DIPARTIMENTO DI GIURISPRUDENZA

CATTEDRA DI INFORMATICA GIURIDICA

LA PROTEZIONE DEI DATI PERSONALI NEL TRATTAMENTO SVOLTO DA OPERATORI ESTERI

RELATORE Prof. Gianfranco Caridi

CANDIDATO Vincenzo Navarra

MATR. 097323

CORRELATORE Prof. Lorenzo Grisostomi Travaglini

ANNO ACCADEMICO 2013/2014

INDICE DEI CONTENUTI

1. Introduzione

"*Per una economia basata sull'informazione, come quella del prossimo futuro, la privacy sarà ciò che protezione del consumatore e la tutela dell'ambiente sono stati per l'economia industrialista del 20° secolo*" (Rotenberg)[1].

Il ruolo delle norme sulla tutela dei dati personali ha storicamente acquisito una maggiore centralità nella società di pari passo all'evoluzione tecnologica. Quest'ultima infatti permette una diffusione dei dati che non ha precedenti nella storia dell'uomo.

Per dirla con le parole di Michael Bogdan, giurista svedese:

"*L'evoluzione e l'avanzamento tecnologico dei computer ha costretto i giuristi a dar risposta a nuovi e complessi problemi […]. Attraverso la rete dei collegamenti e l'elaborazione automatizzata, la tecnologia moderna ha reso possibile raccogliere, comparare e combinare un'enorme quantità di dati riguardanti ogni singola persona. Inoltre, dati che non sono privati di per sé, attraverso la loro frequenza, quantità ed*

[1] Marc Rotenberg, Presidente e Direttore Esecutivo dell'Electronic Privacy Information Center in Washington, DC

intercorrelazione, pongono l'individuo sotto una lente di ingrandimento in grado di esporre gran parte della sua vita privata…".[2]

Questa concezione della tecnologia è piuttosto comune tra i giuristi odierni, ma ciò che rende interessante la visione di Bogdan è la data in cui è stata elaborata, più di 35 anni fa.

Ciò dà consapevolezza di due punti.

Primo, molti dei problemi che la normativa sul trattamento dei dati si trova ad affrontare sono parte della discussione accademica da lunga data.

Secondo, la riforma legislativa è un percorso lungo e laborioso. Ed anche assumendo che la legge non possa tenere il passo dell'avanzamento tecnologico, ci si deve chiedere quanto sia ammissibile che rimanga indietro.[3]

Mantenere uno sguardo al legame tra protezione dei dati personali e tecnologia è di estrema importanza nello studio della protezione dei dati personali nel trattamento svolto da operatori esteri.

[2] Michael Bogdan, "*Dataflykt over gränserna och den svenska datalagstiftningen*", Svensk Juristtidning 1978
[3] Christopher Kuner, "*The (data privacy) law hasn't even checked in when technology takes off*", International Data Privacy Law 2014 vol. 4 n. 3

Ed è proprio il fatto che gli operatori in questione siano “esteri” il punto fondamentale della questione. Se la normativa tende a dividere, a porre una netta distinzione tra Italia, Europa, Paesi membri dell’Unione da un lato e “Paesi stranieri” dall’altro, l’evoluzione tecnologica tende invece ad unire indipendentemente dalla nazionalità.

Questa capacità di unificare ha portato certamente un gran numero di vantaggi nell’”*economia dell’informazione*” definita da Rotenberg, ma al contempo conduce a difficoltà quando Paesi tra cui intercorre un frequente flusso di dati si basano su una concezione del diritto alla privacy differente.

Analizzando la normativa sulla protezione dei dati personali europea e ponendola, con sguardo comparativo, affianco a quella di un Paese straniero come gli Stati Uniti d’America, si individua immediatamente una forte differenza nella tradizione su cui questa si fonda.

E sono inoltre gli USA il Paese dove ad oggi avviene gran parte del trattamento dei dati personali dei cittadini italiani ed europei, soprattutto se si dà uno sguardo all’operato di società quali Google, Facebook, Twitter; è proprio questo il motivo principale che porta a concentrarsi sugli Stati Uniti come protagonista estero nel trattamento dei nostri dati personali.

Per avere un quadro completo delle differenze nella tutela dei dati personali in Europa ed in America è bene partire dalle radici del diritto alla privacy nei due contesti.

Per quanto riguarda il diritto statunitense, bisogna ricordare che il primo emendamento della Costituzione americana tutela il "*right of free speech*".

La tutela della libertà di parola esprime quei valori di libertà su cui si è basata l'indipendenza americana, e come tale viene posta al di sopra del diritto alla privacy. Tanto che la Costituzione americana protegge i potenziali violatori della privacy in maniera più esplicita delle potenziali vittime.[4]

Per trovare un riferimento alla tutela dei dati personali nella cultura giuridica americana la ricerca deve volgere verso la famosa sentenza *Griswold v. Connecticut*[5].

In questo landmark case il Justice William O. Douglas della Supreme Court of the United States sostenne che, nonostante il Bill of Rights non faccia espressa menzione del diritto alla protezione dei dati personali, questo sia implicitamente previsto nella "*penombra*" e nelle "*emanazioni*"

[4] Donald C. Dowling, Jr, "*International Data Protection and Privacy Law*", White & Case, Agosto 2009
[5] Supreme Court of the United States, Griswold v. Connecticut, 381 U.S. 479, 1965

di altre tutele costituzionali (*penumbra doctrine*). Segnatamente, in Grisworld v. Connecticut, si è ricavato tale diritto dal V emendamento, come protezione dalle intrusioni governative (anche se ad oggi la Corte Suprema, con un'interpretazione che tiene in considerazione anche il XIV emendamento, ne trova la fonte nella *substantive due process clause*).

Queste considerazioni hanno portato gli Stati Uniti ad una normativa sulla protezione dei dati personali di tipo settoriale, che pone un'attenzione più o meno maggiore al problema della sua tutela a seconda dell'ambito considerato.

All'approccio normativo settoriale statunitense se ne oppone uno comprensivo europeo, in cui il diritto alla tutela dei dati personali ha una rilevanza di rango elevato.

La Convenzione Europea dei Diritti dell'Uomo prevede infatti all'art.8 che "*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza*". Al contempo la Carta dei diritti fondamentali dell'Unione Europea prevede all'art.8(1) che "*Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano*".

Questo protezione è frutto di una tradizione europea che non pone tanto il diritto alla privacy come contrapposto alla libertà di parola, quanto lo avvicina concettualmente alla proprietà intellettuale.

I dati personali sono di "*proprietà*" dell'individuo almeno al pari di come uno slogan o un trademark lo siano del patrimonio di una società. E se questi ultimi elementi meritano protezione dallo sfruttamento dei competitor, allo stesso modo l'individuo ha diritto di proteggere le proprie convinzioni politiche o la propria vita sessuale da ingerenze esterne, statali o private che siano.

Il divario nelle considerazioni sulla privacy tra USA e Europa si fa ancora più ampio in quegli Stati Membri europei che hanno avuto esperienza in prima persona dei regimi totalitari del secolo scorso. La tradizione di questi paesi porta ad una diffidenza verso lo Stato, e similarmente verso le grandi multinazionali, che ammassano banche dati di informazioni personali per scopi talvolta poco chiari ai loro utenti.

Al contrario, per dare uno sguardo alla cultura americana sull'argomento, Eric Schmidt, ex CEO di Google, sostiene: "*If you have something that*

you don't want anyone to know, maybe you shouldn't be doing it in the first place".[6]

È questo un altro punto di divergenza tra Europa e USA, specialmente considerando i trend odierni nelle pressioni dello Stato sull'accesso ai dati del settore privato.

Uno studio pubblicato sull'International Data Privacy Law Oxford Journal[7] rileva, tra i suoi punti più importanti, come si sia, negli ultimi anni, incrementato l'accesso statale a dati del settore privato, definito come "*accesso diretto da parte dell'apparato statale a banche dati del settore privato, senza mediazione o interazione di un dipendente o agente dell'ente presso cui i dati sono archiviati*" e "*accesso da parte dell'apparato statale, mediato o meno da una società, a grandi volumi di dati del settore privato*". Lo studio rileva inoltre frequente mancanza di trasparenza, una significativa inconsistenza tra ciò che è previsto dalla legge e ciò che avviene nella pratica, e la prevalenza di un "*systematic volunteerism*" (il modo più frequente attraverso cui gli Stati ottengono accesso ai dati privati è la semplice richiesta).

[6] Documentario "*Inside the Mind of Google*", CNBC 3 Dicembre 2009
[7] Christopher Kuner, "*Systematic Government Access to Private-Sector Data Redux*", International Data Privacy Law 2014 vol. 4 n. 1

Se il quadro delle pressioni governative per l'accesso a dati del settore privato non fornisse abbastanza preoccupazioni per i dati raccolti ed elaborati nel proprio Paese, a maggior ragione ne fornisce quando le pressioni governative avvengono in Paesi esteri, verso cui il potere di controllo europeo è molto ridotto.[8]

La problematicità della protezione dei dati trattati all'estero nasce dal bilanciamento di due fattori. Da un lato, il dovere di tutelare il diritto alla protezione dei dati personali con efficacia extraterritoriale, in mancanza del quale il diritto rimarrebbe protetto solo nella teoria. Dall'altro lato pretese giurisdizionali extraterritoriali troppo stringenti sono difficili da attuare, perché gli strumenti di tutela a disposizione del cittadino scemano in efficacia nel contrastare violazioni che avvengono al di fuori della sfera di sovranità del proprio Paese.

A ciò va aggiunta l'impossibilità logistica di una regolamentazione troppo rigida di internet, poiché richiederebbe che i soggetti attivi sulla rete modulino la propria condotta relativamente alle leggi di ogni Paese con cui la diffusione ha contatto.[9]

[8] Ira Rubinstein, New York University School of Law, Greg Nojeim, Center for Democracy & Technology, Ronald Lee, Arnold & Porter LLP, "*Systematic Government Access to Personal Data: A Comparative Analysis*" 13 Novembre 2013

[9] Dan Svantesson, "*Fundamental policy considerations for the regulation of Internet cross-border privacy issues*", Policy & Internet 2011

E se da un lato la recente legislazione e la volontà di riforma della tutela dei dati personali a livello europeo dimostrano una rinnovata serietà nel trovare nuove soluzioni a questi problemi, dall'altro i cittadini, soprattutto le nuove generazioni, non sembrano avere la protezione della propria privacy come una delle priorità nel relazionarsi con le nuove tecnologie, anzi, pare l'opposto.

Già nel '96 James Gleick, pioniere nello studio dell'impatto culturale delle nuove tecnologie, avvertiva sulle pagine del New York Times "*Big Brother is us*".[10] Queste parole sembrano oggi profetiche quando anche Mark Zuckerberg, CEO di Facebook, dichiara che "*l'era della privacy è finita*".[11]

Sembrerebbe da un lato che la protezione dei dati personali sia un argomento di interesse più accademico che insito nella società, ma è ad oggi realmente così?

Nel 2008, anno in cui Facebook iniziò ad espandersi globalmente[12], scriveva Jhon Palfrey: "*Come consumatori e cittadini, continuamente barattiamo il controllo per la convenienza, dando via nel processo un crescente ammontare di informazioni personali. Le nostre vite sono*

[10] New York Times, "*Big Brother is Us*", James Gleick, 29 Settembre 1996
[11] Schneier 2010
[12] Conferenza stampa "*Facebook to Establish International Headquarters in Dublin, Ireland*", Facebook, 2 Ottobre 2008

continuamente mediate da tecnologie digitali e descritte dai dati contenuti in formati digitali. E mentre avanziamo velocemente verso lo sviluppo di nuove tecnologie, le istituzioni designate per la protezione di tali dati paiono restare indietro. Il tradeoff è raramente preso in considerazione".[13]

Tuttavia negli ultimi anni questo costo opportunità, del perdere controllo sui propri dati per ottenerne convenienza, ha ricevuto una nuova attenzione. Ed è un'attenzione che per i motivi già elaborati, non può mancare di volgersi al trattamento estero.[14]

E se finora si è trattato degli interessi degli utenti, a questo dibattito è necessario che partecipino anche gli operatori esteri, che si trovano nella posizione di soggetti attivi nel trattamento dei dati.

Il loro interesse al dibattito è dettato da vari motivi[15], tra cui la portata extraterritoriale della normativa, la circostanza che la definizione di "*data processing*" si sia estesa fino a comprendere parte centrale delle attività in settori come servizi finanziari, assicurazioni, consulting, giornalismo e servizi internet, la considerazione che violazioni della privacy ad oggi comportano conseguenze ben più gravi delle sole

[13] Palfrey, "*Born Digital*" 2008, pag. 243
[14] Christopher Kuner, Fred H. Cate, Christopher Millard, e Dan Jerker B. Svantesson "*The extraterritoriality of data privacy laws — an explosive issue yet to detonate*", International Data Privacy Law 2013 vol. 3 n. 3
[15] Donald C. Dowling, Jr, "*International Data Protection and Privacy Law*", White & Case, Agosto 2009

sanzioni, soprattutto in termini di pubbliche relazioni e dei rapporti con i consumatori.

Questo interesse per i due lati della questione, del bilanciare il diritto alla protezione dei dati con quello speculare delle necessità del trattamento di questi, si rivela il punto centrale della questione.

Nei capitoli successivi verranno analizzati strumenti frutto della normativa , il diritto vivente della giurisprudenza, e come ad oggi si possa rispondere alle nuove sfide sul tema poste da una società globale.

2. Normativa

Non potendo uno studio giuridico prescindere dal testo normativo, questo capitolo sarà dedicato allo studio delle fonti della tutela dei dati personali, secondo la prospettiva del loro trattamento da parte di operatori esteri.

Verranno analizzati anzitutto i principi che il legislatore ha tenuto in primo piano nel regolare la materia. In seguito si passeranno in rassegna le norme del diritto italiano e dell'Unione Europea, per concludere con la regolamentazione derivante da accordi internazionali.

In una seconda parte verranno approfonditi gli enti e gli organi indipendenti previsti dalla normativa allo scopo di tutelare con efficacia il diritto di ogni cittadino alla protezione dei dati personali.

2.1 Principi

I principi su cui si basa la protezione dei dati personali nel contesto del trasferimento estero sono fondamentalmente quelli applicabili per la protezione dei dati nel contesto degli Stati Membri dell'Unione europea.

Ma è proprio questa necessità di far valere anche per il trattamento estero un nucleo minimo di garanzie paragonabili a quelle interne che spinge la normativa europea a regolare tali trasferimenti. Ciò è teso ad evitare che i cittadini, i cui dati sono fuoriusciti dal controllo europeo, possano trovarsi spogliati di ogni tutela.

La base dei principi europei in materia si trova nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (da qui CEDU) all'art. 8, che recita "*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza*". Inoltre la Carta dei diritti fondamentali dell'Unione Europea prevede esplicitamente una protezione dei dati personali, all'art.8(1), prevedendo che "*Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*".

Queste previsioni di carattere generale si esplicano poi in una serie di principi indispensabili per una definizione completa del diritto alla

protezione dei dati personali. Sono qui di seguito indicati e brevemente discussi.

2.1.1 Principio di legalità

Il principio di legalità è previsto dall'art.5(a) della Convenzione 108/81 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (da qui Convenzione 108/81) e dall'art.6(1)(a) della Direttiva sulla protezione dei dati personali 95/46/CE.

I due articoli sono qui riportati

Convenzione 108/81 Art. 5(a):

"*I dati a carattere personale oggetto di elaborazione automatica devono essere:*

a. ottenuti ed elaborati lealmente e legalmente; ..."

Direttiva 95/46 Art 6(1)(a).

"*Gli Stati membri dispongono che i dati personali devono essere:*

a) trattati lealmente e lecitamente; …"

Nessuno dei due articoli dà una definizione di legalità del trattamento. Per comprendere il termine si deve far riferimento alla giurisprudenza della Corte Europea dei Diritti dell'Uomo ed all'art.52 della Carta dei

diritti fondamentali dell'Unione Europea su "*Portata e interpretazione dei diritti e dei principi*".

Il trattamento dei dati deve essere bilanciato col diritto al rispetto della vita privata del soggetto i cui dati vengono trattati. Quest'ultimo diritto non è in ogni caso assoluto, ma è da porre in relazione con interessi privati (di altri soggetti di diritto) e pubblici (della società nel suo insieme).

Le condizioni in cui si possa incidere sul diritto al rispetto per la vita privata, secondo la giurisprudenza della Corte Europea dei diritti dell'uomo (da qui "Corte EDU") sono:

1) Il rispetto per la legge

L'interferenza avvenga nel rispetto di una legge conoscibile da parte degli interessati e prevedibile nei suoi effetti, ovvero formulata con sufficiente precisione da permettere ad ogni individuo di regolare la propria condotta in relazione ad essa.[16]

[16] Per la conoscibilità e la prevedibilità dei suoi effetti:
Corte Europea dei Diritti dell'Uomo, Amann v. Switzerland [GC], N. 27798/95, 16 Febbraio 2000, par. 50; vedi anche Corte Europea dei Diritti dell'Uomo, Kopp v. Switzerland, N. 23224/94, 25 Marzo 1998, par. 55 e Corte Europea dei Diritti dell'Uomo, Iordachi and Others v. Moldova, N.25198/02, 10 Febbraio 2009, par. 50.
Per la sua attitudine a rendere rispettosa la condotta dell'individuo:
Corte Europea dei Diritti dell'Uomo, Amann v. Switzerland [GC], N. 27798/95, 16 Febbraio 2000, par. 56; vedi anche Corte Europea dei Diritti dell'Uomo, Malone v. the United Kingdom, N. 8691/79, 2 Agosto 1984, par. 66; Corte Europea dei Diritti dell'Uomo, Silver and Others v. the United Kingdom, N. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 Marzo 1983, par. 88.

2) Lo scopo del trattamento sia legittimo

Lo scopo legittimo lo si può rinvenire in uno dei pubblici interessi tipizzati, quali sicurezza, difesa, salute etc… ovvero nei diritti e nelle libertà di altri soggetti privati.

3) Sian necessario in una società democratica

La Corte EDU ha previsto, nella sentenza, Leander v. Sweden, n. 9248/81, 26 Marzo 1987, par. 58., che "*the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued*".

D'altra parte la Carta dei diritti fondamentali dell'UE (da qui CDFUE) non tratta di "*interferenze*" statali sui diritti garantiti ai cittadini, ma piuttosto di limitazioni sull'esercizio dei diritti e delle libertà previsti dalla Carta stessa.

Secondo l'art. 52(1) CDFUE, limitazioni al diritto alla protezione dei dati personali sono ammissibili solo se:

1) Siano previste dalla legge.
2) Rispettino il contenuto essenziale di tale diritto.
3) Siano necessarie e sottoposte al principio di proporzionalità.

4) Rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Nonostante la differente impostazione tra CEDU e CDFUE si trova un punto di raccordo formale nell'art 52(3) della CDFUE dove si prevede che "*Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione …*"

Ciò non impedisce comunque che l'Unione Europea preveda una protezione dei dati personali più estensiva, come disposto dall'art. 52(3) CDFUE.

2.1.2 Principio di specificità e limitazione della finalità del trattamento

Questo principio lega la legittimità del trattamento alle sue finalità. La finalità deve essere anzitutto specificata e resa manifesta dal titolare del trattamento prima dell'inizio dello stesso. Il trattamento di dati per finalità indeterminate o senza alcun limite è quindi in violazione di tale principio.

Inoltre ogni nuova finalità del trattamento deve avere una sua base legale e non può basarsi sul semplice fatto che i dati siano stati in origine acquisiti per una finalità diversa. Da qui discende che il trattamento legittimo è limitato alla finalità originariamente prevista.[17]

Nel determinare l'ampiezza ed il limite di una certa finalità, la Convenzione 108/81 e la Direttiva 95/46/CE fanno ricorso al concetto di "*compatibilità*": il trattamento di dati per "*finalità compatibili*" è permesso poggiandosi sulla base legale della finalità originaria.

La definizione di "*finalità compatibile*" è tuttavia lasciata all'interpretazione su base casistica.

