizzo dei dati sensibili del Regno Unito. Tale sentenza è stata confermata con pronuncia 18 aprile 2013, *M.K c. Francia*, 19522/09 con riferimento al sistema francese. In merito, v. anche la più recente sentenza della Corte di

corti nazionali (Bulgaria, Romania, Germania, Cipro e Repubblica Ceca), le quali, chiamate nel biennio 2008-2010 a pronunciarsi sulla compatibilità delle leggi di trasposizione della direttiva 2006/24 con le norme costituzionali inerenti la protezione dei dati, avevano già dichiarato l'invalidità totale o parziale delle prime (32). Considerato poi che nessuno dei detti giudici nazionali, ancorché obbligati ai sensi dell'articolo 267.3 TFUE, aveva mai fatto rinvio pregiudiziale alla Corte UE relativamente alla validità della direttiva, la quale era la vera ragione d'incompatibilità, la sentenza in esame, resa a seguito dell'iniziativa delle Corti costituzionali irlandese e austriaca, ha allora anche risolto il paradosso relativo alla variegata applicazione dell'atto in esame nell'Unione europea. Mentre in effetti nella maggior parte degli Stati membri quest'ultima era stata trasposta e, applicata attraverso le leggi di trasposizione, in Germania, Bulgaria, Romania, Cipro e Repubblica Ceca il medesimo atto, pur inizialmente trasposto, era diventato di fatto inapplicabile per effetto delle decisioni d'annullamento delle leggi di trasposizione, il che, in mancanza dell'adozione di ulteriori atti interni, aveva in alcuni casi indotto la Commissione europea all'apertura di procedure d'infrazione per mancata trasposizione della direttiva (33). La Svezia era inoltre stata condannata al pagamento di un'ammenda di tre milioni di euro per non aver trasposto entro i termini la direttiva 2006/24 (34).

Strasburgo 18 settembre 2014, *Brunet c. Francia*, 21010/10, la quale ha stabilito che l'iscrizione per vent'anni dei dati personali di un soggetto sul sistema STIC (banca dati elaborata dalla polizia nazionale al fine di facilitare la ricerca delle violazioni penali) costituisce una violazione dell'articolo 8 CEDU quando, come nel caso di specie, la denuncia penale sia stata ritirata e non abbia più avuto seguito.

(32) Decisioni Corte suprema amministrativa bulgara dell'11 dicembre 2008 http://www.aipbg.org/documents/data_retention_campaign_11122008eng.htm.; Corte costituzionale rumena dell'8 ottobre 2009 n. 2158 sulla quale C. Murphy, *Romanian constitutional court decision No. 1258 of 8 October 2009*, in *Common Market Law Rev.*, 2010, pp. 933-941; Corte costituzionale tedesca del 2 marzo 2010; Corte costituzionale ceca del 22 marzo 2011; Corte Suprema cipriota del 1 febbraio 2011 sulla quale v. C. Markou, *Law&Security Review*, 2012, pp. 468-475. Analoghe cause erano poi pendenti in Ungheria e in Slovacchia.

(33) L'accertamento dell'inadempimento avverso la Germania di cui alla procedura d'infrazione C-329/12 è stato abbandonato (ordinanza della Corte del 5 giugno 2014) a seguito della sentenza in esame.

(34) Corte di giustizia UE 30 maggio 2013, C-270/11, *Commissione c. Svezia*. Nella seduta plenaria del Parlamento europeo del 16 aprile 2014 il commissiario Malmström ha confermato che, a seguito della dell'annullamento della direttiva 2006/24, la Svezia avrebbe ricevuto il rimborso delle somme pagate a titolo d'ammenda.