[17] Vedi anche Article 29 Working Party, Opinione 03/2013 del 2 Aprile 2013 "*purpose limitation*", WP 203

Un esempio di finalità genericamente compatibile con ogni trattamento di dati è quella del trattamento per motivi storici, statistici o scientifici, purché siano previste certe salvaguardie dalla legge nazionale degli Stati Membri, come indicato dalla direttiva 95/46.[18]

[18] Un esempio di tali previsioni nazionali lo si trova nella legge austriaca sulla protezione dei dati (Datenschutzgesetz), Federal Law Gazette No. 165/1999, par. 46

2.1.3 Principi sulla qualità dei dati

I dati oggetti del trattamento devono essere adeguati, rilevanti e non eccessivi in relazione alla finalità per cui sono stati raccolti o saranno ulteriormente trattati.

E' compito del titolare del trattamento limitare la raccolta di dati a quelli strettamente necessari, e se possibile far uso di tecnologie che permettano l'anonimizzazione di questi.

Dal principio della qualità dei dati derivano vari sottoprincipi.

Uno di questi è il principio dell'accuratezza dei dati ed il relativo dovere di aggiornamento degli stessi. Quest'ultimo dovere sarà più o meno importante a seconda della tipologia del trattamento, potendo essere necessario un frequente aggiornamento per alcuni dati, o la semplice raccolta nel caso di dati storici da mantenere immutati nel tempo.

Un altro sottoprincipio è quello della limitata conservazione dei dati. É previsto dall'art. 6(1)(e) della direttiva 95/46/CE e dall'art. 5(e) della Convenzione 108/81, che "*... i dati personali devono essere conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati*".

Superato tale limite temporale i dati dovranno quindi essere cancellati. Questo principio non è tuttavia di stretta applicazione in due casi eccezionali, ossia qualora i dati siano effettivamente anonimizzati, e quando siano mantenuti per finalità storiche, statistiche o scientifiche: devono comunque in quest'ultimo caso essere previste salvaguardie da parte della legge nazionale.

2.1.4 Principio di lealtà nel trattamento dei dati

Il principio della lealtà nel trattamento definisce la relazione tra titolare del trattamento e l'interessato. Questo principio stabilisce un'obbligazione per il titolare di mantenere il soggetto passivo del trattamento informato circa il suo trattamento dei dati, in termini semplici ed accessibili in modo da assicurarne la comprensione.

L'interessato ha inoltre il diritto di essere messo a conoscenza del trattamento dei suoi dati dietro richiesta.

Il titolare deve documentare la legalità e la trasparenza del trattamento, che non deve essere effettuato in segreto o con conseguenze negative non prevedibili dall'interessato.

Inoltre deve mantenere una condotta che aderisca quanto più possibile alla volontà dell'interessato, soprattutto quando la base del trattamento si trova nel consenso di quest'ultimo.

Nel considerare i doveri, nascenti dalla normativa, in capo al titolare del trattamento, il principio della lealtà fa sì che questi debba agire anche oltre i requisiti minimi di legge se ciò sia richiesto da un legittimo interesse del soggetto passivo del trattamento.

2.1.5 Principio dell'accountability

L'organizzazione per la cooperazione e lo sviluppo economico (OCSE) ha adottato nel 2013 linee guida sulla privacy che pongono in primo piano il ruolo dei titolari del trattamento. Queste linee guida vengono riprese dall'*Handbook on European data protection law* nello sviluppare un principio di accountability che preveda come i titolari abbiano la responsabilità di adottare misure rispettose dei principi sul trattamento dei dati come sopra esposti.

La stessa direttiva 95/46, all'art.6(2) dispone che "*Il responsabile del trattamento è tenuto a garantire il rispetto delle disposizioni del paragrafo 1*", il quale riporta i principi generali su cui deve basarsi il trattamento.

Inoltre secondo l'opinione 3/2010 dell'Art.29 Working Party[19] (di cui si tratterà più ampiamente in 2.5.2 Article 29 Working Party), l'essenza del principio dell'accountability si rinviene in due obblighi del titolare del trattamento:

1) mettere in pratica misure che, in circostanze normali, garantiscano che il trattamento aderisca alle norme sulla protezione dei dati;

[19] Article 29 Working Party, Opinione 3/2010 del 13 Luglio 2010 "*the principle of accountability*", WP 173

2) mantenere una documentazione pronta a dimostrare al soggetto passivo del trattamento e all'autorità di supervisione quali misure siano state messe in pratica per aderire alle norme sulla protezione dei dati.

Questo principio richiede quindi che i titolari si attivino per dimostrare un rispetto delle norme, senza aspettare che gli interessati o le autorità di supervisione mettano in mostra le sue mancanze.

2.2 Normativa italiana, Codice in materia di protezione dei dati personali

Il Codice in materia di protezione dei dati personali è un decreto legislativo della Repubblica Italiana emanato il 30 giugno 2003, al n. 196.

Il Codice abroga la precedente legge 675/96, introdotta per rispettare gli Accordi di Schengen ed entrata in vigore nel maggio 1997. Tale ultima legge, insieme alle norme succedute negli anni per effetto della stratificazione normativa in materia sono state riunite nel Testo Unico vigente, entrato in vigore il 1º gennaio 2004.

La legge che ha formato il corpo maggiore del Testo Unico è la l. 31 Dicembre 1996, n. 675 "*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*", che attuò la direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati.

La l. 31 Dic. 1996, n. 675 fu emanata insieme alla l. 31 Dic 1996, n. 676 "*Delega al governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*" che delegava il governo ad emanare, entro 18 mesi dall'entrata in vigore della legge medesima, disposizioni integrative della legislazione in materia di tutela delle

persone e di altri soggetti rispetto al trattamento dei dati personali. I D.lgs potevano riguardare, tra gli altri, semplificazioni di alcuni degli adempimenti introdotti dalla nuova legge, come la notificazione per il trasferimento di dati all'estero.

Infine la legge delega conteneva una delle prime disposizioni legislative concernenti internet e, in generale, le reti telematiche. La legge, infatti, disponeva che il Governo era delegato ad emanare disposizioni volte a stabilire le modalità applicative della legislazione in materia di protezione dei dati personali ai servizi di comunicazione e di informazione offerti per via telematica, individuando i titolari del trattamento di dati inerenti ai servizi accessibili al pubblico e alla corrispondenza privata, nonché i compiti del gestore anche in rapporto alle connessioni con reti sviluppate su base internazionale.

L'esigenza di un testo unico è nata a causa delle numerose modifiche che si sono succedute nell'arco di circa 7 anni. Il Codice è stato ideato con lo scopo di riordinare la materia, ma non è un semplice testo unico: introduce infatti alcune modificazioni ed inserisce e sistematizza la giurisprudenza del Garante.

É una legge che non tende a vietare, quanto a proceduralizzare, ad indicare il modo di utilizzare le informazioni, riservate o meno.[20]

Il trasferimento dei dati all'estero viene trattato al Titolo VII, agli artt. 42-45. Viene essenzialmente riportata la normativa comunitaria, facendo anche formale rinvio nell'art. 44(b) alla direttiva 95/46/CE.

La regola generale prevede il divieto di restrizione del flusso dei dati fra gli stati membri dell'Unione Europea, all'art.42 del Codice. Ciò dà una prima delimitazione del campo di applicazione della normativa, che verrà maggiormente approfondita nel Cap.3.

L'art.43 prevede i casi in cui i trasferimenti esteri sono consentiti, con norme parallele al comma 1 dell'art. 26 della direttiva 95/46/CE. I due articoli differiscono per tecnica legislativa in quanto la normativa italiana prevede una casistica in cui il trasferimento è consentito, mentre quella europea prevede un divieto generale di trasferimento dei dati verso Paesi che non garantiscono tutela adeguata, per poi prevedere una serie di deroghe a tale divieto.

Artt.44 e 45 riprendono infine il concetto di "*adeguatezza del livello di protezione*" dei paesi terzi verso cui i trasferimenti dei dati avranno

[20] Giusella Finocchiaro, "*Privacy e protezione dei dati personali, disciplina e strumenti operativi*", Zanichelli 2012, pagg.25-29

luogo, concetto di origine comunitaria previsto ad oggi dalla Direttiva pocanzi citata. Come si vedrà più avanti, ruolo principale nel giudizio su tale adeguatezza è conferito alla Commissione Europea ma accanto ad essa hanno ruolo preponderante anche le Autorità di Protezione dei Dati dei Paesi Membri, tra cui il Garante per la protezione dei dati personali italiano.

L'espresso riferimento all'autorità del Garante, prevista all'art.44, è di fondamentale importanza, avendo questo un ruolo essenziale in molteplici procedure di trasferimento dei dati all'estero, tra cui Binding Corporate Rules (BCR) e Model Contractual Clauses (MCC). Tale autorità amministrativa indipendente e le procedure di trasferimento estero sottoposte al suo controllo verranno esaminate più approfonditamente nei capitoli a seguire.

2.3 Normativa europea, Direttiva 95/46/CE

Il principale strumento legale dell'Unione Europea sulla protezione dei dati personali è la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995.[21]

Tale direttiva è stata introdotta nel 1995, dopo che molti Stati Membri avevano già adottato una propria normativa in materia. Tuttavia, nonostante la precedente normativa nazionale, la libera circolazione di beni, capitali, servizi e persone nel mercato interno europeo non poteva essere realizzata senza che gli Stati Membri potessero affidarsi ad un'uniforme livello di protezione nella circolazione dei dati.

L'obbiettivo primario di questa direttiva è dunque l'armonizzazione normativa della protezione dei dati a livello nazionale[22], attraverso un livello di specificità delle sue previsioni paragonabile a quello delle allora esistenti normative nazionali.

[21] GU n. L 281 del 23/11/1995 pag. 0031 - 0050
[22] Vedere considerando 1, 4, 7, 8

Prevede la Corte di giustizia dell'Unione europea a tal proposito che:

"*La direttiva 95/46/CE mira … a rendere equivalente in tutti gli Stati membri il livello di tutela dei diritti e delle libertà delle persone riguardo al trattamento dei dati personali. … Il ravvicinamento delle legislazioni nazionali applicabili in materia non deve avere per effetto un indebolimento della tutela da esse assicurata, ma deve, anzi, mirare a garantire un elevato grado di tutela nella Comunità.*

Si è così giudicato che l'armonizzazione delle suddette legislazioni nazionali non si limita quindi ad un'armonizzazione minima, ma sfocia in un'armonizzazione che, in linea di principio, è completa. È in quest'ottica che la direttiva 95/46/CE intende garantire la libera circolazione dei dati personali, pur assicurando un alto livello di tutela dei diritti e degli interessi delle persone cui si riferiscono tali dati". [23]

Inoltre la Corte di Giustizia dell'Unione europea ha giurisdizione nel determinare se uno Stato Membro abbia rispettato le proprie obbligazioni sotto la Direttiva per la protezione dei dati e dà un proprio giudizio preliminare riguardante validità e interpretazione della Direttiva per assicurare la sua effettiva e uniforme applicazione negli Stati Membri.

[23] Corte di Giustizia dell'Unione europea, Procedimenti riuniti C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 Novembre 2011, par. 28-29

Di conseguenza gli Stati Membri dell'UE hanno solo una limitata libertà di manovra nell'implementazione della stessa.

Inoltre non sono solo gli Stati Membri ad essere ad soggetti alla Direttiva 95/46/CE, avendo la normativa un'applicazione territoriale che si estende anche agli Stati parte dello Spazio Economico Europeo, comprendendo Islanda, Liechtenstein e Norvegia.

La Direttiva sulla protezione dei dati è designata per dare sostanza ai principi sul diritto alla privacy già contenuti nella Convenzione 108/81 del Consiglio d'Europa sulla "*protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*" ed espanderli. La circostanza che tutti i 15 Stati Membri dell'Unione europea del 1995 fossero anche parti contraenti della Convenzione 108/81 evitò l'adozione di norme contrastanti nei due strumenti legali.

La Direttiva sfrutta inoltre la possibilità prevista dall'art. 11 della Convenzione 108/81, di aggiungere strumenti di protezione ulteriori.

In particolare l'introduzione di una supervisione indipendente come strumento per incrementare l'effettività delle norme sulla protezione dei dati europei si è rivelata una scelta efficace (di conseguenza questo strumento è stato ripreso dalla normativa del CoE nel 2001 con il Protocollo aggiuntivo alla convenzione 108/81).

Il trasferimento dei dati all'estero viene trattato al Capo IV "*Trasferimento di dati personali verso paesi terzi*", agli artt.25-26.

La tecnica legislativa della direttiva prevede che l'art.25 definisca i principi, e che l'art.26 ponga una serie di deroghe all'articolo precedente.

Tra i principi viene innanzitutto stabilito il concetto di "*protezione adeguata*" del paese destinatario dei dati come requisito per il trasferimento degli stessi, fatte salve le misure nazionali di attuazione delle altre disposizioni della direttiva.

Ruolo centrale nel giudizio sull'adeguatezza del livello di protezione garantito da un paese terzo è della Commissione, in collaborazione con i Paesi Membri, che restano comunque obbligati ad adottare le misure necessarie per conformarsi alle decisioni della prima.

Ciò porta all'armonizzazione delle legislazioni nazionali pur mantenendo uno spazio di manovra minimo tipico dello strumento della direttiva, come visto poco sopra.

L'art. 26 prevede invece una serie di deroghe, che permettono il trasferimento di dati verso Paesi Terzi anche qualora non garantiscano una tutela adeguata, facendo salve eventuali disposizioni contrarie della legislazione nazionale in casi specifici.

La lista delle deroghe è tassativamente prevista al comma 1, ed è materialmente stata fatta propria della legislazione italiana, compresa nel Codice in materia di protezione dei dati personali.

I comma 2 e 3 sono invece dedicati alle autorizzazioni previste dagli Stati Membri, verso paesi che non garantiscano una protezione adeguata, ed alla procedura scaturente da questa modalità di trasferimento, che coinvolge Stati Membri e Commissione.

In aggiunta, anche in materie già coperte della Direttiva, previsioni più dettagliate sono spesso rese necessarie per raggiungere una maggior chiarezza nel bilanciare altri interessi legittimi. Due esempi sono la Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche[24] e la Direttiva 2006/24/CE riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di serivizi e comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modificava la Direttiva 2002/58/CE[25] (Direttiva sulla conservazione dei dati, annullata l'8 Aprile 2014).

[24] OJ Vol 45, 31 Luglio 2002 L. 201, p. 37
[25] OJ Vol 49, 13 Aprile 2006 L. 105, p. 54

2.4 Consiglio d'Europa, Convenzione 108/81 e protocollo addizionale

Con l'emergere delle tecnologie dell'informazione nel 1960, si è sviluppato un crescente bisogno per regole più dettagliate nel tutelare gli individui nella protezione dei loro dati personali. Durante gli anni '70, il Comitato dei Ministri del Consiglio d'Europa adottò varie risoluzioni sulla protezione dei dati personali, riferendosi all'art.8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.[26]

Nel 1981, è stata adottata la Convenzione 108/81 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (da qui Convenzione 108/81)[27], che al giorno d'oggi resta l'unico strumento legale internazionale vincolante nel campo della protezione dei dati.

La Convenzione 108/81 si applica a tutti i trattamenti dei dati effettuati dal settore privato e pubblico (comprendendo così anche il trattamento

[26] Risoluzione del Consiglio d'Europa (73) 22 "*the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*", 26 September 1973; Risoluzione del Consiglio d'Europa (74) 29 "the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector", 20 September 1974

[27] Consiglio d'Europa, "*Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*" CETS n. 108/1981

dei dati per finalità giudiziarie o di polizia). Ha come scopo la protezione degli individui dagli abusi che possono scaturire da raccolta e trattamento dei dati personali, e cerca, al contempo, di regolare il trasferimento transfrontaliero di tali dati.

I principi previsti nella convenzione sono concernenti, in particolare, il trattamento automatizzato dei dati con modalità legali e secondo principi di *fairness*. Riguardano inoltre la qualità dei dati, in particolare la loro adeguatezza, rilevanza, proporzionalità ed accuratezza.

Oltre a prevedere garanzie per raccolta e trattamento di dati personali, la Convenzione 108/81 vieta, in assenza di apposite salvaguardie legali, il trattamento di dati sensibili.

La Convenzione inoltre prevede il diritto dell'individuo di conoscere se vi siano informazioni raccolte su di lui e se necessario chiederne la correzione. Restrizioni ai diritti previsti dalla convenzione sono previsti solo nel caso di prevalenza di ulteriori interessi secondo un procedimento di bilanciamento degli stessi. Si riportano ad esempio gli interessi pubblici della sicurezza o della difesa.

Anche se la Convenzione prevede un libero trasferimento di dati personali tra gli Stati parte della stessa, essa impone restrizioni tra Stati la cui normativa non preveda una protezione equivalente.

Per sviluppare ulteriormente i principi generali e le regole previste nella Convenzione, una serie di raccomandazioni non vincolanti sono state adottate dal Comitato dei Ministri del Concilio d'Europa, in particolare nel settore delle comunicazioni elettroniche.[28]

Tutti gli Stati Membri dell'Unione Europea hanno ratificato la Convenzione 108. Nel 1999, la Convenzione è stata emendata per abilitare l'UE stessa a diventarne parte.[29]

Nel 2001, è stato adottato un Protocollo Addizionale alla Convenzione 108/81,[30] che introduce norme sui flussi di dati transfrontalieri verso Stati non parte della Convenzione, cosiddette "*Third Countries*", e sull'obbligatoria previsione di autorità nazionali di supervisione sul trattamento dei dati.

Ciò ha aperto la strada all'entrata di Paesi non membri del Consiglio d'Europa come firmatari della Convenzione 108/81. Ad oggi, 45 dei 46 firmatari della Convenzione 108 sono Stati Membri del CoE. L'Uruguay, prima nazione non europea, è divenuta parte dalla convenzione

[28] Raccomandazione del Consiglio d'Europa R (95) 4 "*the protection of personal data in the area of telecommunication services, with particular reference to telephone services*"

[29] CoE, Emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Consiglio d'Europa (ETS N. 108) per permettere l'accesso alle Comunità Europee, adottato dal Comitato dei Ministri, a Strasburgo, il 15 Giugno 1999; Art. 23(2) della Convenzione 108 nella sua forma emendata

[30] Consiglio d'Europa, "*Protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri*", CETS n. 181/2001

nell’agosto 2013 ed il Marocco, invitato dal Comitato dei Ministri, è nel processo di formalizzazione dell’accesso.

Da ciò risulta la speranza che la Convenzione 108/81 possa diventare uno standard internazionale ed il suo carattere aperto possa servire come base per promuovere la protezione dei dati a livello globale.

Questa fiducia nella Convenzione ha portato alla decisione di modernizzarla, a seguito di una consultazione pubblica nel 2011, che ha reso possibile confermare i due principali obiettivi di tale lavoro: rinforzare la protezione della privacy nell’area digitale e rafforzare il meccanismo di follow-up.

2.5 Organi indipendenti

Il sistema di protezione dei dati personali previsto da Unione Europea, Concilio d'Europa e normativa nazionale italiana rimarrebbe solo sulla carta se non fosse per un ecosistema di organi che lo complementi affiancandosi ad esso.

Verranno di seguito analizzati due organi indipendenti che svolgono un ruolo essenziale nel rendere efficace la normativa, quale l'Autorità Garante per la protezione dei dati personali italiana, e nel mantenere la normativa al passo con un campo in continua evoluzione come quello della privacy, quale l'Art.29 Working Party.

2.5.1 Garante per la protezione dei dati personali

L'Autorità garante per la protezione dei dati personali, cosiddetto Garante della privacy, è stato istituito dall'art.30 della legge n.675 del 31 Dicembre 1996 sulla "*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*", abrogata ai sensi dell'art.183(1)(a) del Codice in materia dei dati personali. La figura del Garante è dunque ad oggi disciplinata dall'art.53 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003 n. 196).

Il garante opera in piena autonomia ed indipendenza. Tra i suoi compiti, previsti dall'art.154 del Codice, vi è il controllo che i trattamenti di dati siano effettuati nel rispetto della disciplina, il provvedere dietro reclami, segnalazioni e ricorsi presentati dagli interessati, il potere di divieto di trattamenti illeciti e la segnalazione a Parlamento e Governo dell'opportunità di interventi normativi anche a seguito dell'evoluzione del settore.

Tra i compiti rilevanti nel trattamento dei dati da parte di operatori esteri, è da ricordare la partecipazione del Garante nelle procedure sull'approvazione del trasferimento di dati attraverso i modelli di BCR ed

SCC [31] e le funzioni di controllo previste da accordi e convenzioni internazionali.

La figura del Garante viene inoltre espressamente menzionata dalla Convenzione 108/81 del Consiglio d'Europa, che lo prevede quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13.

Tra i suoi recenti impegni vi sono provvedimenti di autorizzazione nazionale di trasferimento dei dati mediante BCR[32], la partecipazione nella revisione della Convenzione 108/81 del Consiglio d'Europa e la continua collaborazione con l'Art.29 Working Party per il nuovo Regolamento in materia di protezione dei dati che sostituirà la Direttiva 95/46/CE.

[31] Garante per la protezione dei dati personali, doc. 1728496 "*Autorizzazione al trasferimento di dati personali del territorio dello Stato verso Paesi non appartenenti all'Unione europea, effettuati in conformità alle clausole contrattuali tipo*"

[32] Garante per la protezione dei dati personali, doc. 1717863 "*Trasferimento di dati personali relativi ai dipendenti e alla clientela verso paesi non appartenenti all'Ue mediante Bcr - provvedimento di autorizzazione nazionale (gruppo Hyatt)*"

2.5.2 Art.29 Working Party

L'art.29 Data Protection Working Party è un organo istituito con la Direttiva 95/46/CE, ed ha carattere consultivo ed indipendente.

Il gruppo è composto da un rappresentante delle autorità di supervisione previsto da ogni Stato Membro europeo, un rappresentante delle autorità create per le istituzioni e gli organi comunitari, ed un rappresentante della Commissione.

L'art.30 della direttiva 95/46/CE ne prevede i compiti, tra cui vi sono funzioni concernenti l'applicazione della normativa sulla protezione dei dati tra gli Stati Membri europei, in modo da contribuire all'uniformità della stessa.

In secondo luogo, il Working Party ha la funzione di formulare, ad uso della Commissione, un parere sul livello di tutela nei paesi terzi. Questa valutazione è strumentale al giudizio sull'adeguatezza della protezione offerta dai paesi verso cui approvare il trasferimento di dati ai sensi dell'art.25 della direttiva 95/46/CE.

Ulteriore compito rilevante nel trasferimento di dati verso paesi terzi è la redazione, ai sensi dell'art 30(6) della Direttiva 95/46/CE di una relazione annuale sullo stato della tutela delle persone fisiche, con

riguardo al trattamento dei dati personali in Paesi terzi. Tale relazione viene trasmessa a Commissione, Parlamento europeo, Consiglio ed è oggetto di pubblicazione.

Al di fuori della direttiva attraverso cui il Working Party è stato istituito, un ulteriore compito viene stabilito dall'art.15 della Direttiva 2002/58/CE nella estensione dei suoi compiti previsti precedentemente anche per quanto concerne la tutela dei diritti e delle libertà fondamentali e degli interessi legittimi nel settore delle comunicazioni elettroniche.

L'insieme di questi poteri hanno permesso al Working Party, fin dalla sua creazione, di essere una colonna portante dell'innovazione del diritto europeo sulla protezione dei dati.

Tra i maggiori lavori nel campo della normativa sul trasferimento estero di dati personali si ricorda lo studio delle Binding Corporate Rules[33] e la successiva spinta per l'adozione di Binding Corporate Rules for Processors (BCR-P), raccomandazioni riguardanti Model Contractual

[33] Art.29 Working Party, Working Document 74 del 3 Giugno 2003 "*Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*", WP74

Clauses[34], ed uno sguardo a soluzioni extralegislative nella sua opinione sul principio dell'accountability[35].

[34] Art.29 Working Party, Explanatory Document del 19 Aprile 2013 "*The Processor Binding Corporate Rules*" WP 204
[35] Art.29 Working Party, Opinione 3/2010 del 13 Luglio 2010 "T*he principle of accountability"* WP 173

3. Ambito di applicazione della normativa

Una volta esposta la normativa alla base del trattamento dei dati personali da parte di operatori esteri, sorge la necessità di individuare l'ambito di applicazione di tale normativa. Non rimane quindi che chiedersi: chi sono gli operatori, e quali sono i dati personali a cui fare riferimento?

Tali dubbi, a prima vista di semplice risoluzione, nascondono in realtà una serie di problematiche, che verranno qui affrontate.

3.1 Criterio della Territorialità

È innanzitutto da considerare che le cautele poste alla base dei trasferimenti esteri di dati hanno alla base una singola ratio: la preoccupazione che dati personali, fuoriusciti dalla sfera di protezione comunitaria, potrebbero non essere opportunamente tutelati in Paesi che non riconoscono alla protezione dei dati personali la stessa importanza che le è data dall'Unione Europea.

Per questo motivo si possono individuare le restrizioni al trasferimento dei dati con un procedimento di esclusione, valutando prima l'ambito entro cui la loro circolazione non può essere limitata.

Recita in merito l'art.1 comma 2 della Direttiva 95/46/CE "*Gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri*".

Nello stesso senso, prevede l'art. 42 comma 1 del Codice in materia di protezione dei dati personali, "*Le disposizioni del presente codice non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea*".

Da queste due disposizioni sembrerebbe che, per esclusione, il trasferimento di dati personali possa essere legittimamente limitato solo verso Stati non membri dell'Unione Europea. Ciò è tuttavia da raccordare con la Decisione 94/1/CECA relativa alla conclusione dell'accordo sullo Spazio Economico Europeo tra gli Stati Membri dell'allora Comunità Europea ed Austria, Finlandia, Islanda, Liechtenstein, Norvegia, Svezia e Svizzera.[36]

Tale accordo mirava a rafforzare le relazioni economiche e commerciali della Comunità Europea con i paesi dell'Associazione Europea di Libero Scambio (AELS) estendendo in parte a questi ultimi le quattro libertà di circolazione del mercato unico.

Da ciò discende che l'ambito di applicazione territoriale odierno della Direttiva 95/46/CE comprende, oltre ai 28 Stati Membri UE, gli Stati non membri dell'UE ma parte dello Spazio Economico Europeo, segnatamente Islanda, Liechtenstein e Norvegia.[37]

E' da ricordare in merito come anche la Convenzione 108/81 del Consiglio d'Europa preveda un'area di libero trasferimento dei dati tra i

[36]Decisione 94/1/CECA del 13 dicembre 1993, OJ 1994 L 1, che entrò in vigore il 1 Gennaio 1994

[37] È importante notare che la libertà di trasferimento tra membri del SEE non comprende finalità che ricadono al di fuori del mercato interno, come quelle investigative e di polizia.

suoi membri, che oltre agli Stati Europei comprendono l'Uruguay (dall'agosto del 2013) ed a breve il Marocco.

Tra i Paesi esteri non ricompresi nell'ambito appena descritto, si dovrà effettuare un'analisi casistica tesa ad individuare la disciplina di applicazione. Alcuni operatori esteri potranno sfruttare accordi internazionali in materia di protezione dei dati personali intercorrenti tra il proprio Stato di stabilimento e l'UE.

Altri operatori potranno avvantaggiarsi di vari strumenti, elaborati dalla normativa europea, in modo da garantire essi stessi una tutela minima dei diritti accettabile per i cittadini europei.

Infine, per i restanti soggetti, sarà applicata la disciplina generale come disposto dalla normativa esaminata nel capitolo precedente.

3.1.1 Case study: Sentenza C-131/12 Google Inc. v Agencia Española de Protección de Datos

Per approfondire il criterio territoriale verrà analizzato un landmark case che nel 2012 chiarì la definizione di operatore estero in tema di trattamento dei dati personali, ed individuò i limiti entro cui esso è sottoposto alla normativa europea.

La sentenza è la C-131/12 Google Inc. v Agencia Española de Protección de Datos.

Il 5 Marzo 2010, Mario Costeja González, cittadino spagnolo, presentò un reclamo all'Agencia Española de Protección de Datos (AEPD), contro La Vanguardia (un quotidiano spagnolo), Google Spain SL ("Google Spain"),[38] e Google Inc.

Al tempo del ricorso, un utente internet che abbia cercato il nome di Costeja González attraverso il motore di ricerca di Google avrebbe ricevuto link a due pagine di un quotidiano spagnolo che annunciavano la vendita all'asta di immobili connessa ad un pignoramento effettuato

[38] Google Spain è una società sussidiaria di Google Inc. che agisce come rappresentante commerciale di quest'ultima, principalmente per le sue attività pubblicitarie in Spagna. Google Spain non esegue trattamenti di dati in quanto estranea alle funzioni del motore di ricerca di Google, quindi quando ricevette il reclamo dell'attore Costeja González, lo inoltrò a Google Inc., fornitore del servizio del motore di ricerca

per la riscossione coattiva di crediti previdenziali del sig. Costeja González.

Nel suo reclamo, Costeja González richiese che il giornale spagnolo rimuovesse il suo nome dal proprio articolo, e che Google Spain eliminasse od occultasse i suoi dati personali così che non sarebbero apparsi più tra i risultati di ricerca. [39]

Costeja González sostenne che, considerato il procedimento di pignoramento concluso, riferimenti a questo mancassero del criterio della rilevanza dei dati personali,[40] ed egli avesse dunque diritto alla loro rimozione.[41]

L'AEPD negò il reclamo di Costeja González contro il giornale,[42] ma lo garantì contro Google.

L'Agenzia per la protezione dei dati spagnola sostenne che gli operatori di motori di ricerca rientrano nella definizione di "*responsabile del trattamento*" come definita dalla Direttiva 95/46/CE, e che Google Spain e Google Inc. fossero di conseguenza obbligati a rimuovere link ai dati su richiesta dell'interessato.

[39] Sentenza C- 131/12, par. 15
[40] Rifacendosi al concetto di rilevanza dei dati, art.6 Direttiva 95/46/CE
[41] Rimedio garantito dall'art.12 Direttiva 95/46/CE
[42] Sentenza C-131/12, par. 16 Il giornale non aveva infatti alcuna obbligazione a rimuovere gli annunci, essendo stati pubblicati legalmente ed inoltre dietro richiesta governativa per dare pubblicità alla procedura di pignoramento

Google Spain e Google Inc si appellarono al Tribunal Supremo (Corte Suprema spagnola), che rinviò una serie di questioni alla Corte di Giustizia dell'UE con un procedimento di domanda pregiudiziale riguardo la corretta interpretazione della Direttiva 95/46/CE.

Tra le varie questioni ne fu presentata una di fondamentale importanza per l'interpretazione dell'ambito di applicazione della Direttiva riguardo gli operatori esteri. È Google, come società non facente parte dell'Unione europea, soggetta alla portata territoriale della Direttiva?

La decisione della Corte di Giustizia dell'UE fu affermativa, rivelandosi consistente con l'interpretazione della direttiva da parte dell'AEPD.

Nell'esaminare se Google fosse soggetta alla direttiva, la corte determinò innanzitutto la sua qualità di titolare del trattamento.[43]

Proseguì inoltre con l'affermare che la sola presenza di Google Inc. in Spagna, attraverso la sussidiaria Google Spain, fosse sufficiente a rendere Google Inc. soggetta alla direttiva.

[43] Sentenza C-131/12, par. 28. Viene constatato che "*esplorando Internet in modo automatizzato, costante e sistematico alla ricerca delle informazioni ivi pubblicate, il gestore di un motore di ricerca «raccoglie» dati siffatti, che egli «estrae», «registra», «organizza»[…] «conserva» […] «comunica» e «mette a disposizione» […]"*. Poiché tali operazioni sono contemplate in maniera esplicita e incondizionata all'articolo 2, lettera b), della direttiva 95/46, esse devono essere qualificate come «trattamento» ai sensi di tale disposizione, senza che rilevi il fatto che il gestore del motore di ricerca applichi le medesime operazioni anche ad altri tipi di informazioni e non distingua tra queste e i dati personali.

La Corte, sostenuta tra gli altri anche dal governo italiano, sentenziò che nonostante l'intero trattamento dei dati sia avvenuto al di fuori dalla Spagna, Google Spain comporti nella pratica uno "stabilimento" di Google Inc. sul territorio europeo. Google Spain infatti effettua promozione e vendita degli spazi pubblicitari di Google Inc. entro il territorio nazionale spagnolo e la pubblicità è parte essenziale dell'attività commerciale del gruppo Google. Ciò rende le due entità "strettamente connesse".[44]

Google Spain comporta dunque un effettivo stabilimento di Google Inc. in Spagna, rendendo quest'ultimo soggetto alla direttiva.[45]

Questa decisione si rifà direttamente all'art.4 comma 1(a) della Direttiva 95/46/CE, nel punto in cui prevede che "*ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro*".

Le questioni poste dal Tribunal Supremo alla Corte di Giustizia dell'UE comportavano anche l'identificazione della legge spagnola come applicabile nel caso di specie anche secondo la lettera c) dello stesso art.

[44] Sentenza C- 131/12, par. 46
[45] Sentenza C- 131/12, par. 60

4 comma 1, che prevede tale applicazione al trattamento dei dati "*il cui responsabile, non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea.*"

Ciò avviene, a detta dell'AEPD, attraverso gli strumenti di web spiders e crawler utilizzati da Google per analizzare la rete al fine di procedere all'indicizzazione delle informazioni contenute in pagine web alloggiate su server situati in uno Stato membro europeo. La questione dell'utilizzo di strumenti sul territorio europeo da parte di operatori esteri non è stata tuttavia affrontata dalla Corte di Giustizia dell'UE, avendo nel suo procedimento logico già riscontrato la legge spagnola come applicabile nel caso specifico in un punto precedente della sentenza.

Ultimo caso, per quanto riguarda il criterio territoriale, è quello in cui il responsabile del trattamento non stabilito nel territorio di uno Stato membro dell'UE, sia comunque stabilito in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico. È infatti così previsto dall'art. 4 comma 1(b) della Direttiva 95/46/CE.

3.2 Case study - Sentenza C-101/01 Criminal proceedings against Bodil Lindqvist

Abbiamo sin qui analizzato cosa si intende per operatore estero, rimane ora da definire la nozione di "*trasferimento*" dei dati.

Ci si avvarrà del procedimento C-101/01 avente ad oggetto la domanda di pronuncia pregiudiziale proposta dinanzi alla Corte di Giustizia Europea dal Göta hovrätt (Corte d'appello della regione del Götaland) nel procedimento penale contro Bodil Lindqvist, signora di nazionalità svedese.

La sig.ra Lindqvist, nell'esercizio della sua funzione di formatrice di cresimandi nella parrocchia di Alseda, creò a casa sua e con un personal computer, alcune pagine internet allo scopo di consentire ai parrocchiani che si preparavano alla cresima di ottenere facilmente le informazioni di cui avevano bisogno. Dietro richiesta, l'amministratore del sito della Chiesa di Svezia creò un collegamento ipertestuale fra tali pagine e il suddetto sito.

Le pagine in questione contenevano informazioni sulla sig.ra Lindqvist e su 18 suoi colleghi della parrocchia, compreso il loro nome e cognome. La sig.ra Lindqvist inoltre descrisse le mansioni dei colleghi e le loro

abitudini nel tempo libero, ed in molti casi la loro situazione familiare e recapiti telefonici.

Dell'esistenza di tali pagine la sig.ra Lindqvist non informò i colleghi, né chiese il loro consenso, né dichiarò la loro realizzazione alla Datainspektion (ente pubblico svedese per la protezione dei dati).

Il Pubblico ministero svedese promosse dunque un procedimento penale nei confronti della sig.ra Lindqvist per violazione della Personunppgiftslag (Legge svedese sui dati personali, che recepì la direttiva 95/46/CE), che si concluse con la sua condanna a vario titolo, tra cui per aver trasferito verso Paesi terzi dati personali sottoposti ad un trattamento non autorizzato.[46]

Riguardo tale trasferimento, nella sentenza furono riportate le considerazioni dei governi di Paesi Bassi e Regno Unito. Il primo ricordò come la nozione di "trasferimento" non sia definita dalla direttiva 95/46/CE, e ritenne, da un parte, che tale nozione debba essere intesa come riferita a un atto mirante deliberatamente a trasferire dati personali dal territorio di uno Stato membro verso un paese terzo e, dall'altra, che non possa essere operata una distinzione tra le diverse

[46] In violazione dell'art. 33 della Personunppgiftslag

forme nelle quali i dati sono resi accessibili a terzi.[47] Il Regno unito affermò invece che "*l'art. 25 della direttiva 95/46 riguarda i trasferimenti di dati verso paesi terzi e non la loro accessibilità a partire da paesi terzi. La nozione di "trasferimento" implicherebbe la trasmissione di un dato da una persona che si trova in un luogo preciso ad una terza persona che si trova in altro luogo*".[48]

La Corte di Giustizia Europea rilevò come le pagine internet della sig.ra Lindqvist non contenessero i meccanismi tecnici che avrebbero consentito l'invio automatico dei dati trattati a persone che non avessero deliberatamente cercato di accedere a dette pagine.

Ne consegue che i dati personali che giungono al computer di un soggetto che si trova in un paese terzo, provenienti da una soggetto che li ha condivisi attraverso un sito Internet, non sono dati trasferiti direttamente tra queste due persone, ma attraverso l'infrastruttura informatica del web hosting provider presso il quale la pagina è caricata.[49]

Se ne deduce che per aversi un "*trasferimento*" di dati ai sensi della Direttiva 95/46/CE, occorre una trasmissione diretta degli stessi da una

[47] Sentenza C-101/01, Par 54
[48] Sentenza C-101/01, par 55
[49] Sentenza C-101/01, par 60-61

persona ad un'altra, anche attraverso invio automatico ad una pluralità di persone, purché esse siano determinate. La condivisione di dati attraverso la possibilità di accesso agli stessi da parte di una pluralità di persone indeterminate, come avviene attraverso l'utilizzo di internet, non rientra dunque nel campo del trasferimento dei dati verso Paesi terzi.

Se così non fosse, la condivisione di dati su internet sarebbe da considerare necessariamente un trasferimento verso tutti i paesi terzi in cui esistono i mezzi tecnici necessari per accedere ad Internet, e di conseguenza il regime speciale previsto dal Capo IV della suddetta direttiva diverrebbe necessariamente, per quanto riguarda le operazioni su Internet, un regime di applicazione generale. Infatti, non appena la Commissione constatasse, ai sensi dell'art. 25 comma 4 della Direttiva 95/46, che via sia anche un solo paese terzo in cui non sia garantito un livello di protezione adeguato, gli Stati membri sarebbero tenuti ad impedire qualsiasi condivisione su Internet di dati personali da parte dei propri cittadini.[50]

[50] Sentenza C-101/01, par 69

4. Restrizioni dei trasferimenti dei dati verso Paesi esteri

4.1 Criteri della restrizione

Si è visto nel Cap. 3.1 come la norma generale per quanto riguarda i trasferimenti di dati personali nello Spazio Economico Europeo preveda la libertà di circolazione degli stessi. Una limitazione potrà avvenire solo in casi eccezionali.

Nel trasferimento verso Paesi terzi la norma, invece, si capovolge. Nella generalità dei casi si dovrà provvedere alla restrizione degli stessi, che saranno permessi solo in presenza di requisiti determinati tassativamente.[51]

Dispone in tal senso l'art.25 comma 1 della Direttiva 95/46/CE, prevedendo che "*Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo*

[51] Considerando 57 Direttiva 95/46/CE

soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato".

Mancando tale requisito dell'adeguatezza del livello di protezione del Paese terzo in cui si intende trasferire dati personali, il comma 4 del medesimo art. 25 prevede che "*gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati della stessa natura verso il paese terzo in questione*"

Lo stesso concetto di "adeguatezza" si riscontra nella protocollo addizionale alla Convenzione 108/81 del Consiglio d'Europa, in cui si prevede che "*each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer*".

4.2 Lo standard di adeguatezza e la sua interpretazione

Essendo il requisito dell'adeguatezza al centro del discorso sul trasferimento dei dati personali verso gli operatori esteri, è bene individuare nello specifico i suoi caratteri.

Innanzitutto è da considerare come si parli di adeguatezza, e non di equivalenza. La distinzione semantica rende possibile onorare tale requisito attraverso una varietà di modi di implementazione della normativa sulla protezione dei dati. È perciò possibile che sia riconosciuta come adeguata anche la protezione offerta da una normativa che, in quanto estera, non abbia punti di contatto con quella europea. Ciò contribuisce a rendere il sistema più flessibile.