5. Segue. *L'invalidità della direttiva 2006/24.*

La sentenza in esame è particolarmente severa anche quanto al tipo d'invalidità imposta. Da un lato, infatti, i giudici UE hanno sancito l'invalidità non di alcune parti dell'atto, così come per lo più fatto in passato (35), ma bensì dell'intera direttiva. Al riguardo, la Corte si è anche premurata di precisare che, trattandosi di un'ingerenza particolarmente seria nei confronti di un diritto fondamentale, il margine di discrezionalità riconosciuto al legislatore UE è soggetto a importanti limitazioni e a un intenso sindacato giurisdizionale (punto 48). Dall'altro lato, la Corte di giustizia, respingendo la proposta dell'avvocato generale di sospendere l'applicazione della direttiva solo per il futuro (punti 154-158), ha annullato quest'ultima *ex tunc*.

La scelta, particolarmente rigorosa e poco frequente nella prassi, di non fare salvi gli effetti definitivi già prodotti dalla direttiva e quindi di non utilizzare una facoltà ammessa da tempo dalla giurisprudenza anche per il rinvio pregiudiziale di validità grazie all'applicazione analogica dell'articolo 264 TFUE, dimostrerebbe una volta di più la volontà dei giudici UE di considerare particolarmente grave la violazione da parte di atti comuni dei diritti fondamentali e in particolare di quello alla tutela dei dati personali, così come accade peraltro già da tempo nel sistema CEDU.

Ancora una volta a differenza di quanto sostenuto dell'avvocato generale (punto 157), i giudici UE non hanno dunque ritenuto sufficiente che gli Stati membri si fossero generalmente avvalsi con moderazione delle facoltà d'indagine loro attribuite dalla direttiva o che all'invalidità di quest'ultima si potesse porre rimedio nell'ambito delle misure di trasposizione. Anzi, la Corte, annullando l'*intera* direttiva con effetti *ex tunc*, ha sollecitato la Commissione e il legislatore UE a ripensare all'intero impianto dell'atto, offrendo peraltro anche indicazioni positive in merito quale, ad esempio, l'introduzione di limiti sostanziali e procedurali alla raccolta, alla conservazione e all'uso dei dati personali, nonché norme specifiche per garantirne la conservazione sul territorio dell'Unione e dunque in conformità al diritto UE. Quest'ultima esigenza sarebbe garantita in particolare richiedendo, conformemente all'articolo 8.3 della Carta, che i garanti nazionali di protezione dei dati controllino l'uso

(35) Ad esempio, Corte di giustizia UE 1 marzo 2011, C-236/09, *TestAchats*, punto 35.

dei predetti dati da parte delle autorità pubbliche. Tale supervisione da parte di autorità garanti indipendenti, la cui funzione assume così un ruolo essenziale nel ragionamento dei giudici di Lussemburgo (punto 68), assicurerebbe ai cittadini UE l'uso dei propri dati personali in conformità del diritto UE, cosicché *a contrario* sarebbe in violazione degli articoli 7 e 8 della Carta anche solo il trasferimento di tali dati al di fuori dell'Unione e in particolare in Paesi terzi con un livello di tutela inferiore a quello europeo quale è, ad esempio, il sistema USA.

6. Segue. *Gli effetti della sentenza sulle leggi nazionali di trasposizione della direttiva invalidata.*

L'annullamento della direttiva 2006/24 pone inoltre anche problemi per gli Stati membri e in particolare per quelli ove siano in vigore le leggi di trasposizione della direttiva invalidata. Queste ultime non sono, infatti, automaticamente nulle per effetto della sentenza della Corte, la quale è relativa a un atto UE e non a norme interne, cosicché spetta a ogni Paese membro — e in particolare ai legislatori nazionali anche con l'ausilio dei giudici interni — stabilire la sorte di questi atti. Almeno presupponendo che questi ultimi rispettino le indicazioni dalla direttiva e quindi non stabiliscano parimenti condizioni alla raccolta, alla conservazione e all'uso dei dati dei cittadini UE da parte di autorità pubbliche è probabile allora che anche tali leggi siano da ritenersi incompatibili con i diritti fondamentali di cui agli articoli 7 e 8 della Carta, applicabili anche nei Paesi membri in virtù della giurisprudenza *ERT* (36), secondo la quale gli Stati membri hanno l'obbligo di rispettare i diritti fondamentali definiti nell'ambito dell'Unione quando agiscano nel quadro del diritto UE.