L'art.29 Working Party ricorda, nel suo Working Document 12 del 1998, che la Direttiva 95/46/CE prese direttamente spunto dalla Convenzione 108/81 del Consiglio d'Europa, che a sua volta riportò le linee guida OECD del 1980. [52] L'insieme dei principi su cui si basano questi documenti erano nel 1990 già stati fatti propri anche dall'ONU.[53]

[52] OECD Council Recommendation "*concerning guidelines governing the protection of privacy and transborder flows of personal data*", 23 Settembre 1980

[53] Risoluzione ONU 45/95 "Guidelines for the Regulation of Computerized Personal Data Files", 14 Dicembre 1990

Ciò serve a dimostrare che esiste un certo consenso internazionale riguardo ciò che dovrebbe ad oggi costituire la tutela dei dati personali.

Un consenso sulla carta è tuttavia da ritenere marginale, se non è accompagnato da un sistema di protezione dei dati che applichi in modo efficace tali principi estremamente generali. In Europa tale sistema è stato assicurato da una direttiva che permette l'armonizzazione delle legislazioni nazionali, complementata da autorità di supervisione con funzioni di monitoraggio, decisionali e sanzionatorie.

Al di fuori dell'Unione Europea è molto più raro trovare una disciplina procedurale che assicuri il rispetto delle norme alla base della protezione dei dati personali.

Se si considerano infatti gli impegni presi dagli Stati contraenti attraverso la Convenzione 108/81 e le linee guida OECD, ne risulta un quadro fatto solamente di soft law. Spesso l'unica obbligazione prevista da parte dei contraenti è che tali norme vengano "*prese in considerazione*" nella legislazione nazionale.[54]

Ne risulta che, secondo l'Art.29 Working Party, un'analisi significativa del concetto di adeguatezza deve comprendere due elementi base: il

[54] OECD Council Recommendation "concerning guidelines governing the protection of privacy and transborder flows of personal data", 23 Settembre 1980, Part 4 – National Implementation

contenuto delle norme applicabili e la capacità di assicurarne l'effettiva applicazione.

L'analisi può prendere come punto di partenza una lista minima di condizioni, che si basi sui principi della protezione dei dati personali facenti parte della direttiva. Queste condizioni minime dovranno essere accompagnate da requisiti procedurali e di applicazioni a loro volta adeguati.

In alcuni casi saranno necessari requisiti addizionali, mentre in altri la protezione sarà da ritenere adeguata anche in mancanza di alcuni di essi. Ciò è dipendente dai rischi che il trasferimento pone sugli interessati in casi specifici.

Tra i principi generali già esposti nel Capitolo 2.1 ve ne è inoltre da aggiungere un ulteriore, da applicare nell'analisi dell'adeguatezza.

E' questo il principio della restrizione dei trasferimenti ulteriori, che prevede come ulteriori trasferimenti di dati personali dal titolare originario del trattamento siano permessi solo qualora il ricevente dei trasferimenti ulteriori sia anch'esso soggetto a norme che garantiscano un adeguato livello di protezione. Le uniche eccezioni ammesse devono essere in linea con le deroghe previste dall'art.26 comma 1 della Direttiva 95/46/CE. In mancanza di questo requisito si potrebbe

sfruttare un Paese terzo come "*ponte*", grazie al quale trasferire dati in Paesi mancanti un'adeguata garanzia di protezione.

Per quanto riguarda invece il sistema di applicazione della normativa, l'Art.29 Working Party distingue tre obbiettivi a cui deve tendere un sistema che voglia definirsi completo:

1) assicurare un buon livello di rispetto delle norme, in cui ci sia un alto grado di consapevolezza degli operatori per le loro obbligazioni, e conoscenza dei propri diritti da parte dei soggetti interessati dal trattamento dei dati. Un importante ruolo in questo campo è assunto da un insieme effettivo di sanzioni;

2) provvedere supporto ai soggetti interessati nell'esercizio dei propri diritti, che deve essere caratterizzato da efficacia, rapidità e costi non proibitivi. Questo è solitamente permesso da un meccanismo istituzionale che permetta una risoluzione dei reclami in indipendenza;

3) provvedere ad un appropriato rimedio per la parte lesa, qualora le norme non siano state rispettate.

Per quanto riguarda le Nazioni contraenti della Convenzione 108/81, si presume l'adeguatezza della loro protezione dei dati. Tuttavia, per ogni Paese contraente ma non membro dell'UE, è necessario che esso sia

anche il paese finale del trasferimento, o dia garanzie di non trasferire tali dati in Paesi che non offrano protezione adeguata, non essendo questo requisito previsto dalla Convenzione. Inoltre deve esistere un meccanismo che assicuri il rispetto delle norme, essendo lasciata dalla Convenzione molta libertà in materia.

Tra le problematiche nell'analisi dell'adeguatezza, vi è da considerare che molti Paesi esteri non prevedono una protezione dei dati personali uniforme in tutti i settori normativi. Per esempio gli USA prevedono una disciplina più o meno approfondita a seconda dell'area normativa (è ad esempio presente una tutela dei dati personali specificamente nel campo del noleggio video attraverso il Video Privacy Protection Act [55]). Si aggiungono difficoltà quando certi Stati federali come USA, Canada, Australia, presentano una differente normativa per ogni stato che ne faccia parte.

[55] Public Law 100-618 5 Novembre 1988

4.2.1 Modalità dell'accertamento dell'adeguatezza

Consiglio e Parlamento Europeo hanno conferito alla Commissione il potere di determinare, sulla base dell'Art.25 Comma 6 della Direttiva, se un Paese terzo presenta un adeguato livello di protezione dei dati personali.

Il procedimento decisionale, con una modalità che è tecnicamente definita una procedura del comitato (o comitatologia) è descritto dall'Art. 31 comma 2 della Direttiva, e comprende:

1) una proposta dalla Commissione;

2) l'opinione delle autorità di protezione dei dati personali degli stati membri e dell'EDPS (European Data Protection Supervisor), secondo il framework individuato dall'Art.29 Working Party;

3) l'approvazione, da parte del Comitato Articolo 31 (composto da rappresentanti degli Stati membri) del progetto proposto dalla Commissione;

4) l'adozione della decisione da parte del Collegio dei Commissari in seno alla Commissione.

In qualunque momento, Parlamento Europeo e Consiglio possono richiedere che la Commissione mantenga, modifichi o ritiri la sua decisione sull'adeguatezza qualora questa abbia ecceduto i poteri che le sono stati conferiti dalla Direttiva.

L'effetto di tale decisione è il libero trasferimento di dati personali dai Paesi Membri dell'UE e del SEE al paese la cui protezione dei dati è stata ritenuta adeguata.

Un accertamento dell'adeguatezza della Commissione europea ha effetto vincolante. Tutti gli Stati membri dell'UE e dello Spazio Economico Europeo saranno dunque tenuti ad ammettere il libero trasferimento di dati personali senza controlli ed autorizzazioni da parte delle autorità nazionali.

I Paesi che non sono ritenuti a protezione adeguata non finiscono comunque esplicitamente o implicitamente in una "*lista nera*". Semplicemente sarà da considerare come manchino linee guida generali verso tali Paesi.

La Commissione Europea è inoltre in grado di valutare parti del sistema legale di tali Paesi, o limitarsi a determinati settori. La commissione ha

effettuato un accertamento dell'adeguatezza, per esempio, concernente soltanto la normativa commerciale privata del Canada.[56]

Esistono inoltre una serie di accertamenti dell'adeguatezza riguardanti singoli accordi intervenuti tra UE e Paesi esteri riguardanti trasferimenti di un singolo tipo di dati, come trasmissione dei PNR (Passenger Name Records) da compagnie aeree alle autorità di controllo di confine di Paesi esteri.

Pratiche più recenti di trasferimento di dati basati su accordi speciali tra EU e Paesi terzi in genere evitano la necessita di accertamenti dell'adeguatezza del livello di protezione dei dati personali di tali Paesi, con la presunzione che l'accordo in sè sia sufficiente a garantire la tutela di tipi specifici di dati.[57]

Una delle più importanti decisioni sull'adeguatezza in realtà non è relazionata ad una serie di previsioni legali. Piuttosto riguarda regole, non dissimili da un Codice di Condotta, conosciute come i Safe Harbour Privacy Principles. Questi principi furono elaborati tra EU ed USA per le

[56] Commissione Europea 2002, Decisione 2002/2/CE del 20 Dicembre 2001 conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio "*riguardante l'adeguatezza della protezione fornita dalla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (Canadian Personal Information Protection and Electronic Documents Act)*"

[57] Per esempio l'accordo tra USA ed UE riguardo il trasferimenti di PNR all'US Department of Homeland Security (OJ 2012 L 215, pp. 5–14) o l'accordo tra USA e UE riguardo trattamento e trasferimento di Financial Messaging Data dall'Unione Europea agli Stati Uniti d'America utilizzati per il Terrorist Finance Tracking Program (OJ 2010 L 8, pp. 11–16)

società statunitensi. La membership nel Safe Harbour è ottenuta con impegno volontario dichiarato all'US Commerce Department e documentato in una lista pubblicata da tale dipartimento. Tale strumento legale per i trasferimenti di dati verso operatori statunitensi troverà approfondimento nel Cap 6.

Fino ad oggi è stato approvato il libero trasferimento di dati verso Andorra, Argentina, Canada, Svizzera, Isole Faroe, Guernsey, Israele, Isola di Man, Isola di Jersey, Nuova Zelanda, Uruguay e Stati Uniti (nei limiti dei principi di protezione dei dati del Safe Harbour dell'US Department of Commerce).[58]

[58] Andorra 2010/625/EU, Argentina 2003/490/EC, Canada 2002/2/EC, Svizzera 2000/518/EC, Isole Faroe 2010/146/EU, Guernsey 2003/821/EC, Israele 2011/61/EU, Isola di Man 2004/411/EC, Isola di Jersey 2008/393/EC, Nuova Zelanda 2013/65/EU, Uruguay 2012/484/EU, Stati Uniti d'America 2000/520/EC

4.3 Deroghe generali alle restrizioni del trasferimento dei dati verso Paesi terzi

L'art.26 comma 1 della Direttiva prevede un numero limitato di situazioni in cui sia permesso derogare al requisito di adeguatezza della protezione dei dati personali già discusso.

Queste deroghe, tassativamente previste, riguardano per la maggior parte casi in cui i rischi dell'interessato siano relativamente minori o dove vi siano altri interessi in gioco (pubblici o dell'interessato stesso) che abbiano priorità rispetto al diritto alla protezione dei dati personali.[59]

Come deroghe ad un principio generale, queste devono essere interpretate in modo restrittivo.

Ed è proprio riguardo la loro interpretazione che l'Art.29 Working Party ha elaborato due documenti in materia. Il "*Working Document 12 - Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*" effettuò nel 1998 una prima analisi delle deroghe. Tuttavia, negli anni successivi si notò una divergente interpretazione tra gli Stati Membri riguardo alcune di esse, soprattutto a seguito del Report sull'implementazione della Direttiva 95/46/CE del

[59] Come previsto anche dall'art.2 comma 2(a) del Protocollo addizionale alla Convenzione 108/81

2003.[60] Il Working Party decise quindi di approfondire le linee guida sull'interpretazione dell'art.26 nel 2005, attraverso il "*Working Document 114 - Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*".

A seguire si elencano le varie deroghe previste dall'art. 26 comma 1 e la loro più recente interpretazione comunitaria.

A) La persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto.

La prima di queste regole copre i casi in cui l'interessato abbia dato il suo consenso al trasferimento estero dei dati. Un importante punto da tenere a mente è che il consenso, seguendo la definizione dell'art.2(h) della Direttiva, deve essere libero, specifico ed informato.

Il requisito dell'informazione è particolarmente importante, essendo richiesto che l'interessato sia correttamente informato sui particolari rischi che comporta un trasferimento verso un paese mancante dei requisiti di adeguatezza previsti dall'art.25 della Direttiva. In mancanza dell'informativa, la deroga non troverà applicazione.

[60] Commissione Europea COM(2003) 265 "First report on the implementation of the Data Protection Directive (95/46/CE)", 15 Maggio 2003

Considerato che il consenso debba essere chiaro, ogni dubbio sul fatto che esso sia stato dato rende la deroga non applicabile. Ciò toglie validità al consenso implicito, come nei casi in cui il soggetto sia stato informato e non abbia obiettato al trasferimento.

B) Il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento o per l'esecuzione di misure precontrattuali prese a richiesta di questa, oppure
C) Il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo.

Seconda e terza deroga coprono i trasferimenti necessari per l'esecuzione del contratto tra interessato e titolare del trattamento (o implementazione di misure precontrattuali), ovvero per la conclusione o esecuzione di un contratto concluso nell'interesse della persona interessata, tra responsabile del trattamento e un terzo. Queste deroghe appaiono potenzialmente molto ampie, ma la loro applicazione pratica, secondo il Working Party,[61] è limitata dal cd. "*necessity test*". Tutti i dati trasferiti devono essere necessari per l'esecuzione del contratto. Se

[61] Art.29 Working Party, Working Document 12 del 24 Luglio 1998 *"Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive*", WP 12

vengono trasferiti dati ad altri scopi, anche correlati al contratto in senso ampio (ad esempio per marketing), la deroga viene a mancare.

Per quanto riguarda situazioni precontrattuali, si dovranno includere solo quelle ad iniziativa dell'interessato (come la richiesta di informazioni per un particolare servizio) e non quelle risultanti da approcci di marketing effettuati dal responsabile del trattamento.

A dispetto di tali limiti, seconda e terza deroga non sono senza impatto. Saranno spesso applicabili, per esempio, ai trasferimenti necessari per la prenotazione di biglietti aerei o al trasferimento di dati personali necessari per operazioni bancarie internazionali.

D) Il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per costatare, esercitare o difendere un diritto per via giudiziaria.

La quarta deroga prevede due elementi disgiunti. Il primo copre i trasferimenti necessari o prescritti dalla legge per la salvaguardia di un interesse pubblico rilevante. Ciò potrebbe coprire certi trasferimenti di dati tra pubbliche amministrazioni, anche se si deve far attenzione, secondo l'Art.29 Working Party,[62] a non interpretare questa previsione

[62] Art.29 Working Party, Working Document 12 del 24 Luglio 1998 "*Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive*", WP 12

in maniera eccessivamente ampia. Un semplice interesse pubblico non sarà sufficiente ma dovrà avere caratteristica di "*rilevanza*". Tra i casi compresi in tale regola, il considerando 58 della Direttiva 95/46/CE prende ad esempio gli scambi internazionali di dati tra le amministrazioni fiscali o doganali oppure tra i servizi competenti per la sicurezza sociale.

Il secondo elemento della deroga D) riguarda i trasferimenti che hanno luogo nel contesto dei procedimenti giudiziari internazionali, nello specifico per costatare, esercitare o difendere un diritto per via giudiziaria.

E) Il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata

La deroga comprende i trasferimenti necessari per la protezione di interessi vitali dell'interessato. Un ovvio esempio è il trasferimento urgente di cartelle cliniche in Paesi terzi, quando un turista che abbia precedentemente ricevuto un trattamento medico nell'UE sia in condizioni di pericolo vitale. E' da ricordare in ogni caso la definizione del considerando 31 della Direttiva, che definisce l'interesse vitale come un "*interesse essenziale alla vita della persona interessata*". Questo esclude

normalmente, secondo il Working Party, interessi patrimoniali, finanziari o familiari.

F) Il trasferimento avvenga a partire da un registro pubblico il quale, in forza di disposizioni legislative o regolamentari, sia predisposto per l'informazione del pubblico e sia aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione

La sesta ed ultima deroga riguarda i trasferimenti provenienti da registri predisposti dalla legge per l'informazione del pubblico, nella misura in cui siano rispettate le condizioni previste dalla legge per la consultazione nel caso specifico.

La ratio di questa deroga si basa sul presupposto che quando un registro in uno Stato Membro sia reso disponibile al pubblico o a chi dimostri un legittimo interesse per la consultazione, non sia rilevante che chi abbia il diritto a consultarlo sia situato in una Paese terzo, e l'atto della consultazione, che è in sè un trasferimento di dati, non dovrebbe limitare il trasferimento di tali informazioni.

Il considerando 58 della Direttiva rende chiaro come non sia permesso il trasferimento della totalità dei dati o delle categorie di dati contenuti in

tali registri. Date queste restrizioni la deroga non dovrebbe essere considerata come una deroga generale al trasferimento di dati da registri pubblici. Per esempio è chiaro che il trasferimento di massa di dati da pubblici registri per scopi commerciali non sia permesso, così come l'analisi di registri pubblici per attività di profiling (analisi comportamentale a fini investigativi).

Inoltre, sempre secondo il considerando 58, il trasferimento di un registro destinato ad essere consultato dalle persone aventi un interesse legittimo dovrebbe essere possibile soltanto su richiesta di tali persone e qualora esse ne siano i destinatari.

Oltre alle deroghe qui analizzate, sono previsti infine ulteriori casi in cui sia possibile il trasferimento di dati verso Paesi che non garantiscono un livello di protezione adeguata, ossia Binding Corporate Rules, Standard Contractual Clauses e trasferimenti di singoli tipi di dati specificamente ammessi dalla normativa europea. Questi strumenti, per la loro complessità, saranno analizzati approfonditamente nel prossimo capitolo.

5. Trasferimento di dati attraverso strumenti legali

Le decisioni sull'adeguatezza del livello di protezione dei dati di un Paese estero, come analizzato in precedenza, possono riguardare uno specifico settore normativo e, di conseguenza, ammettere trasferimenti basati su singole tipologie di dati.

È proprio questo che avviene attraverso accordi internazionali bilaterali stipulati tra UE e Paesi esteri per il trasferimento di *Passenger Name Record* (PNR) ed attraverso il *Terrorist Finance Tracking Programme* (TFTP).

Ciò permette ad operatori che vogliano trasferire specifici dati in Paesi mancanti dei requisiti generali di adeguatezza della tutela dei dati personali di poter basare tale trasferimento su accordi ad hoc.

Come già anticipato, nel caso non ci si possa appoggiare ad uno di questi strumenti ovvero ad una delle deroghe previste dall'art. 26 comma 1 della Direttiva 95/46/CE, dovrà essere il titolare del trattamento estero stesso a garantire la protezione dei dati trasferiti.

È infatti previsto dall'art.26 comma 2 della Direttiva 95/46/CE che "s*alvo il disposto del paragrafo 1, uno Stato membro può autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un*

paese terzo che non garantisca un livello di protezione adeguato […], qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi; tali garanzie possono segnatamente risultare da clausole contrattuali appropriate".

Questa modalità di trasferimento è prevista anche dal Protocollo addizionale alla Convenzione 108/81, all'art.2 comma 2(b) " *[…] each Party may allow for the transfer of personal data: if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law*".

Entrambi gli articoli fanno riferimento ad appropriate clausole contrattuali da cui risultino le salvaguardie poste dal titolare del trattamento. Questo genere di clausole sono state tipizzate dalla giurisprudenza ed analizzate dall'Art.29 Working Party, riconducendole oggi alla tipologia delle Standard Contractual Clauses (SCC) e Binding Corporate Rules (BCR).

5.1 Accordi per singoli tipi di dati: Passenger Name Records (PNR)

A seguire l'attacco terroristico dell'11 Settembre 2001 in territorio statunitense, la sicurezza dei voli aerei è stata resa più stringente. Gli USA posero restrizioni a tutti i voli in arrivo e partenza, richiedendo che i PNR (Passenger Name Records) raccolti dalle compagnie aeree fossero resi disponibili al Department of Homeland Security (DHS) ed in particolare al Bureau of Customs and Border Protection (CBP). Queste richieste furono dirette anche verso i voli provenienti dall'Unione Europea, con evidente incidenza sulla protezione dei dati personali dei passeggeri comunitari.

I PNR comprendono infatti una pluralità di informazioni sui passeggeri, quali nome, indirizzo, date dei voli, itinerario, informazioni dei ticket, dettagli di pagamento, posto a sedere ed informazioni sul bagaglio. Questi dati sono conservati nelle banche dati di prenotazione e controllo delle partenze da parte delle compagnie di volo e gli sviluppi tecnologici più recenti ne hanno permesso l'utilizzo in maniera sistematica.

Per assicurare che i PNR europei inviati al DHS siano adeguatamente protetti ai sensi della Direttiva 95/46/CE, nel 2004 fu adottato un PNR

package[63] comprendente una valutazione dell'adeguatezza da parte della Commissione sulla protezione dei PNR trasferiti ed una decisione del Consiglio europeo sulla conclusione dell'accordo tra UE ed USA in merito al trasferimento.

Tale accordo fu annullato in breve tempo dalla Corte di Giustizia Europea, attraverso i procedimenti unificati C-317/04 e C-318/04.[64]

La sentenza C-317/04 riguardò la decisione della Commissione 2004/535/CE sull'adeguatezza della protezione dei PNR in USA. La Corte determinò che la Commissione non era competente, essendo il campo della sicurezza pubblica esterno all'ambito di applicazione della Direttiva 95/46/CE. E' infatti previsto in generale all'art.3 comma 2 della Direttiva, che "*Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali: effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario […] e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello*

[63] Decisione del Consiglio Europeo 2004/496/CE del 17 Maggio 2004 "*conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection*", OJ 2004 L 183, p. 83. Decisione della Commissione 2004/535/CE del 14 Maggio 2004 "*adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection*", OJ 2004 L 235, pp. 11-22

[64] Corte di Giustizia Europea, procedimenti unificati C-317/04 e C-318/04, "*European Parliament v. Council of the European Union*", 30 Maggio 2006, par. 57, 58 e 59, in cui la Corte sentenziò che entrambe le decisioni di adeguatezza e l'accordo relative al trattamento dei dati erano al di fuori dell'ambito della Direttive 95/46/CE

Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale".

Nonostante questa conclusione, la Corte notò come i dati PNR siano in origine raccolti da compagnie aeree e non agenzie governative. Tuttavia la raccolta ed il trasferimento di tali dati sono richiesti dalla legge per ragioni di pubblica sicurezza non correlate alla loro prestazione del servizio di trasporto verso i passeggeri.

D'altra parte la sentenza C-317/04 chiarì che la decisione del Consiglio 2004/496/CE sulla conclusione dell'accordo per il trasferimento dei PNR tra UE ed USA non poteva trovare una base legale nell'art. 95 del Trattato che istituisce la Comunità Europea, essendo essenzialmente rilevante solo per le decisioni consiliari riguardanti il mercato interno.

Da tali due sentenze ne risulta un quadro normativo mancante di una base legale adeguata che tuteli i dati PNR trasferiti in territorio americano.

A seguito dell'annullamento di tale PNR package UE ed USA firmarono dunque due accordi separati con un duplice obiettivo: stabilire una base legale per il trasferimento dei dati PNR e provvedere un'adeguata

protezione degli stessi nel paese ricevente. L'accordo ad oggi in vigore è stato firmato nel 2012.[65]

Tale nuovo accordo offrì miglioramenti significativi. Vennero innanzitutto limitate e chiarite la finalità per cui le informazioni possono essere utilizzate, in particolare per gravi crimini internazionali e terrorismo, ed è stato stabilito un tempo limite entro cui i dati possono essere conservati: dopo sei anni dovranno essere anonimizzati.

Se i dati dovessero essere usati impropriamente l'interessato avrà inoltre il potere di ricorso amministrativo o giudiziario secondo la legge statunitense. Lo stesso ha diritto di accesso ai propri dati PNR e di rettifica da parte del DHS, inclusa la possibilità di rimozione nel caso i dati siano inaccurati.

L'accordo resterà in vigore per 7 anni, fino al 2019.

I piani futuri europei in tema di PNR includono lo sviluppo di linee guida globali[66], l'edificazione di uno schema EU-PNR[67] ed il negoziato di accordi con ulteriori Paesi terzi.[68]

---

[65] Decisione del Consiglio 2012/472/UE del 26 Aprile 2012 "*conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security*" OJ 2012 L 215/4. Il testo dell'accordo è in allegato alla decisione, OJ 2012 L 215, pp. 5-14.

[66] Vedere in particolare la Comunicazione della Commissione del 21 Settembre 2010 "*global approach to transfers of Passenger Name Record (PNR) data to third countries*", COM(2010)492. Vedere inoltre Art.29 Working Party (2010), Opinion 7/2010 "*European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries"*, WP 178.

[67] Proposta per una Direttiva del Parlamento Europeo e del Consiglio del 2 Febbraio 2011 "*use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*",

Tali nuovi negoziati seguiranno il sentiero già tracciato con l'accordo statunitense, che presenta questi punti principali:

a) i dati PNR possono essere inviati all'US Department of Homeland Security, Bureau of Customs and Border Protection, solo per finalità di prevenzione, individuazione, investigazione e persecuzione dei reati legati al terrorismo ed altri crimini transnazionali punibili con la pena della reclusione da un minimo di 3 anni. L'accordo contiene la definizione di tali crimini per una migliore definizione del suo ambito;

b) i dati PNR trasferiti e nella disponibilità degli operatori statunitensi sono dettagliatamente indicati in un allegato all'accordo stesso;

c) le compagnie aeree trasferiscono i dati PNR al DHS con un "*push system*" (tali dati vengono inviati direttamente dalle compagnie dietro richiesta del DHS, senza intermediari e quindi con maggior protezione);

COM(2011)32. Nell'Aprile 2011, il Parlamento Europeo richiese all'European Union Agency for Fundamental Rights (FRA) un'opinione in merito a tale proposta ed il suo rispetto della Carta dei diritti fondamentali dell'Unione. Vedere FRA 14 Giugno 2011 Opinione 1/2011 "*Passenger Name Record*".

[68] Al momento eistono accordi PNR solamente verso USA, Australia e Canada (quest'ultimo in fase di rinegoziazione per sostituire l'accordo del 2006 attualmente in vigore).

d) tutti i passeggeri, indipendentemente da nazionalità e Paese di residenza, hanno accesso ad un ricorso giudiziario ed amministrativo in relazione alle decisioni del DHS;

e) l'implementazione dell'accordo è revisionata periodicamente. In aggiunta, l'accordo deve essere valutato congiuntamente dalle parti 4 anni dopo la sua entrata in vigore;

f) i dati sensibili devono essere filtrati o mascherati e non dovranno essere ulteriormente trattati, a meno di circostanze eccezionali in cui la vita di un individuo possa essere in pericolo. In ogni caso i dati PNR non contengono normalmente dati sensibili;

g) i dati possono essere conservati per 5 anni in un "*active database*" e fino a 10 anni in un "*dormant database*".[69] Oltre questo periodo i dati conservati devono essere resi completamente anonimi;

[69] La qualità di "active" o "dormant" indica il grado di attività della banca dati, e ne determina il livello di sicurezza necessario. Il "dormant database" è infatti soggetto a "*controlli supplementari, tra cui un numero più ristretto di personale abilitato nonché un livello di approvazione da parte delle autorità di vigilanza più elevato per accedervi. I PNR contenuti nella banca dati inattiva non sono ripersonalizzati, salvo per operazioni di pubblica sicurezza e in tal caso solo in relazione a un caso, una minaccia o un rischio identificabili*", Decisione 2012/472/UE della Commissione Europea del 26 Aprile 2012, "*relativa alla conclusione dell'accordo tra gli Stati Uniti d'America e l'Unione europea sull'uso e il trasferimento delle registrazioni dei nominativi dei passeggeri al dipartimento degli Stati Uniti per la sicurezza interna*" , art.8(3)

h) il DHS ha l'obbligo di assicurare la condivisione delle informazioni analitiche ottenute dai PNR europei con le autorità competenti UE, ed in casi appropriati con Europol ed Eurojust, in modo da rafforzare la cooperazione nel campo giudiziario e di polizia;

i) l'accordo resta in vigore per 7 anni e può essere rinnovato per un seguente periodo di 7 anni.

L'implementazione dell'accordo è stata esaminata nel 2010 ed è stato provato come i dati PNR siano idonei alla finalità di supporto alla lotta contro il terrorismo. Inoltre le norme riguardanti i diritti dei passeggeri hanno trovato piena applicazione, considerato che gli Stati Uniti hanno trasposto le proprie obbligazioni verso l'UE nella legislazione nazionale.
Sono da riconoscere tuttavia delle problematiche legate ad un recente trend statunitense che, attraverso "*memorandum of understanding*", ha stretto nel Febbraio 2008 un accordo con la Repubblica Ceca[70] che permette a quest'ultima di far parte del *Visa Waiver Program* statunitense in cambio dei dati PNR dei voli in partenza, di fatto

[70] Memorandum of understanding between the ministry of the interior or the Czech Republic and the Department of Homeland Security of the United States of America regarding the United States Visa Waiver Program and related enhanced security measures, 27 Febbraio 2008

bypassando l'accordo PNR europeo. Sono inoltre stati rilevanti contatti dello stesso tenore con Regno Unito, Estonia, Germania e Grecia.[71]

[71] Statewatch, Marzo 2008

5.1.1 Accordo SWIFT

La seconda tipologia di dati, espressamente prevista dal "*Terrorist Finance Tracking Programme*"[72] è quella SWIFT.

Questi dati hanno origine dalla società belga per il Worldwide Interbank Financial Telecommunication (SWIFT), responsabile per la maggior parte dei trasferimenti globali di denaro da parte delle banche europee. Essa possiede un centro secondario di trattamento dei dati negli USA e fu da tale Paese confrontata con una richiesta di divulgazione di dati all'US Department of the Treasury per finalità investigative nell'ambito del finanziamento terrorismo.[73]

Da una prospettiva europea, non era presente una base legale sufficiente per la divulgazione di dati così sostanziali, soprattutto considerato come tali dati erano accessibili negli Stati Uniti solo per via di un centro SWIFT secondario. Un accordo speciale tra US e UE, lo

[72] Programma dell'US Treasury Department in collaborazione con la CIA, elaborato a poca distanza dall'attacco terroristico dell'11 Settembre 2001 e rivelato dal New York Times nel Giugno 2006 riguardo l'accesso allo SWIFT transaction database

[73] Vedere in tale contesto Art.29 Working Party, Opinione 14/2011 del 13 Giugno 2011 "*data protection issues related to the prevention of money laundering and terrorist financing"*, WP 186; Art.29 Working Party, Opinione 10/2006 del 22 Novembre 2006 "*processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT)",* WP 128; Autorità per la protezione dei dati personali del Belgio (Commission de la protection de la vie privée) Decisione del 9 Dicembre 2008, "*Control and recommendation procedure initiated with respect to the company SWIFT scrl*'

SWIFT Agreement, è quindi intervenuto nel 2010 per provvedere la necessaria base legale ed un'adeguata protezione.[74]

Secondo tale accordo, i dati finanziari raccolti da SWIFT potranno essere comunicati all'US Treasury Department per le finalità della prevenzione, investigazione, individuazione o persecuzione del terrorismo e del suo finanziamento.

L'US Treasury Department potrà richiedere dati finanziari da SWIFT, a condizione che la richiesta:

a) identifichi nella maniera più chiara possibile i dati finanziari

b) comprovi la necessità dei dati

c) sia il più possibile precisa, in modo da minimizzare la quantità di dati richiesti

d) non richieda dati riguardanti la Single Euro Payments Area (SEPA)

L'Europol riceve copia di ogni richiesta dell'US Treasury Department e verifica che siano stati rispettati i principi dello SWIFT Agreement.[75] Se tale rispetto delle norme viene confermato, SWIFT dovrà comunicare i

[74] Decisione del Consiglio 2010/412/EU del 13 Luglio 2010 "*conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program",* OJ 2010 L 195, pp. 3 e 4. Il testo dell'accordo è allegato alla decisione, OJ 2010 L 195, pp. 5-14

[75] Il Joint Supervisory Body dell'Europol ha condotto controlli sulle attività dell'Europol in quest'area, I risultati sono disponibili su "*http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en"*, visitato il 09/02/2015

dati finanziari direttamente all'US Treasury Department. Quest'ultimo ha l'obbligo di conservare i dati in modo adeguatamente sicuro e permettere l'accesso ai soli analisti per l'investigazione del terrorismo, evitando che siano interconnessi con ogni altro database.

In generale, i dati finanziari ricevuti da SWIFT potranno essere conservati per non più di 5 anni. I dati finanziari rilevanti per investigazioni o procedimenti giudiziari specifici potranno essere mantenuti per il tempo necessario.

È concesso all'US Treasury Department di trasferire informazioni dai dati SWIFT a specifiche forze dell'ordine, di pubblica sicurezza o di contro-terrorismo purché siano mantenute le stesse finalità previste per la loro raccolta.

Qualora l'ulteriore trasferimento dei dati finanziari riguardi un cittadino o residente di uno stato membro UE, ogni comunicazione alle autorità di un Paese terzo sarà soggetta al previo consenso dell'Autorità di protezione dei dati competente nello Stato membro. In tal caso una particolare eccezione è prevista quando la condivisione dei dati sia essenziale per la prevenzione di una minaccia seria ed immediata alla pubblica sicurezza.

Il rispetto dei principi dello SWIFT Agreement è monitorato da supervisori indipendenti, uno dei quali è nominato dalla Commissione

europea, ed i soggetti interessati dal trattamento hanno diritto di ottenere conferma che i loro diritti siano stati rispettati dalla competente autorità europea per la protezione dei dati. Hanno inoltre diritto di rettifica o rimozione dei dati raccolti e conservati dall'US Treasury Department qualora siano in violazione delle salvaguardie poste dall'art.5 dello SWIFT Agreement, "*Safeguards Applicable to the Processing of Provided Data*". In ogni caso, il diritto d'accesso degli interessati può essere soggetto a limitazioni. Qualora l'accesso sia negato, il soggetto interessato deve essere informato per iscritto del rifiuto e del suo diritto ad un ricorso amministrativo o giudiziario negli Stati Uniti.

Lo SWIFT Agreement è valido per 5 anni, fino ad Agosto 2015. Si estenderà automaticamente per seguenti periodi di un anno a meno che una parte non notifichi l'altra, almeno 6 mesi in anticipi, dell'intenzione di non estendere l'accordo.

I benefici portati dall'accordo SWIFT sono stati recentemente analizzati in un report,[76] a seguito del quale si è discusso della possibile adozione di un EU Terrorist Finance Tracking System (EU TFTS), soprattutto riguardo alla sua necessità, proporzionalità, convenienza economica e rispetto dei diritti fondamentali. Come risulta dalla valutazione della

[76] "*Report on the value of TFTP Provided Data*" 27 Novembre 2013

Commissione conclusa con la Comunicazione del 27 Novembre 2013, in questo momento non è ancora stata dimostrata chiaramente la necessità di un tale programma.

5.2 Standard Contractual Clauses

Sia la Direttiva 95/46/CE che la Convenzione 108/81 fanno menzione di Standard Contractual Clauses (SCC), ovvero clausole contrattuali tipo, previste per formare la base di un contratto tra chi trasferisce dati personali e un operatore estero stabilito in un Paese che non fornisce un'adeguata protezione dei dati personali ai sensi dell'art.25 della Direttiva 95/46/CE. Queste clausole permettono al titolare del trattamento stesso di garantire l'adeguatezza della protezione di tali dati, essendo il loro inserimento in un contratto considerato garanzia sufficiente al fine del trasferimento.

La procedura di adozione delle clausole standard da parte della Commissione è, similarmente a quella relativa alle decisioni sull'adeguatezza, prevista dall'art. 31 comma 2 della Direttiva 95/46/CE e prevede la comitatologia.[77] Passando invece al contesto del Consiglio d'Europa, il Comitato consultivo della Convenzione 108/81 non ha

[77] Tale competenza le è stata conferita dall'art. 26 comma 4 della Direttiva 95/46/CE nel prevedere che "*Qualora la Commissione decida […] che alcune clausole contrattuali tipo offrono garanzie sufficienti […], gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.*"

tipizzato le clausole standard ma ha preparato una guida alla loro stesura.[78]

È comunque da ricordare che l'esistenza di clausole contrattuali standard nel framework europeo non proibisce agli operatori di formulare altre clausole contrattuali ad hoc. Tali clausole non standard devono anche esse, in ogni caso, garantire un livello adeguato di protezione dei dati.

Per quanto riguarda la varietà di SCC, esistono diversi set, da adottare a seconda della qualifica dell'importatore estero dei dati. Per i trasferimenti da titolare del trattamento europeo ad un importatore estero qualificato anch'esso come titolare sono previsti due insiemi di clausole. Il primo è stato implementato dalla Commissione con la Decisione 2001/497/CE del 15 Giugno 2001, a cui è allegato.[79]

Il secondo insieme di clausole è stato aggiunto il 27 Dicembre 2004 con la Decisione 2004/915/CE[80] a seguito della presentazione di un insieme alternativo di clausole contrattuali da parte di un consorzio di imprenditori (tra cui Camera di commercio internazionale (ICC),

[78] Consiglio d'Europa, Comitato consultivo della Convenzione 108/81 (2002), "*Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data*".

[79] Garante per la protezione dei dati personali italiano, doc. web n. 42156, "*Autorizzazione al trasferimento verso Paesi senza adeguato livello di protezione*", 10 ottobre 2001

[80] Garante per la protezione dei dati personali italiano, doc. web n. 1151949, "Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso paesi terzi", 9 Giugno 2005

European Information and Communications Technology Association (EICTA), Confederation of British Industry (CBI)).

Se invece l'importatore dei dati è qualificato come responsabile del trattamento, si applicheranno clausole contrattuali apposite previste in origine dalla Decisione 2002/16/CE, in seguito abrogata e sostituita dalla Decisione 2010/87/UE.[81]

Questo ultimo caso è particolarmente importante se si considerano le necessità degli operatori economici moderni. È infatti frequente che le società europee si appoggino ad operatori esteri che offrano servizi di cloud computing, outsourcing, application service providing (ASP), software as a service (SaaS) o Human Resources Information System (HRIS). Tutti casi in cui i dati del cliente vengono conservati in banche dati rese disponibili dal fornitore del servizio. L'importanza nel loro uso ha reso le clausole titolare-responsabile al centro della recente normativa e dello studio dottrinale. In particolare l'Art.29 Working Party ha cercato di dare risposta alle domande più frequenti in materia nel Luglio 2010 attraverso il Working Document 176.

La discussione si è inizialmente concentrata sulla distinzione tra titolare e responsabile del trattamento, che talvolta può essere flebile e andrà

[81] Garante per la protezione dei dati personali, doc. web n. 1728496, "*Autorizzazione al trasferimento di dati personali del territorio dello Stato verso Paesi non appartenenti all'Unione europea, effettuati in conformità alle clausole contrattuali tipo, di cui all'allegato alla decisione della Commissione europea del 5 febbraio 2010, n. 2010/87/UE*", 27 maggio 2010

valutata caso per caso. È ad esempio possibile che l'importatore agisca come titolare in relazione ad alcuni dati e responsabile in relazione ad altri. L'Art.29 Working Party, ha pubblicato un'opinione sulla distinzione tra tali due figure nel febbraio 2010, direttamente a seguire la Decisione della Commissione sulle clausole titolare-responsabile.[82]

Le SCC sono determinate con Decisione della Commissione e contengono un allegato con le clausole standard ed uno da compilare per le parti, con i loro dettagli, i dati trasferiti, le modalità di trattamento dei dati, l'organizzazione ed i dettagli tecnici delle misure di sicurezza che saranno implementate dall'importatore.

Mentre il tenore letterale delle clausole standard resta il medesimo in ogni Stato membro UE, esistono diversi approcci per quanto riguarda i requisiti formali: talune giurisdizioni nazionali prevedono come sufficiente l'accordo tra le parti, altre richiedono l'invio di tale accordo alla competente autorità garante per la protezione dei dati, altre ancora la previa approvazione da parte di quest'ultima. Il Garante per la protezione dei dati personali italiano ha previsto in proposito che la

[82] Art.29 Working Party, Opinione 1/2010 del 16 Febbraio 2010 *"the concepts of "controller" and "processor"",* WP 169

copia del contratto relativo al trasferimento e le altre informazioni necessarie debbano essere fornite solo su sua richiesta.[83]

Tra le recenti problematiche legate alle clausole contrattuali standard titolare-responsabile, va analizzata la possibilità dell'importatore dei dati di subcontrattare il trattamento, inserita nella normativa con la Decisione della Commissione 2010/87/UE.