Ulteriori profili d'incompatibilità dei regimi nazionali di raccolta dei dati potrebbero poi essere rilevati con riferimento al diritto secondario in materia di protezione dei dati. L'articolo 13.1 della direttiva 46 del 1995 autorizza, infatti, deroghe al regime generale di tutela per le persone fisiche al fine di perseguire la lotta al crimine esclusivamente con misure *necessarie e proporzionate* e in ogni caso nel rispetto dei diritti fondamentali di cui all'articolo 6 TUE, cosic-

(36) Corte di giustizia UE 18 giugno 1991, C-260/89, *ERT* confermata in 13 aprile 2000, *Omega*, C-292/97, punto 37.

ché leggi nazionali che, conformemente alla direttiva 2006/24, non subordinino a particolari cautele la raccolta, la conservazione e l'uso dei dati difficilmente possono sfuggire a un giudizio d'incompatibilità con tale diritto derivato in quanto, per l'appunto, non proporzionate. Considerato poi che l'articolo 13 della direttiva 95/46 è richiamato all'articolo 15.1 della direttiva 2002/58, la quale ha tradotto i principi enunciati dalla direttiva 95/46 in norme specifiche per il settore delle telecomunicazioni, tali leggi ben potrebbero essere stimate contrarie anche a tale norma. Per effetto della sentenza *Digital Rights Irland* non sembra in effetti più applicabile, in quanto parimenti contrario agli articoli 7 e 8 della Carta, l'articolo 15.1.*bis* della direttiva 2002/58, introdotto dalla direttiva 2006/24 annullata, il quale prevedeva l'inapplicabilità dell'articolo 15.1 della direttiva 2002/58 — e quindi la facoltà delle autorità pubbliche d'accedere senza limiti ai dati di cittadini UE — a ogni informazione la cui conservazione fosse specificamente prevista dalla direttiva 2006/24.

Tutto ciò ammesso, i legislatori nazionali, in virtù della giurisprudenza *ERT* e del principio di supremazia del diritto UE su quelli interni, si trovano così davanti alla scelta (i) d'abrogare le leggi inerenti sistemi nazionali di raccolta dei dati modellati sulla direttiva annullata, attendendo poi l'iniziativa della Commissione europea in merito (37), o invece (ii) di modificare tali leggi alla luce degli articoli 7 e 8 della Carta così come interpretati dalla Corte nella sentenza *Digital Rights Irland*, nonché degli articoli 13 della direttiva 95/46 e 15.1 direttiva 2002/58. A seguito dell'annullamento della direttiva 2006/24, infatti, l'applicazione senza adattamento di tali leggi esporrebbe i sistemi interni al rischio sia di procedure d'infrazione sia di ricorsi proposti davanti ai giudici nazionali da propri cittadini, organizzazioni non governative o dalle stesse società attive nel settore delle comunicazioni telefoniche o elettroniche (38).

In tali casi, i giudici interni potranno poi disapplicare tali leggi per incompatibilità con il diritto UE (se direttamente applicabile) o dichiararne, se del caso, l'invalidità per violazione del diritto costi-

---

(37) Sulla difficoltà di proporre a breve una nuova direttiva, v. il discorso del Commissario Malmström al Parlamento europeo del 16 aprile 2014, reperibile sul sito www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//TEXT+CRE+20140416+ITEM017+DOC+XML+V0//EN&language=EN.