Il subcontratto va inteso in senso ampio: la normativa trova applicazione anche qualora la terza parte abbia solamente accesso ai dati, in toto o a parte di essi.

La validità del subcontratto è inoltre legata a due requisiti: il consenso dell'esportatore e l'imposizione al subresponsabile degli stessi termini contrattuali previsti nel trasferimento estero.

a) Consenso

Il consenso al subcontratto del trattamento dei dati deve essere fornito dall'esportatore in un documento separato dall'accordo contenente le clausole contrattuali standard, così che le modifiche alla lista dei subresponsabili non influisca su quest'ultimo, eliminando ulteriore

[83] Garante per la protezione dei dati personali italiano, doc. web n. 1151949, "*Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso paesi terzi*", 9 Giugno 2005, in quanto fa riferimento all'art. 157 del Codice in materia di protezione dei dati personali

burocrazia quando sia necessario la notifica o l'approvazione da parte dell'autorità locale di protezione dei dati.

Frequentemente l'esportatore acconsentirà al subcontratto di determinati trattamenti come il mantenimento dei server, la conservazione dei dati o l'amministrazione delle banche dati da parte del soggetto subresponsabile, identificato da ragione sociale ed indirizzo. Talvolta, per questione di flessibilità, l'importatore dei dati può ottenere un consenso più ampio, come per il subcontratto a qualunque società affiliata. All'esportatore sarà in ogni caso inviata copia di ogni subcontratto concluso, come previsto dalla clausola 5(j).

Alternativamente le parti possono decidere che l'importatore debba semplicemente notificare l'esportatore riguardo l'intenzione di affidarsi ad un certo subresponsabile, ed il consenso sarà implicitamente dato qualora l'esportatore non obietti entro un periodo previsto previamente dalle parti.

b) Imposizioni delle condizioni contrattuali sul subresponsabile

La seconda condizione consiste nell'imposizione degli stessi obblighi gravanti sull'importatore anche sul subresponsabile. In una nota alla clausola 11(1) si prevede come questo requsito possa essere soddisfatto

anche attraverso la co-sottoscrizione da parte del subresponsabile del contratto intervenuto tra esportatore ed importatore dei dati.

Il Working Party ha tuttavia riconosciuto come ciò presenti vari svantaggi, tra cui:

a) In molti casi l'importatore non subcontratta l'intero trattamento dei dati, ma solo parte di esso. In tal caso resterebbe poco chiaro fino a che punto gli allegati firmati, che contengono informazioni specifiche su dati trasferiti, finalità del trattamento, misure tecniche ed organizzative di sicurezza, si applicherebbero al subresponsabile.

b) La co-sottoscrizione può comportare un procedimento dispendioso qualora il subresponsabile si avvalga a sua volta di subcontratti, meccanismo esplicitamente ammesso dalla normativa. Il tal caso tutti i soggetti coinvolti dovranno co-firmare a loro volta il contratto, ed in aggiunta rivelare l'esistenza della relazione con operatori europei.

c) La comprensione delle clausole direttamente applicabili al subresponsabile diviene per esso di più difficile comprensione, dovendo individuarle tra la totalità delle altre clausole.

d) Una co-sottoscrizione potrebbe essere costruita in modo tale che il subresponsabile sia obbligato non solo verso il proprio partner contrattuale, ma anche verso l'esportatore dei dati, nei confronti del quale non ha alcuna relazione.

Per questi motivi appare preferibile che importatore e subresponsabile prevedano un accordo separato, che potrà essere previsto come sottostante ad un contratto di fornitura di servizi. Va comunque considerato che, visto l'obbligo dell'importatore di fornire il subcontratto all'esportatore (clausola 5(j)) e, dietro richiesta, ai soggetti interessati dal trattamento (clausola 5(g)), l'accordo dovrebbe essere formalmente separato da contratti sottostanti in modo da evitare la divulgazione di termini commerciali.

Per rendere più semplice il dovere amministrativo del notificare l'accordo all'esportatore, si può prevedere un meccanismo semplificato: copie elettroniche dei subcontratti possono essere rese disponibili online su un server sicuro, e notificate regolamente all'esportatore dei dati. Questo meccanismo permetterebbe all'importatore di rispettare la propria obbligazione di mantenere una lista dei subcontratti aggiornata annualmente.

Per quanto riguarda i diritti dell'interessato dal trattamento, questi possono essere fatti valere nei confronti dell'esportatore, come previsto dalla clausola 3, in qualità di terzo beneficiario. L'interessato potrà rifarsi su importatore dei dati e subresponsabile solo in mancanza

dell’esportatore, perché scomparso o abbia giuridicamente cessato di esistere.

La stessa disciplina si applica nel caso l’interessato abbia subito un pregiudizio per la violazione degli obblighi da parte di esportatore, importatore o subresponsabile, con l’opzione di sottoporre la controversia alla mediazione di un terzo indipendente, all’autorità di controllo o agli organi giurisdizionali del Paese dell’esportatore (clausole 6-7).

È previsto, all’art.157 del Codice in materia di protezione dei dati personali, che sia comunicata al Garante per la protezione dei dati personali la scelta effettuata in caso di controversia non risolta in via amichevole e sottoposta all'esame di un soggetto diverso da esso o dall'autorità giudiziaria.

Sia importatore che subresponsabile, secondo la clausola 8(2), devono permettere il controllo da parte dell’autorità garante per la protezione dei dati personali del Paese in cui sia stabilito l’esportatore dei dati. Tali controlli si applicano alle stesse condizioni a cui sarebbe sottoposto l’esportatore secondo la sua normativa locale. Al termine dell’attività di trattamento, sia importatore che subresponsabile devono restituire e

distruggere tutti i dati ricevuti, certificando l'avvenuta distruzione all'esportatore ai sensi della clausola 12(1).

Un importante punto di discussione nel periodo seguente la Decisione 2010/87/UE per i trasferimenti titolare-responsabile riguardò il subcontratto tra un responsabile del trattamento che agisce sul territorio europeo in nome e per conto del titolare ed un subresponsabile estero, quindi una sorta di SCC responsabile-responsabile.

L'Art.29 Working Party, nelle sue risposte alle domande più frequenti in materia trovò tre soluzioni:

a) sottoscrizione delle clausole direttamente tra titolare del trattamento e subresponsabile estero, senza coinvolgimento del responsabile;

b) sottoscrizione delle clausole tra responsabile del trattamento e subresponsabile, attraverso mandato in nome e per conto del titolare;

c) sottoscrizione di un contratto ad hoc tra titolare del trattamento e responsabile che dia tale potere a quest'ultimo, previa approvazione dell'autorità garante del Paese del titolare.

Il Garante chiarì la situazione attraverso il provvedimento n. 342 del 15 Novembre 2012, prescrivendo "*al titolare del trattamento stabilito nel*

territorio dello Stato, il quale abbia designato un responsabile stabilito nell'Unione europea che intenda affidare, a sua volta, il trattamento dei dati ad un altro responsabile stabilito in un Paese terzo che non assicuri un livello di protezione adeguato, di conferire al responsabile con sede nella Unione europea un apposito mandato […] per la sottoscrizione delle clausole contrattuali tipo […]; resta comunque ferma la facoltà, per il titolare del trattamento che intenda trasferire i dati personali senza avvalersi del mandato, di chiedere all'Autorità una specifica autorizzazione".[84]

[84] Le motivazioni dietro tale scelta si possono rinvenire nella relazione annuale 2012 del Garante per la protezione dei dati personali

5.3 Binding Corporate Rules

Alcune società multinazionali, a seguito della Direttiva 95/46/CE, hanno dimostrato un forte interesse verso quello che l'Art.29 Working Party definì nel 2003 una sorta di "codice di condotta per trasferimenti internazionali".[85]

Tali gruppi societari, per la complessità della loro struttura mondiale, hanno sostenuto che la possibilità di iniziative unilaterali accompagnate da solide garanzie sia una risorsa da sfruttare nel panorama europeo della protezione dei dati personali.

Da questa necessità nascono le Binding Corporate Rules (BCR), ossia le regole vincolanti d'impresa, che permettono il trasferimento di dati tra tutte le società partecipanti al gruppo richiedente la loro approvazione, garantendo un'adeguata protezione dei dati oggetto dei trasferimenti.

Tale strumento non va considerato come l'unico od il migliore per il trasferimento di dati personali tra le società partecipanti al gruppo, ma come uno strumento in aggiunta a quelli già esistenti.

[85] Art.29 Working Party, Working Document del 3 Giugno 2003 "*Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*", WP74

Nella comparazione con le Standard Contractual Clauses si può immediatamente notare come la differenza maggiore si riscontri sul tema della flessibilità e personalizzazione.

Mentre le SCC sono una soluzione predefinita e standardizzata, ogni BCR ha bisogno di essere predisposta fin dal principio tenendo a mente i bisogni particolari dello specifico gruppo societario richiedente. Inoltre, mentre le prime sono utilizzabili senza alcuna particolare implementazione, le seconde sono basate su un'organizzazione per la protezione dei dati che deve essere già insita nei rapporti intra-gruppo.

Per definizione le BCR sono globali, quindi nessuna distinzione territoriale deve essere prevista in merito alla loro applicazione. Le regole devono applicarsi generalmente per tutto il gruppo societario indipendentemente dal luogo di stabilimento delle partecipanti o dalla nazionalità dei soggetti interessati dal trattamento dei dati.

Tuttavia non si può individuare il gruppo societario se prima non si definisca la sua nozione. Ciò può rivelarsi problematico, poichè l'ampiezza del termine può variare da una Paese all'altro, fino a corrispondere a realtà piuttosto differenti: da società multinazionali dominate da una forte struttura gerarchica a conglomerati di società che agiscono ognuno con un gran margine di indipendenza l'una dall'altra;

da gruppi societari che condividono simili attività economiche e quindi di trattamento dei dati, a gruppi che operano sul lato opposto dello spettro. Ovviamente queste differenze in struttura ed attività influiscono su applicabilità, design e finalità delle BCR, e ciò deve essere tenuto a mente nella presentazione delle stesse di fronte all'autorità di protezione competente.

Per gruppi non strutturati con una forte gerarchia, le BCR si rivelano spesso uno strumento poco adatto. La diversità tra i loro membri e l'ampiezza delle finalità nel trattamento dei dati renderebbe molto difficile rispettare i requisiti e le limitazioni previste. Per essi sarebbe necessario differenziare sottogruppi interni al gruppo societario, prevedere forti limitazioni e condizioni per i trasferimenti di dati e modellare di conseguenza le regole vincolanti. In altre parole, se un prodotto finale dovesse risultare accettabile secondo l'art.26(2) della Direttiva, certamente sarebbe molto differente dalle BCR descritte nei documenti dell'Art.29 Working Party.

Individuare con precisione i limiti del gruppo societario è essenziale anche per l'applicazione della disciplina sui trasferimenti ulteriori, ossia quei trasferimenti da membri del gruppo societario non stabiliti nell'UE a società al di fuori del gruppo. Questi sono possibili solo attraverso la previsione delle Clausole Contrattuali Tipo già trattate.

In questo caso, oltre alle clausole, deve essere specificato che a seguito del trasferimento ulteriore, i dati potrebbero essere trattati da un titolare che non è sottoposto alle BCR e stabilito in un Paese che non garantisce un adeguato livello di protezione dei dati.

Elemento essenziale per garantire un'adeguata tutela dei trasferimenti verso Paesi terzi è poi la vincolatività delle norme, fatta valere sia internamente al gruppo che esternamente da parte dei terzi.

La valutazione della natura vincolante delle BCR implica una valutazione comprensiva della loro legalità così come dell'effettività nella pratica. Coloro che chiedono l'approvazione delle BCR dovranno garantire che ogni membro del gruppo rispetti le regole, di solito attraverso una previsione della responsabilità per la società capogruppo o con un codice di condotta interno accompagnato da accordi intragruppo.

Come per le SCC, gli interessati dal trattamento dei dati coperti dalle finalità delle BCR acquistano la qualità di terzi beneficiari. Ciò avviene secondo diverse basi legali: per gli effetti legali discendenti da un impegno unilaterale (qualora previsto dalla legge nazionale) ovvero attraverso accordi contrattuali tra i membri del gruppo.

Come terzi beneficiari, tali soggetti hanno diritto al rispetto delle regole sia attraverso reclamo all'autorità di protezione dei dati competente che procedendo con azione legale presso la Corte del Paese scelto

dall'interessato tra due opzioni: quella dello Stato Membro da cui ha origine il trasferimento ovvero il Paese della società capogruppo europea o della società partecipante al gruppo a cui è stata delegata la responsabilità per la protezione dei dati.

L'ampiezza dei diritti dei terzi beneficiari dovrebbero essere pari a quella garantita dalla Decisione della Commissione 2001/947/CE sulle Standard Contractual Clauses nei confronti di esportatore ed importatore dei dati.

La vincolatività di cui si tratta talvolta presenta limitazioni legate alla legislazione nazionale estera. Pertanto le BCR dovrebbero contenere una chiara previsione che indichi i casi in cui un membro del gruppo societario abbia ragione di credere che la legislazione nazionale a lui applicabile potrebbe contrastare con la sua capacità di rispettare le proprie obbligazioni ed avere un effetto negativo sostanziale sulle garanzie da queste previste. In tal caso deve informare prontamente la capogruppo nell'UE o il membro UE del gruppo delegato con la responsabilità di protezione dei dati (a meno che sia impossibilitato a ciò dalla legge, come per i divieti della legge penale allo scopo di preservare la riservatezza di un'investigazione).

Riguardo gli aggiornamenti delle regole, l'Art. 29 Working Party riconosce come i gruppi societari siano entità mutevoli i cui membri e le cui pratiche possano cambiare col tempo e quindi potrebbero non essere perfettamente corrispondenti alla realtà del tempo in cui l'autorizzazione per le BCR sia stata rilasciata. Gli aggiornamenti sono possibili, senza necessità di un nuovo procedimento di approvazione delle BCR, a certe condizioni:

a) Nessun trasferimento di dati personali sia effettuato verso un nuovo membro finché l'esportatore dei dati non abbia assicurato che il nuovo membro è effettivamente vincolato dalle regole e possa assicurarne il rispetto

b) Una persona o un dipartimento del gruppo ben specificato dovrebbe mantenere una lista aggiornata dei membri, tenere traccia di ogni modifica delle regole e provvedere le necessarie informazioni in merito ad ogni interessato o autorità di protezione dei dati che ne faccia richiesta

c) Ogni aggiornamento alle regole o modifica alla lista dei membri deve essere comunicata annualmente all'autorità di protezione dei dati che ha

garantito l'autorizzazione, accompagnata da una breve spiegazione che lo giustifichi.

Passando alla capacità del gruppo di assicurare il rispetto delle regole, l'Art.29 Working Party individua varie condizioni che permettono di valutarne il livello di adeguatezza complessivo:[86]

1) Previsioni che conducano al rispetto delle norme

Ci si aspetta che le regole creino un sistema che garantisca consapevolezza delle stesse sia all'interno che all'esterno dell'UE. La predisposizione da parte della capogruppo di una policy interna per il trattamento dei dati deve essere considerata solo come il primo passo nel procedimento per garantire sufficienti salvaguardie previste dall'art.26(2) della Direttiva. Il gruppo societario richiedente deve anche essere in grado di dimostrare che questa policy sia conosciuta, compresa ed effettivamente applicata da parte di tutto il gruppo e che i dipendenti ricevano una formazione adeguata.

[86] Art.29 Working Party, Working Document del 3 Giugno 2003 "*Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*", WP74

2) Adeguatezza dei controlli

Le regole devono prevedere, su base regolare, dei controlli interni o in alternativa la supervisione esterna da parte di enti di controllo accreditati che comunichino i risultati all'amministrazione della società capogruppo. Le autorità di protezione dei dati dovranno ricevere una copia di tali report.

Le regole devono anche indicare che il dovere di cooperazione tra Autorità di protezione dei dati (indicato al punto 4) potrebbe anche richiedere l'ammissione di controlli effettuati da ispettori delle autorità stesse ovvero ispettori indipendenti che agiscono per conto dell'autorità.

3) Gestione dei reclami

Deve essere istituito un sistema attraverso cui i singoli reclami siano risolti da un dipartimento chiaramente indicato. I cd. data protection officers o ogni persona che tratti tali reclami deve beneficiare di un appropriato livello di indipendenza nell'esercizio di tali funzioni. L'uso di metodi alternativi di risoluzione delle controversie, col possibile coinvolgimento di autorità di protezione dei dati quando appropriato, dovrebbe essere promosso nel rispetto della legge nazionale.

4) Il dovere di cooperazione con le autorità di protezione dei dati

Come previsto in nel Working Document 12 dell'Art.29 Working Party, [87] uno dei più importanti elementi per valutare l'adeguatezza di un sistema di autoregolazione è il livello di supporto disponibile per i singoli soggetti interessati dal trattamento: "A key requirement of an adequate and effective data protection system is that an individual faced with a problem regarding his personal data is not left alone, but is given some institutional support allowing his/her difficulties to be addressed"

Questo è uno dei più importanti elementi delle BCR: le regole devono contenere chiari doveri di cooperazione con le autorità di protezione dei dati così che gli interessati possano beneficiare dal supporto istituzionale menzionato.

5) Responsabilità

Le regole dovrebbero indicare che i soggetti interessati possono beneficiare dei rimedi e responsabilità previsti dagli articoli 22 e 23 della Direttiva (o simili previsioni che riportino tali articoli nella legislazione nazionale degli Stati Membri) nello stesso modo e con la stessa ampiezza di cui beneficierebbero se il trattamento fosse stato effettuato da un gruppo sociatario sottoposto alla Direttiva stessa.

[87] Art.29 Working Party, Working Document 12 del 24 Luglio 1998 "*Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive*", WP12

La società capogruppo (se stabilita nell'UE) o il membro del gruppo cui è stata delegata la protezione dei dati deve prendere i necessari provvedimenti per rimediare alle violazioni delle altre partecipanti al gruppo che si trovino al di fuori del territorio comunitario, e qualora appropriato, sostenere il risarcimento per ogni danno risultante dalla violazione delle BCR.

Il gruppo dovrà allegare alla richiesta di autorizzazione delle BCR la prova che la società responsabile abbia sufficienti risorse economiche per sostenere il pagamento dei risarcimenti in circostanze normali o che abbia preso misure per garantirne il pagamento (per esempio attraverso un assicurazione che copra tale responsabilità).

6) Trasparenza

In aggiunta alle previsioni sulle informazioni contenute agli artt.10 e 11 della Direttiva, i gruppi societari che garantiscono sufficienti salvaguardie devono essere in una posizione di dimostrare che i soggetti interessati siano consapevoli dei trasferimenti esteri dei loro dati personali verso gli altri membri del gruppo esterni all'UE. A tal fine l'esistenza ed il contenuto delle BCR deve essere facilmente accessibile per gli individui. Devono essere garantite informazioni aggiornate

riguardo i membri del gruppo vincolati dalle regole ed i modi disponibili per gli interessati al fine di assicurare il rispetto delle regole.

5.3.1 Procedura di approvazione e cooperazione tra autorità di protezione nazionali

La procedura di approvazione di BCR di fronte al Garante per la protezione dei dati personali italiano inizia con la richiesta del titolare del trattamento. Tale richiesta, delineata in ogni suo punto dal Garante[88] deve contenere:

1) Le tipologie di dati personali oggetto delle attività di trasferimento per cui si chiede l'autorizzazione.

2) Le finalità oggetto delle attività di trasferimento, specificandole per tipologia di dato trasferito.

3) I rapporti esistenti tra la società capogruppo e la società che presenta la richiesta di autorizzazione al fine di dimostrare che quest'ultima ha assunto un impegno giuridicamente vincolante al rispetto delle BCR medesime.