(38) Sulla dichiarazioni di alcune società di telecomunicazioni di non proseguire più nella raccolta dei dati fino a che non sia fatta chiarezza in merito, L. Tung, *Four of Sweden's telcos stop storing customer data after EU retention directive overthrown*, 11 aprile 2014, reperibile http://www.zdnet.com.

tuzionale alla protezione dei dati o dell'articolo 8 CEDU, i quali sembrano parimenti configgere con leggi nazionali come quelle in esame. Quanto ai profili europei, le corti nazionali hanno poi sempre la possibilità di rinviare nuovamente alla Corte di giustizia qualora nutrano dubbi sull'interpretazione delle disposizioni comuni alla luce delle quali valutare la compatibilità delle leggi interne. Al riguardo, mentre alcuni Paesi, come il Lussemburgo, il Regno Unito e la Danimarca (39), probabilmente al fine di cercare di fare salvi i dati raccolti sotto il previgente regime, sembrano orientati al mantenimento con adattamento delle leggi nazionali inerenti il sistema di raccolta dei dati, le Corti costituzionali austriaca e slovena, le quali avevano sospeso il giudizio interno in attesa della sentenza *Digital Rights Irland*, hanno, successivamente a quest'ultima e riprendendone per ampi tratti il ragionamento, deciso più correttamente d'annullare le prime (40). Con sentenza del 3 luglio 2014, la Corte slovena ha inoltre ordinato anche la cancellazione dei dati personali raccolti e conservati fino a quel momento dalle società di comunicazioni (41).

7. Segue. *Gli effetti della sentenza sul quadro normativo UE inerente la lotta contro il terrorismo e la criminalità organizzata anche con Stati terzi.*

Il principio alla base della pronuncia *Digital Rights Irland*, secondo cui ogni deroga al diritto fondamentale della protezione dei dati personali deve essere stabilita in modo chiaro, puntuale e prevedibile, potrebbe produrre effetti anche su ogni altro atto comune, proposta UE e accordo internazionale che, al fine di lottare contro il terrorismo e la criminalità, permetta ad autorità anche extra-europee d'accedere e usare i dati di cittadini UE. Spetta allora alle istituzioni europee valutare ora se ed eventualmente in che misura tali atti o proposte UE, nonché accordi diritto internazionale

---

(39) V. il parere dell'autorità garante dei dati lussemburghese 214/2014 del 13 maggio 2014, www.cnpd.public.lu/fr/decisions-avis/2014/Vorratsdatenspeicherung/index.html. Per la Danimarca, v. il rapporto *Denmark: Data retention is here to stay despite the CJEU ruling* del 4 giugno 2014 reperibile sul sito http://edri.org. Il Regno Unito ha introdotto in luglio una legislazione nazionale d'emergenza reperibile sul sito https://www.gov.uk.

(40) V. decisioni del 27 giugno 2014 della Corte costituzionale austriaca G 47/2012 e 3 luglio 2014 della Corte costituzionale slovena U-I-65/13-19.

(41) www.noodls.com/view/CBCC11E1961CEAD647CBDAE7AB42C32F1DFA58E2?7018xxx1405095291.

siano conformi agli articoli 7 e 8 della Carta così come interpretati dalla Corte (42).

Il rispetto delle dette condizioni di proporzionalità sembra, ad esempio, doversi valutare innanzitutto con riguardo alla proposta di direttiva inerente il trattamento dei dati al fine di prevenire, indagare, accertare e perseguire reati o eseguire sanzioni penali. In particolare, l'importanza assegnata dalla Corte al controllo da parte delle autorità garanti indipendenti degli Stati membri (punto 68) potrebbe sollevare dubbi di legittimità, come rilevato dal Parlamento europeo nel marzo 2014 (43), quanto all'articolo 36, il quale ammette il trasferimento di dati personali di cittadini europei verso un Paese terzo anche in assenza di una decisione d'adeguatezza della Commissione di cui all'articolo 34 o con opportune garanzie stabilite dagli Stati di cui all'articolo 35 quando ciò sia essenziale per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o terzo (lettera *c*), nonché senza prevedere alcun ruolo delle autorità garanti indipendenti nazionali di cui all'articolo 39. Il fatto poi che la Corte di giustizia (punto 60) censuri il generico riferimento ai *reati gravi* di cui all'articolo 1.1 della direttiva 2006/24 quale presupposto per giustificare l'ingerenza nella vita privata di cittadini UE, sembra imporre la precisazione di questa nozione di base anche nella citata proposta di direttiva.