[88] Visionabile su http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi,visitato il 09 Febbraio 2015

4) In allegato il testo di cui si compongono le Bcr rispettivamente in lingua inglese ed italiana (quest'ultima asseverata da traduzione giurata)

5) In allegato l'*application form*[89] predisposta dalla società capogruppo in lingua inglese ed italiana

6) L'attestazione dell'avvenuto pagamento dei diritti di segreteria (quantificato nella misura di 1000 € per ciascun titolare del trattamento stabilito nel territorio dello Stato)

Il procedimento trova conclusione entro 45 giorni con la comunicazione da parte del Garante al richiedente della decisione adottata.
Ogni autorizzazione da parte dell'autorità di uno Stato Membro deve essere comunicata agli altri Stati membri ed alla Commissione Europea come previsto dall'art.26 comma 3 della Direttiva 95/46/CE. Ciò ha portato alla consapevolezza che tali notificazioni potrebbero essere coadiuvate da attività addizionali di cooperazione tra autorità di protezione dei dati, ancor prima di approvare le relative BCR. Questa cooperazione è infatti prevista dall'art. 28 comma 6 della Direttiva in

[89] Art.29 Working Party, Raccomandazione 1/2007 del 10 Gennaio 2007 "*Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data*", WP133

tutti i casi in cui una decisione di un'autorità nazionale può avere effetto sul trattamenti dei dati effettuato dal medesimo gruppo societario in uno Stato membro differente.

Da ciò nasce la possibilità per gruppi societari interessati alle BCR al fine di esportare dati da vari Stati Membri di fare uso di una procedura coordinata. L'idea principale dietro questa procedura è il dare la possibilità ai gruppi di avvantaggiarsi di un unico procedimento di richiesta di BCR attraverso una singola autorità di protezione dei dati, che attraverso una cooperazione coinvolgente molteplici autorità, porti alla concessione di un'autorizzazione da parte di tutte le differenti autorità degli Stati Membri dove il gruppo opera.

I dettagli di questa procedura erano inizialmente determinati caso per caso dalle autorità coinvolte, finché l'Art.29 Working Party non intervenne con per specificarla,[90] indicando come individuare la "*lead-autority*" sulla base di certi criteri:

a) La locazione della capogruppo europea.

b) La locazione della società partecipante al gruppo a cui è stata delegata la responsabilità di protezione dei dati.

[90] Art.29 Working Party, Working Document 107 del 14 Aprile 2005 "*Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"", WP107*

c) La locazione della società che è meglio adatta (in termini di funzioni mangeriali, carico amministrativo ecc…) per affrontare il procedimento di approvazione delle BCR e far rispettare le BCR all'interno del gruppo.

d) Il luogo in cui sono prese la maggior parte delle decisioni in quanto a finalità e modalità del trattamento.

e) Lo stato membro UE da cui hanno luogo la maggior parte dei trasferimenti.

Una volta presa una decisione sulla lead authority, questa inizierà la discussione con l'applicante. Il risultato di tale discussione formerà una bozza (cd. consolidated draft) che sarà distribuita tra le autorità di protezione dei dati coinvolte per ottenere i loro commenti. In circostanze normali, il periodo per tali commenti non dovrà eccedere un mese.
La lead authority trasmetterà tali commenti sulla bozza al richiedente e potrà continuare la discussione, se necessario. Se la lead authority è del parere che il richiedente sia in posizione di rispondere in modo soddisfacente a tutti i commenti, lo inviterà ad inviare una bozza finale. Questa formerà la base su cui la lead autority e le altre autorità

dovranno confermare che siano soddisfatti i requisiti di adeguatezza delle salvaguardie proposte.

Recentemente la procedura è stata semplificata attraverso l'aderimento di alcune autorità ad una "dichiarazione di mutuo riconoscimento". Grazie a questa procedura, accettata anche dal Garante italiano, la lead autority viene supportata da due autorità nel dialogo con la società capogruppo per l'approvazione delle BCR. Una volta riconosciute adeguate, le Binding Corporate Rules saranno automaticamente valide negli Stati Membri le cui autorità hanno aderito a tale modalità di cooperazione.

La procedura di approvazione è stata inoltre semplificata grazie al costante lavoro dell'Art.29 Working Party che ha permesso ai richiedenti di avere più trasparenza in merito ai requisiti loro necessari.

Col Working Document 133 è stata prevista una richiesta standard da compilare a cura del richiedente, che può formare una base adeguata una volta allegate le regole vincolanti specifiche attraverso cui ogni gruppo intende soddisfare i requisiti previsti. A tale documento seguì il Working Document 153, in cui una tabella chiarifica il contenuto necessario delle BCR come indicato separatamente nei Working

Document 74 e 108; distingue tra ciò che va incluso nelle BCR e ciò che va presentato alla DPA nella richiesta di approvazione; presenta i riferimenti testuali dei principi delle BCR e provvede spiegazioni e commenti sui singoli principi.

5.3.2 Binding Corporate Rules for Processors (BCR-P)

Fino alla fine del 2012, le BCR erano disponibili solo per legittimare i trasferimenti effettuati entro i limiti di un gruppo societario per i propri bisogni economici. Il trasferimento da parte del titolare del trattamento verso responsabili esterni, o entro un gruppo societario di responsabili del trattamento, doveva essere risolto separatamente ed al di fuori dello schema delle BCR.

Le nuove Binding Corporate Rules for Processors (BCR-P) permettono ad un gruppo societario di trovare approvazione per utilizzare le BCR nella sua qualità di responsabile. Ciò consente ai clienti di trasferire dati personali ai membri di tale gruppo, e permette a questi ultimi di trasferire tra di loro i dati personali per conto dei propri clienti. Ciò conduce alla distinzione tra BCR, da intendere come “BCR for your own data”, e BCR-P utilizzate in quanto “BCR for third party data”.

In modo simile, nel 2010 la Commissione Europea aveva adottato un set di Standard Contractual Clauses per i trasferimenti titolare-responsabile. Mentre le SCC sono efficienti per i trasferimenti di una quantità non eccessiva di dati da un esportatore europeo ad un importatore estero, le società di outsourcing hanno da anni richiesto un nuovo strumento

legale che permetta un approccio globale alla protezione dei dati e che riconoscesse ufficialmente le regole interne all'organizzazione.

Questo nuovo strumento legale si rivela più efficiente nell'organizzazione di un continuo flusso di trasferimenti effettuati da un responsabile ad un subresponsabile parte dello stesso gruppo per conto e dietro le istruzioni di un titolare del trattamento.

Visto il crescente interesse degli operatori economici per tale strumento, l'Art.29 Working Party ha adottato nel 2012 un Working Document che determina gli elementi ed i principi sottostanti le BCR-P, oltre ad un modulo standard per richiederne l'approvazione.[91]

Essendo le BCR-P in stretta relazione al trattamento dei dati determinato dalle istruzioni del titolare del trattamento, è richiesto che siano allegate al contratto col responsabile, definito dal Working Party "*Service Level Agreement*", che comprenda le misure tecniche ed organizzative richieste dall'art.17 della Direttiva 95/46/CE.

I partecipanti al gruppo del responsabile si impegnano a rispettare i principi contenuti nelle BCR-P e sono ritenuti responsabili nei confronti del titolare del trattamento per violazione delle sue istruzioni in merito a trattamento, sicurezza e confidenzialità.

[91] Art. 29 Working Party, Working Document 02/2012 del 6 Giugno 2012 *"Setting up a table with the elements and principles to be found in Processor Binding Corporate Rules",* WP195

È da sottolineare che Il titolare ha comunque la responsabilità che siano presenti le idonee garanzie per i dati trasferiti e trattati dal responsabile. Il Working Party ricorda che le BCR-P non hanno la funzione di traslare i doveri del titolare verso i responsabili, analogamente allo strumento delle clausole contrattuali tipo.

Le BCR-P devono anche contenere un chiaro dovere per ogni responsabile di cooperazione ed assistenza al titolare nel rispettare le norme sulla protezione dei dati, come per il suo dovere di rispettare i diritti degli interessati o gestire i loro reclami entro tempi ragionevoli.

Le norme riguardanti gli interessati dal trattamento nella loro qualità di terzi beneficiari sono riprese dallo schema delle clausole contrattuali tipo, con tutti i diritti azionabili verso titolare e responsabile che ciò comporta.

Inoltre le BCR-P devono identificare quale membro del gruppo tra:

a) La capogruppo stabilita sul territorio europeo

b) Il partecipante europeo al gruppo del responsabile a cui è stata delegata la responsabilità per la protezione dei dati

c) Il responsabile esportatore europeo

abbia accettato la responsabilità e prenso i necessari provvedimenti per rimediare alle azioni degli altri membri del gruppo qualora abbiano violato BCR-P o il Service Level Agreement ovvero per violazioni di un

subcontratto con subresponsabili stabiliti al di fuori del territorio europeo, e quando appropriato sostenere il risarcimento per ogni danno causato.

Nel caso nessun membro del gruppo sia stabilito nell'UE, sarà ritenuta responsabile la capogruppo stabilita all'estero.

Nonostante le BCR-P possano sembrare non troppo dissimili dalle BCR in quanto a rischi per la protezione dei dati, il recente dibattito sul cloud computing ne ha dimostrato la pericolosità.

Infatti mentre i titolari del trattamento che istituiscono il servizio di cloud processing e le modalità del trattamento sono facilmente identificabili, gli interessati dal trattamento restano spesso all'oscuro dei responsabili.

Viene pertanto sostenuto che i servizi di cloud dovrebbero essere equiparate ad "attività rischiose".[92]

È dello stesso parere il dipartimento del Parlamento Europeo per I diritti dei cittadini e gli affair costituzionali, che sostiene "the strategic risk to EU data sovereignty, which arises directly from the concept of BCR-P, is that the global Cloud industry is dominated by software "platforms" from Microsoft, Google, Amazon, and a few others. Microsoft's goal for its

[92] Joanna Kulesza, "Cloud Computing Transboundary data protection and international business compliance" International Data Privacy Law 2014, vol. 4 n. 4

public-sector salesforce from 2010 was to compete for every contract for data processing by governments".[93]

[93] EU Parliament policy department C citinzens' rights and constitutional affairs, "The US surveillance programmes and their impact on EU citizens' fundamental rights", 2013

6. Safe Harbor

6.1 Nascita del Safe Harbor

Gli International Safe Harbor Privacy Principles formano uno schema semplificato per il trasferimento di dati dall'Unione Europea agli operatori statunitensi che vi partecipano. Tale schema assicura l'adeguatezza della protezione dei dati nel trattamento di tali operatori, garantita da una procedura di certificazione e dal controllo di Department of Commerce, Federal Trade Commission e Department of Transport.

I negoziati per il raggiungimento di tale accordo iniziarono nel 1998, a breve distanza dall'entrata in vigore della Direttiva 95/46/CE e furono accompagnati nel 1999 da una serie di opinioni dell'Art.29 Working Party.[94]

Secondo il parere di quest'ultimo, il punto di criticità nella protezione assicurata dalla normativa statunitense si può rinvenire nella "*sectoral*

[94] Art. 29 Working Party, Opinione 1/99 del 26 Gennaio 1999 "*Level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government",* WP15
Art. 29 Working Party, Opinione 2/99 del 3 Maggio 1999 "*Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19th April 1999*", WP19
Art.29 Working Party, Opinione 4/99 del 7 Settembre 1999 "*Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed "Safe Harbor Principles" on the Adequacy of the "International Safe Harbor Principles""*, WP21

regulation" e "*self-regulation*" degli operatori. È stato così sostenuto che "*the current patchwork of narrowly-focussed sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union*".[95]

Ciò contrasta con il sistema comprensivo scelto dall'Europa per la protezione dei dati personali: come afferma il Wall Street Journal nel 2003, "EU privacy rules are increasingly shaping the way businesses operate around the globe".[96]

Per trovare una piattaforma comune attraverso cui iniziare i lavori si decise quindi di basare la discussione sulle linee guida dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) del 1980, di cui sia Stati Uniti che Unione Europea sono membri. [97]

Il Department of Commerce proseguì i negoziati inviando una versione revisionata dei Principi di Safe Harbor il 19 Aprile 1999 ed a seguito di alcuni dubbi espressi dall'Art.29 Working Party furono aggiunte un insieme di Frequently Asked Questions il 30 Aprile 1999. La particolarità

[95] Art. 29 Working Party, Opinione 1/99 del 26 Gennaio 1999 "*Level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government"*, WP15, Punto 1

[96] David Scheer, "*For Your Eyes Only, Europe's New High-Tech Role: Playing Privacy Cop to the World*", Wall Street Journal, 10 Ottobre 2003

[97] Gli USA inoltre hanno confermato il loro supporto a tali linee guida nella Ministerial Conference di Ottawa nel 1998

di tali FAQs si riscontra nella volontà del DoC di renderlo, piuttosto che un documento chiarificativo dei principi, una guida autoritativa agli stessi, dandogli forza legale.

I negoziati continuarono a mostrare punti di conflitto, prontamente rilevati dall'Art.29 Working Party, mentre la Commissione cercava seppur con lentezza di trovare un punto di comunione tra i principi previsti dal Department of Commerce e quelli comunitari.

Ciò risultò, nel Luglio 2000, in una risoluzione non vincolante del Parlamento Europeo[98] che richiamò la Commissione per non aver avuto un piano d'azione precedente all'entrata in vigore della Direttiva 95/46/CE, causando anni di incertezza sulla protezione dei dati dei cittadini europei e mancanza di chiarezza sulla situazione durante i negoziati. Il Parlamento faceva anche notare che il Safe Harbor avrebbe creato due sistemi di protezione dei dati negli USA, a seconda che il trattamento riguardasse i dati europei o di altri paesi terzi, in contrasto con la clausola OECD che proibisce discriminazioni basate sulla nazionalità. Questa e le altre problematiche evidenziate dall'Art.29

[98] Report A5- 0177/2000 "*on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles (C5-0280/2000 – 2000/2144(COS))"*

Working Party portarono il Parlamento a sconsigliare la conclusione dell'accordo del Safe Harbor nella forma al tempo prevista. [99]

Nonostante ciò, la Commissione rilasciò lo stesso mese il testo finale del "Safe Harbor Agreement" attraverso la decisione 2000/520/CE, secondo il potere conferitole dall'art.25 comma 6 della Direttiva 95/46/CE, accompagnandola negli anni seguenti da testi supplementari sulla sua applicazione. [100]

[99] Paul M. Schwartz , "*The EU-US Privacy collision: a turn to institutions and procedures*", 126 Harvard Law Review 1966, Maggio 2013 Vol 3

[100] Commission Staff Working Paper SEC(2002)196 "*The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*" e Commission Staff Working Document SEC(2004)1323 "*The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*"

6.2 Normativa del Safe Harbor

Come anticipato, le società americane che aderiscono agli standard di protezione, ai principi ed alle procedure del Safe Harbor si presume garantiscano una protezione adeguata ai sensi della Direttiva 95/46/CE. La decisione 2000/520/CE di adeguatezza di tali principi è infatti vincolante per tutti i Paesi dello Spazio Economico Europeo.

Ciò comporta, per società multinazionali che abbiano sussidiarie o partner commerciali in USA ed UE e partecipanti allo schema del Safe Habor, una importante riduzione degli oneri amministrativi richiesti dalla Direttiva per la protezione dei dati personali ed assicura la semplicità nei trasferimenti di dati dall'Europa.

Per partecipare al Safe Harbor, un operatore statunitense deve essere monitorato o regolato da un organo indipendente che possa proteggere i dati personali trasferiti in modo effettivo e che abbia il potere di investigare i reclami. Sono stati determinati dalla Commissione Europea come tali organi la Federal Trade Commission (FTC) ed il Department of Transportation (DOT). La partecipazione al Safe Harbor è quindi permessa solo alle organizzazioni sottoposte alla giurisdizione di FTC e DoT, quindi la generalità delle società commerciali e delle compagnie

aree. Da questo insieme mancano importanti settori come quello bancario, finanziario, delle telecomunicazioni ed associazioni non-profit.

Per essere qualificata al fine del Safe Habor, una società americana ha tre opzioni, potendo:

a) sviluppare una propria policy per il trattamento dei dati personali conforme ai requisiti del Safe Harbor;

b) partecipare ad un programma per la tutela dei dati personali che aderisca a tali requisiti, creato da società quali VeriSign o TRUSTe (opzione ad esempio fatta propria da Facebook Inc. che ha optato per una soluzione delle controversie affidata a TRUSTe fin dalla propria partecipazione al Safe Harbor del 05/10/2007);[101]

c) essere soggetta ad un insieme di leggi o regole che realizzino effettivamente tale standard.

[101] Come visionabile attraverso la lista aggiornata delle società partecipanti al Safe Harbor mantenuta da safeharbor.export.gov. Per Facebook: http://safeharbor.export.gov/companyinfo.aspx?id=23019

Gli operatori devono impegnarsi nel rispettare tutti i sette principi del Safe Harbor, accompagnati dalle FAQs previste dal Department of Commerce, avendo queste ultime forza legale. Sono di seguito delineati.[102]

1) Notice **-** è necessario informare gli individui delle finalità per cui i dati siano stati raccolti, le terze parti a cui tali dati potrebbero essere divulgati, le modalità per contattare il responsabile del trattamento al fine di presentare reclami o chiedere chiarimenti, le scelte e le modalità a disposizione degli interessati per limitare il trattamento e la diffusione dei dati. Tali informazioni devono essere comunicate in modo chiaro e completo al momento in cui gli interessati provvedono i loro dati o al primo momento seguente più opportuno; in ogni caso prima che tali dati siano usati per una finalità diversa da quella per cui siano stati inizialmente raccolti e trattati dall'esportatore europeo, o comunicati per la prima volta ad un terzo.

[102] US Department of Commerce, "*Safe Harbor Privacy Principles*", 21 Luglio 2000, visionabile su http://export.gov/safeharbor/eu/eg_main_018475.asp (visitato il 10 Febbraio 2015)

L'Art.29 Working Party fa notare, nell'opinion 4/99,[103] la discrepanza tra principi comunitari e di Safe Harbor nella previsione "*this notice must be provided […] when individuals are first asked to provide personal information to the organisation or as soon as practicable*". Il Safe Harbor, come già detto, si riferisce a trasferimenti da parte di titolari del trattamento europei a operatori statunitensi. Sono quindi i titolari europei a raccogliere i dati personali, e quindi essi saranno sottoposti alla normativa europea. Ciò contrasta con la possibilità di informare gli interessati dal trattamento al momento della raccolta dei dati "*ovvero il prima possibile*".

2) Choice - deve essere offerta agli interessati la possibilità di opt-out dalla comunicazione dei dati a terzi e dall'uso dei dati per finalità incompatibili con quelle per cui sono stati originariamente raccolti. Se il trattamento riguarda dati sensibili, la scelta, in entrambi i casi sopra esposti, sarà nel senso dell'opt-in, quindi richiederà un consenso esplicito. Per dati sensibili saranno da intendere anche quei dati qualificati come tali pure solamente dall'esportatore. Il fatto che la scelta di opt-out sia stata prevista solo per l'uso dei dati per finalità

[103] Art.29 Working Party, Opinione 7/99 del 3 Dicembre 1999 "*The Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce",* WP27

"incompatibili", e non semplicemente "diverse" ha provocato critiche per il contrasto con gli standard europei e l'"*Use Limitation Principle*" delle linee guida OECD.[104]

3) Onward transfers - i dati possono essere comunicati solamente alle terze parti che sottoscrivano i principi di Safe Harbor, siano soggette alla Direttiva europea sulla protezione dei dati ovvero abbiano garantito un equivalente livello di protezione attraverso accordo contrattuale. Qualora il terzo ricevente il trasferimento ulteriore abbia tali requisiti e tuttavia proceda a trattare i dati in violazione delle previsioni di legge o contrattuali, la società che ha trasferito i dati sarà ritenuta esente da ogni responsabilità, a meno che non fosse o sarebbe dovuta essere consapevole della violazione e non abbia preso gli opportuni provvedimenti per evitare tale trattamento.

Questo principio è stato inserito per via della mancanza di una normativa comprensiva sulla protezione dei dati negli Stati Uniti. Ciò avrebbe comportato la mancanza di responsabilità nel caso la società importatrice dei dati li avesse trasferiti ad una terza facente parte di un

[104] Tale principio prevede che "*Personal Data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with paragraph 9 (Purpose Specification) except:*
a) with the consent of the data subject; or
b) by the authority of law."

settore diverso e quindi sottoposta ad altre norme. Seppure il concetto di responsabilità del superiore per i danni causati da un soggetto subordinato (per esempio del datore di lavoro rispetto al dipendente) non è nuovo nel sistema legale statunitense, questo non ha mai trovato applicazione in tema di protezione dei dati personali.

4) Security - è necessario prendere ragionevoli precauzioni nel proteggere i dati personali da smarrimenti o trattamenti non autorizzati, oltre che da accesso, comunicazione, alterazione o distruzione non autorizzata.