Tali valutazioni sembrano inoltre doversi effettuare anche con riguardo a tutti quegli accordi internazionali volti a garantire lo scambio di dati personali tra UE e Stati terzi al fine di prevenire e lottare contro il terrorismo, quali quello sul trattamento e il trasferimento di dati di messaggistica finanziaria raccolti tramite il sistema SWIFT dall'UE agli USA ai fini del programma di controllo delle transazioni finanziarie dei terroristi (TFTP) (44) o quello relativo al trasferimento delle registrazioni dei nominativi dei passeggeri europei (PNR) al dipartimento statunitense per la sicurezza interna (DHS) (45). In particolare, mentre la Corte richiede di stabilire

---

(42) Controllo già avviato dalla Commissione europea come rilevato nella comunicazione del 27 novembre 2013, *Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*, COM(2013) 846.

(43) V. l'emendamento del Parlamento europeo nella risoluzione del 12 aprile 2014 quanto al coinvolgimento delle autorità nazionali indipendenti, il quale ha portato alla proposta di modifica dell'articolo 36.

(44) *GUUE* L 195 del 27 luglio 2010, p. 5 ss.

(45) *GUUE* L 215 dell'11 agosto 2012, p. 5 ss. Sull'uso di dati raccolti medinati questi strumenti dale autorità USA, I. Brown, *The feasibility of transatlantic privacy-protective*

condizioni sostanziali e procedurali tanto all'accesso quanto all'uso da parte delle autorità nazionali (punto 61), l'articolo 4 dell'accordo PNR pone espressamente tali limiti solo all'uso degli stessi. L'articolo 3 di tale accordo autorizza, in particolare, il trasferimento dei dati PNR dai vettori aerei alle autorità USA « in blocco », ossia a prescindere da eventuali sospetti sull'affiliazione terroristica o criminale di un soggetto e in ogni caso in mancanza di un controllo delle autorità nazionali indipendenti degli Stati membri. Quanto poi all'accordo TFTP, nonostante gli articoli 2 e 4 stabiliscano regole più puntuali di quelle PNR quanto alle possibilità per il ministero del tesoro USA d'ottenere e usare dati di messaggistica finanziaria di cittadini UE, la Commissione e l'agenzia europea Europol hanno rilevato che la maggioranza dei dati trasferiti è relativa a soggetti non connessi ad attività terroristiche (46).

Inoltre, nonostante l'articolo 4.1 PNR consenta alla predetta autorità USA di usare e trattare i dati di cittadini europei al fine di prevenire, accertare, indagare e perseguire reati di terrorismo e i reati connessi (lettera *a*), nonché altri reati punibili con una pena detentiva non inferiore a tre anni (lettera *b*), il secondo e il terzo comma ampliano ulteriormente l'ambito d'applicazione *ratione materiae* dell'accordo (e la discrezionalità delle autorità USA in merito), prevedendo il trattamento dei PNR anche solo in vista di una (generica) minaccia grave e per salvaguardare gli interessi vitali di ciascun individuo o se così disposto dall'autorità giudiziaria, nonché per individuare i soggetti che *potrebbero* essere sottoposti a interrogatorio o esame approfondito al momento dell'arrivo o della partenza dagli USA. Come rilevato inoltre dalla dottrina (47), il quarto comma dell'articolo 4, precisando che i paragrafi 1, 2 e 3 non pregiudicano le competenze delle autorità di pubblica sicurezza e giudiziarie qualora siano individuate altre (imprecisate) violazioni

---

standards for surveillance, in *International Journal of Law and Information Technology*, 2014, pp. 1-18. In generale sul sistema USA prima e dopo l'11 settembre 2001, R. Levinson-Waldman, *What the Government does with Americans' data?*, Brennan Center for Justice at New York University School of Law, 2013.

(46) In merito, comunicazione della Commissione europea COM(2011)429 e il *Report* di Europol del 18 marzo 2013 reperibile sul sito http://europoljsb.consilium.europa.eu/reports.

(47) G. Hornung, F. Boehm, *Comparative Study on the 2011 draft Agreement between the Unites States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security* del 14 marzo 2012 reperibile sul sito www.uni-muenster.de/Jura.itm/hoeren/itm/wpcontent/uploads/PNR-Study-FINAL-120313 pdf, p. 11.

del diritto o indizi di violazione, apre di fatto la porta all'uso dei PNR anche per reati minori, inizialmente esclusi dall'accordo.

L'accordo PNR non prevede inoltre il coinvolgimento delle autorità garanti indipendenti degli Stati membri al momento della raccolta, del trasferimento o dell'uso dei dati, il cui ruolo è, come anzi detto, essenziale per valutare come proporzionata l'ingerenza di autorità pubbliche nella sfera privata dei cittadini europei. Né invero tale mancanza può essere compensata dal fatto che l'articolo 14 PNR preveda, al fine di prevenire abusi, la supervisione dei *Privacy Officers* del DHS. Quest'ultimo non è, infatti, un'autorità garante di uno degli Stati membri, come pare invece richiedere la Corte, e non ha neppure le caratteristiche d'indipendenza richieste dall'articolo 8 della Carta (48). I *Privacy Officers*, pur godendo di una certa autonomia funzionale, sono infatti integrati nella struttura organizzativa del DHS, ossia nell'autorità che riceve e tratta i dati personali in questione.

Ulteriori problemi d'incompatibilità potrebbero poi rilevare quanto al periodo di conservazione dei dati, il quale, come rilevato dalla Corte di giustizia (punti 63-64), deve essere determinato in funzione d'elementi oggettivi e deve differenziarsi a seconda del tipo di dato preso in esame, della sua utilità o delle persone interessate. L'articolo 8.1 PNR stabilisce, infatti, che *ogni* dato di cittadini europei, peraltro anche non sospetti, sia conservato per cinque anni personalizzato e per ulteriori dieci anni spersonalizzato (commi 2 e 3). Inoltre, dopo quindici anni (e quindi dopo un periodo ben più lungo dei ventiquattro mesi di cui alla direttiva 2006/24) i dati conservati non sono cancellati ma devono solo essere resi completamente anonimi, cancellando tutti i tipi di dati che potrebbero servire per individuare il passeggero (comma 4).

La necessità di chiarire tali dubbi di compatibilità e quindi il giusto equilibrio tra, da un lato, attività di contrasto e mantenimento della sicurezza pubblica e, dall'alto, tutela dei dati personali sembra essere condivisa anche dal Parlamento europeo, il quale ha proprio di recente chiesto alla Corte di giustizia un parere sulla compatibilità con i trattati e la Carta dei diritti fondamentali del progetto d'accordo UE-Canada del 25 giugno 2014 sul trasferimento dei dati dei

(48) Sulle caratteristiche di un'autorità indipendente in materia di protezione dei dati, Corte di giustizia UE 16 maggio 2014, C-288/12, *Commissione c. Ungheria*; 16 ottobre 2012, C-614/10 *Commissione c. Austria*.

passeggeri (PNR), il quale riprende per ampi tratti l'accordo PNR UE-USA (49). Tale parere avrà inoltre anche il merito di precisare se i principi elaborati nella sentenza *Digital Rights Irland* abbiano una portata generale e siano quindi applicabili anche in ambiti contigui, ancorché più circoscritti (ad es. il PNR riguarda (solo) i dati dei passeggeri di vettori aerei), o invece, posto che la direttiva 2006/24 riguardava la raccolta, la conservazione e l'utilizzo *su larga scala* di *ogni* dato personale di *tutte* le persone residenti nell'UE, essi siano invece limitati alla direttiva annullata.

Ulteriori risposte potrebbero inoltre trarsi a breve anche per effetto del rinvio pregiudiziale proposto dalla Corte costituzionale irlandese il 25 luglio 2014 (C-362/14) quanto alla compatibilità, ancora una volta con gli articoli 7 e 8 della Carta, della decisione 2000/520 (50) (c.d. « Approdo sicuro » o « *Safe Harbour* »), la quale fornisce una base giuridica per il trasferimento di dati personali dall'UE a società stabilite negli USA per fini commerciali. In particolare, nell'ambito di una controversia tra uno studente austriaco e il garante della privacy irlandese in relazione al trattamento dei dati personali del primo da parte di Facebook Ireland, l'alta corte irlandese, investita del ricorso presentato dal sig. Schrems avverso il rifiuto dell'autorità irlandese di sindacare il livello di protezione offerto dal regime « Approdo sicuro », ha domandato alla Corte di chiarire se ed eventualmente in quale misura le autorità garanti degli Stati membri possano verificare i presupposti sui quali si basa la decisione 2000/520. In effetti l'articolo 3 della stessa autorizza dette autorità a sospendere, a certe condizioni, i flussi di dati verso imprese USA, facoltà che peraltro il garante federale tedesco per la protezione dei dati sta al momento valutando d'azionare (51). In estrema sintesi, il rinvio verte sulla questione di sapere se, a seguito delle c.d. « rivelazioni *Snowden* » che hanno rivelato programmi di sorveglianza massiccia e apparentemente indiscriminata da parte dei servizi statunitensi, il regime « Approdo sicuro » è ancora in grado di

(49) In merito, la comunicazione della Commissione europea del 27 novembre 2013 COM(2013)844, nonché il rapporto del 2014 del *Department of Homeland Security* al Congresso www.dhs.gov/sites/default/files/publications/dhs-privacy-office-2014-annual-report-FINAL.pdf.

(50) Decisione della Commissione del 26 luglio 2000 a norma della direttiva 95/46 sull'adeguatezza della protezione offerta dai principi di Approdo sicuro (*GUCE* L 215 del 25 agosto 2000).

(51) http://linkis.com/pcworld.idg.com.au/bHMxM.

assicurare un appropriato livello di protezione dei dati personali provenienti dall'UE.

La possibilità di sospendere unilateralmente il regime Approdo sicuro potrebbe tuttavia non essere la soluzione migliore. Da un lato, infatti, misure nazionali di questo tipo ben possono creare disparità nell'applicazione di un meccanismo, quello inerente il trasferimento di dati tra UE e USA, ideato invece come uniforme a livello UE. Dall'altro lato, l'azione nazionale s'aggiungerebbe a quella di controllo dell'esecutivo UE di cui agli articoli 3 e 4 della decisione 520, la quale è stata in effetti già avviata. Come risulta dalla comunicazione del 27 novembre 2013, infatti, quest'ultimo ha già individuato alcuni punti deboli ed insufficienti garanzie del regime « Approdo sicuro » e, ritenendo di non poter continuare ad applicarlo secono le modalità stabilite, ha avviato all'inizio del 2014 una negoziazione con le autorità USA finalizzata rafforzarne il funzionamento in base a 13 puntuali raccomandazioni (52). Due di queste raccomandazioni riguardano proprio la problematica oggetto del rinvio pregiudiziale, e cioè la necessità di garantire che l'accesso di autorità pubbliche per motivi di sicurezza nazionale o di contrasto al crimine a dati personali trasferiti nell'ambito del regime « Approdo sicuro » sia limitato a quanto necessario e proporzionato al perseguimento di tali finalità. In tale contesto, la sentenza pregiudiziale della Corte potrebbe allora fornire, così come già fatto in occasione delle pronunce *Google Spagna* e *Digital Rights Irland*, utili indicazioni agli Stati membri, alla Commissione europea e anche alle stesse autorità nord americane.

(52) www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_it.pdf.