A tale proposito la FAQ 10 del Safe Harbor, nell'indicare come nel caso i dati siano trasferiti solo al fine del trattamento sia necessario un contratto (che specifichi finalità, limitazioni etc…), prevede che non sia necessario specificare le misure di sicurezza previste. Tale previsione è tuttavia necessaria per i contratti titolare-responsabile anche quando entrambi siano sottoposti alla normativa comunitaria, quindi sarà necessario che sia inserita a cura della società europea trasferente i dati.

5) Data integrity - è necessario assicurare che i dati siano accurati, aggiornati, rilevanti ed adatti all'uso previsto.

6) Access - gli interessati devono avere accesso ai dati che li riguardino ed il diritto, dietro richiesta, di correzione, modifica o rimozione qualora gli stessi siano inaccurati a meno che l'onere o il costo sia disproporzionato al rischio per la privacy del soggetto in questione o violi i diritti di un'altro individuo. Il diritto d'accesso è essenziale in quanto strumentale alla corretta applicazione di buona parte dei principi del Safe Harbor, come data integrity, choice ed enforcement. Per tale motivo la FAQ 8 è stata interamente dedicata alla sua specificazione.

Innanzitutto viene previsto, seguendo l'Explanatory Memorandum alle linee guida OECD[105] come l'accesso non sia un diritto assoluto, non avendo ad esempio la forza di strumenti legali quali il *writ of subpoena*. Il dovere di garantire l'accesso, speculare al diritto dell'interessato dal trattamento, dovrebbe comunque essere sempre adempiuto in buona fede. Si riporta l'esempio di informazioni segrete riguardanti il soggetto, che nel caso specifico potrebbero essere oscurate in parte o separate e rese comunque disponibili.

Tra i motivi di restrizione dell'accesso si ha la presenza di informazioni commerciali confidenziali ed una serie di circostanze legate ad interessi pubblici quali la sicurezza nazionale, difesa, o il trattamento per soli

[105] OECD Council Recommendation "concerning guidelines governing the protection of privacy and transborder flows of personal data", 23 Settembre 1980, Explanatory Memorandum, Par 13(58)

scopi statistici o scientifici. Queste eccezioni sono a detta dell'Art.29 Working Party eccessivamente ampie, tuttavia l'onere della prova della loro validità ricade sulla società americana che intenda farle valere, trovando così una via di mezzo.

Non si trovò invece un accordo pieno sui casi in cui l'interessato dal trattamento abbia diritto alla rimozione dei dati. Viene indicato nelle FAQs e nei principi come questo sia presente qualora i dati siano inaccurati. Si evita tuttavia di menzionare la possibilità di rimozione di dati trattati in violazione della normativa. Tale rimozione fa parte delle sanzioni e dei rimedi della FAQ 11 "*Dispute Resolution and Enforcement*", ma dovrebbe essere resa disponibile anche senza la complessità comportata da un ricorso a tali meccanismi.

7) Enforcement - è necessario garantire degli effettivi meccanismi di rispetto dei principi di Safe Harbor, la possibilità di ricorso degli interessati dal trattamento e conseguenze per le società che abbiano violato la normativa.

Come minimo tali meccanismi devono includere:

a) modalità facilmente disponibili di ricorso attraverso cui ogni reclamo sia investigato e risolto in relazione ai principi di Safe Harbor e permetta di accedere al risarcimento dei danni;

b) procedure per la verifica della certificazione delle società sul fatto che le loro pratiche di trattamento siano veritiere ed implementate per come presentate;

c) obbligazioni di rimediare ai problemi nascenti dalla violazione delle norme di safe harbor da parte delle società che vi aderiscono.

Una volta che una società statunitense abbia stabilito una propria policy per il trattamento dei dati che rispetti i principi del Safe Harbor ed abbia deciso di partecipare a tale schema, essa deve autocertificare la propria conformità attraverso una comunicazione all'US Department of Commerce. Ciò può avvenire attraverso una lettera che includa dettagli sulle attività societarie in relazione ai dati raccolti ed una descrizione della propria policy nel trattarli. Il Department of Commerce mantiene e

rende pubblica una lista di tali società autocertificate e delle loro comunicazioni di certificazione.

I principi di Safe Harbor prevedono che la policy della società partecipante sia obbligante. Esistono pertanto vari modi per cui viene assicurato che l'autocertificazione non venga risolta in una mera dichiarazione di intenti ma risulti efficace.

Una volta registrata nel Safe Harbor, la società deve procedere ad autocertificazione annuale. Ciò avviene verificando il suo rispetto per i principi attraverso controlli interni ed esterni. Almeno annualmente, una dichiarazione deve essere firmata da un funzionario o un altro rappresentante autorizzato dalla società, che affermi come sia stata effettuata una valutazione che verifichi il rispetto dei principi. Questa dichiarazione deve essere resa disponibile dietro richiesta nel caso di reclami o qualora il rispetto delle norme da parte della società sia sotto investigazione.

La policy di una società sotto lo schema del Safe Harbor deve dunque specificare:

1) l'organo che ha giurisdizione nella gestione dei reclami;

2) il nome di ogni privacy program di cui è membro;

3) il meccanismo indipendente di risoluzione delle controversie.

Quest'ultimo assicura che ogni individuo possa essere messo a conoscenza delle modalità per presentare i reclami. Il ricorso può essere deciso affidandosi ad un'autorità di protezione dei dati europea ovvero attraverso metodi alternativi di risoluzione delle controversie.

Si può anche effettuare una scelta mista basata sul tipo del trattamento, per esempio Google Inc. si affida in linea generale alla mediazione internazionale della Judicial Arbitration and Mediation Services Inc. (JAMS), mentre per dati sulle risorse umane ha scelto la via della cooperazione con le autorità europee.[106]

Le sanzioni per la violazione delle norme includono pubblicità, rimozione dei dati, compensazione ed ordini ingiuntivi. Inoltre, se ci si affida ad un metodo alternativo di risoluzione delle controversie, il mancato rispetto di tali decisioni dovrà essere notificato al sistema giudiziario, alla FTC o al DOT ed in caso di violazione continuata del Safe Harbor anche al Department of Commerce.

FTC e DOT hanno il dovere di prendere provvedimenti qualora le società non rispettano le policy autocertificate. Secondo il Federal Trade Commission Act (FTCA) "*unfair or deceptive acts or practices in or*

[106] Certificazione 10/15/2005, http://safeharbor.export.gov/companyinfo.aspx?id=25007, visitato il 10 Febbraio 2015

affecting commerce are […] unlawful"[107] e la Federal Trade Commission ha il dovere di prevenirli, considerato che il trattamento dei dati è compreso tra le "practices" delle società.

Dopo un'audizione formale la FTC può imporre sanzioni per violazione dell'FTCA, inclusi cease and desist orders, restraning orders ed injunctions. La violazione da parte di una società partecipante al Safe Harbor di un provvedimento finale da parte delle autorità di supervisione comporta il decadimento dai benefici di tale schema. In tal caso la società deve comunicare l'accaduto al Department of Commerce, a pena di violazione del False Statement Act.[108] La violazione dei provvedimenti in sè comporta un'ulteriore sanzione di $12.000 al giorno finché non siano rispettati. Allo stesso modo il DOT ha pari poteri in relazione alle compagnie aeree.

Infine, oltre alla responsabilità nascente dai principi del Safe Harbor, le società partecipanti a tale schema che non rispettino i propri impegni al momento della certificazione possono essere chiamati in causa dagli interessati del trattamento per "misrepresention".[109] Tali soggetti sono inoltre tutelati da violazioni dei dati personali secondo common law e legislazione sia statale che federale.

[107] 15 U.S. Code § 45 - Unfair methods of competition unlawful, a(1)
[108] 18 U.S. Code § 1001
[109] Concetto di common law che fa riferimento a come della false dichiarazioni di una parte abbiano avuto l'effetto di indurre l'altra parte in errore nella sottoscrizione di un contratto

I principi elencati possono essere oggetto di limitazioni:

1) in quanto necessario per la sicurezza nazionale, l'interesse pubblico o perché richiesto dalle forze dell'ordine;

2) qualora la legge, regolamento governativo o giurisprudenza preveda obbligazioni in conflitto o esplicite autorizzazioni, purché sia previsto che, nell'esercizio di tali autorizzazioni, la società possa dimostrare che il non rispetto dei principi posti dal Safe Harbor è limitato a quanto necessario per il rispetto degli interessi prevalenti giustificati da tale autorizzazione;

3) se l'effetto della Direttiva 95/46/CE o della legge nazionale di uno Stato Membro permetta eccezioni o deroghe, purché queste siano applicate in un contesto comparabile.

In quanto consistente con l'obbiettivo di migliorare la tutela dei dati personali, le società dovrebbero cercare di implementare tali principi in modo completo e trasparente, inclusa la specificazione nella loro policy per il trattamento dei dati qualora le eccezioni previste da 1-2 trovino applicazione su base regolare. Per la stessa ragione, dove sia permesso

sotto i principi di Safe Harbor o dalla legge statunitense, ci si aspetta che le società optino per il più elevato livello di protezione possibile.

6.3 Implementazione del Safe Harbor

Negli anni a seguire l'implementazione dello schema di Safe Harbor, questo si è rivelato lo strumento prescelto dalla maggioranza delle società americane interessate al trasferimento di dati dallo Spazio Economico Europeo. Nel 2013 vi partecipavano 3246 operatori (rispetto ai 400 del 2004), tra cui Amazon, Facebook, Google, Hewlett-Packard, IBM e Microsoft. [110]

Tale successo è certamente da attribuire alla semplicità burocratica per la partecipazione ed al crescente incremento del flusso di dati UE-USA. [111]

Restano tuttavia ancora molti punti di conflitto.

Innanzitutto, considerato come tutto il sistema si basi sull'autocertificazione da parte delle società americane e sulla partecipazione volontaria, ogni mancanza nell'ambito della trasparenza o del controllo può rivelarsi deleteria per la protezione dei dati. Queste preoccupazioni sono talvolta risultate in prese di posizione da parte delle

[110] Al 26 Settembre 2013 il numero di società Safe Harbor indicate come "current" era di 3246, come "not current" 935. Organizzazioni Safe Harbour con 250 dipendendi o meno: 60% (1925 di 3246). Organizzazioni Safe Harbour con 251 o più: 40% (1295 di 3246)

[111] Secondo certi studi, se i servizi ed I trasferimenti di dati transnazionali dovessero essere sospesi l'impatto negative sul PIL UE potrebber raggiungere dallo 0.8% all'1.3% e le esportazioni verso gli USA calerebbero del 6.7% per perdita di competitività. Vedere "*The Economic Importance of Getting Data Protection Right*", uno studio dell'European Centre for International Political Economy for the US Chamber of Commerce, Marzo 2011

autorità nazionali europee. Per esempio l'autorità di protezione dei dati tedesca ha richiesto, nel 2010, che le società esportatrici di dati negli Stati Uniti controllassero attivamente che la certificazione della società importatrice sia valida e rispettosa dei principi di Safe Harbor. [112]

Ciò è stato reso necessario anche per il crescente numero di società americane che falsamente hanno preteso di partecipare al Safe Harbor, dalle 206 del 2008 alle 427 del 2013.[113]

Inoltre, sempre nel 2013, fino al 10% delle società certificate non rendevano disponibile la propria policy sul trattamento dei dati nei propri siti web.

Questa situazione ha portato all'attivazione del Department of Commerce, con la notificazione di centinaia di operatori statunitensi. Tale mancanza di trasparenza e rispetto delle norme comporta uno svantaggio nella competizione tra società europee ed americane, specialmente in settori non coperti dalla Federal Trade Commission. Sostiene al riguardo la European Telecommunications Network Operators' Association (ETNO) "this is in clear conflict to the most

[112] Decisione 28/29 Aprile 2010 del Düsseldorfer Kreis, un insieme delle autorità garanti dei dati personali statali e federali tedesche.

[113] Conferenza della società australiana di consulting Galexia di fronte all'EU Committee on Civil Liberties, Justice and Home Affairs su "*Electronic mass surveillance of EU citizens*", 7 Ottobre 2013

important plea of telecommunication operators regarding the need for a level playing field".[114]

Al problema della trasparenza e del grado di rispetto delle norme va aggiunto quello correlato della tutela dei diritti degli interessati dal trattamento e delle loro possibilità di ricorso contro gli abusi.

In tale ambito si riscontra l'incremento dei metodi alternativi di risoluzione delle controversie, o Alternative Dispute Resolution (ADR). Come fatto notare dallo studio Galexia 200[115] tale soluzione non è sempre facilmente percorribile per i consumatori. Per esempio l'American Arbitration Association (AAA) prevede costi tra $120 e $1200 l'ora (con un minimo di 4 ore oltre a spese amministrative per $950), mentre il Judicial Arbitration Mediation Service (JAMS) a cui si affida tra gli altri anche Google Inc. prevede costi tra $350 e $800. Tali costi inoltre mancano di trasparenza nella presentazione della possibilità di una mediazione con gli interessati.

È da rilevare negli ultimi anni una spinta per rendere preferibile per società e consumatori il ricorso giudiziario, in particolare attraverso l'accordo sulla mutua assistenza giudiziaria tra UE ed US, incorporato

[114] "*ETNO consideration*" ricevute dalla Commissione il 4 Ottobre 2013 in cui si indica inoltre che "*US companies can transfer data with much less restrictions than their European counterparts [which] … constitutes a clear discrimination of European companies and is affecting the competitiveness of European companies*"

[115] Galexia 2008, "*The US Safe Harbor - Fact or Fiction?*"

con la decisione 2009/820/PESC del Consiglio Europeo ed entrato in vigore il 1 Febbraio 2010.

La cooperazione è stata anche incrementata da vari Memorandum of Understanding tra la Federal Trade Commission e le autorità di protezione dei dati europee, ad esempio il 26 Luglio 2013 con l'autorità irlandese (l'Irlanda è il paese di stabilimento della sussidiaria europea di Facebook Inc.).

Nell'Agosto 2013 la FTC ha inoltre annunciato maggiori impegni nella monitorazione delle società con banche dati considerevoli e creato un portale attraverso cui i consumatori possono presentare reclami (*https://www.ftccomplaintassistant.gov/*).

Non si può tuttavia mancare di osservare come il 2013 si sia rivelato un anno di tensioni nelle relazioni tra Europa e Stati Uniti, a seguito delle rivelazioni di Edward Snowden del 5-6 Giugno 2013 sul monitoraggio di massa da parte della National Security Agency (NSA) dei dati sul territorio americano, compresi quelli trasferiti dai Paesi UE.[116]

Ciò ha portato ad un'inchiesta del Citizens' Rights and Constitutional Affairs Deparment del Parlamento Europeo, dal titolo "The US surveillance programmes and their impact on EU citizens' fundamental rights".

[116] The Washington Post, "*NSA slides explain the PRISM data-collection program*", pubblicato il 6 Giugno 2013, aggiornato il 10 Luglio 2013June 6, 2013

Il 12 Marzo 2014 il Parlamento ha adottato una risoluzione a larga maggioranza (544 voti a favore, 78 contrari e 60 astenuti)[117] attraverso cui vengono indicate delle raccomandazioni per incrementare la tutela dei dati personali dei cittadini europei in questo contesto. La risoluzione implica che la Commissione sospenda immediatamente i principi di "Safe Harbor" e ne rinegozi di nuovi e più appropriati. Viene richiesta inoltre la sospensione del Terrorist Finance Tracking Programme (TFTP, analizzato al capitolo 5.2.1) finchè un'investigazione completa non ristabilisca la fiducia nell'accordo.

Ed è proprio in quest'ultima direzione che si erano già mossi Commissione e Department of Commerce, da cui è scaturita la Comunicazione dalla Commissione al Parlamento europeo ed al Consiglio COM(2013)846 "Rebuilding Trust in EU-US Data Flows".

Questo non ha tuttavia impedito un coinvolgimento della Corte di Giustizia Europea, nel procedimento C-362/14 - Schrems, in cui viene indicato come "*in the light of the revelations made […] by Edward Snowden concerning the activities of the US National Security Agency (NSA), there was no meaningful protection in US law and practice in*

[117] Report del Parlamento Europeo 2013/2188(INI), "*US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*"

respect of data so transferred to the US so far as Stale surveillance was concerned".[118]

[118] Procedimento della Corte di Giustizia Europea C-362/14, dalla richiesta di domanda pregiudiziale da parte dell'Autorità di protezione dei dati Irlandese verso la Corte, punto 3

6.3.1 Procedimento C-362/14 Schrems

Il signor Schrems, di nazionalità austriaca, era al tempo dei fatti un utente del servizio di social network offerto da "*Facebook.com*". Essendo stabilito in Europa, il suo uso di Facebook era governato dai termini contrattuali previsti da Facebook Ireland (sussidiaria di Facebook Inc.), secondo i quali quest'ultima ha la facoltà di raccogliere dati personali sui suoi utenti ed inviarli a Facebook Inc., rendendo di fatto i dati trasferiti e conservati negli Stati Uniti d'America.

Schrems aveva da tempo provveduto a presentare 22 reclami all'autorità per la protezione dei dati personali irlandese per violazioni concernenti, tra gli altri: "pokes", "tagging", riconoscimento facciale, sicurezza dei dati e consenso al trattamento.

A seguito delle rivelazioni di Edward Snowden, si aggiunse un ventitreesimo reclamo, riguardante l'inadeguatezza della protezione dei dati personali trasferiti negli Stati Uniti, e quindi l'invalidità della Decisione 2000/520/CE che istituì il Safe Harbor.[119]

[119] Complaint against Facebook Ireland Ltd – 23 "PRISM", 25 Giugno 2013, consultabile su http://www.europe-v-facebook.org/prism/facebook.pdf, visitato il 13 Febbraio 2015

Schrems rilevò, a tal proposito, che le garanzie presenti al momento dell'approvazione di tale schema nel 2000 sono scemate nei 15 anni successivi, specialmente a seguito dell'adozione da parte degli USA dell'"*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*" (USA PATRIOCT Act) del 2001 e dell'emendamento del "*Foreign Intelligence Surveillance Act*" (FISA) del 2008.

In particolare, la sezione 702 dell'emendamento FISA [120] permette all'Attorney General ed al Director of National Intelligence statunitensi di autorizzare congiuntamente l'acquisizione, anche da parte di società private, di comunicazioni appartenenti a soggetti non cittadini americani (non-US Person) e localizzati al di fuori degli Stati Uniti.

Il reclamo fu tuttavia ignorato dall'autorità di protezione dei dati irlandese, adducendo come fosse vincolata dalla Decisione 2000/520/CE della Commissione Europea in merito all'adeguatezza dei trasferimenti di dati su suolo americano, e non potendo dunque entrare nel merito dei fatti.

Il Signor Schrems, trovandosi in disaccordo con tale posizione, decise di rivolgersi all'High Court of Justice irlandese. Quest'ultima procedette a

[120] U.S. CODE § 1881a

riconoscere come le preoccupazioni del ricorrente non fossero infondate, ed anzi ritenne i fattori presentati idonei a creare incertezza sull'adeguatezza della protezione dei dati americana.

Basti citare il parere della Corte sulle modalità di richiesta dei dati da parte delle autorità di sicurezza statunitensi, con una procedura di previa approvazione della FISA Court: "FISA Court's hearing are entirely conducted in secret, so that even the court orders and its jurisprudence remain a closed book. The US security authorities are, in effect, the only parties who are or who can be heard in respect of such applications before the FISA Court. […] the essentially secret and ex parte nature of the FISA Court's activities makes an independent assessment of its orders and jurisprudence all but impossible".[121]

Il Justice Hogan considerò infine come l'autorità di protezione dei dati irlandese, restando fedele alla Decisione della Commissione Europea, non aveva fatto altro che rispettare i propri obblighi. Decise dunque di procedere attraverso una domanda pregiudiziale, proposta dinanzi alla Corte di Giustizia Europea.

Il punto della procedimento che ne scaturì (C-362/14), ancora oggi pendente, consiste nella possibilità o meno per il garante della

[121] Irish High Court of Justice, 2013 765JRJ, "*Maximillian Schrems v. Data Protection Commissioner*", IV(15)

protezione dei dati irlandese di procedere ad una investigazione in proprio riguardo l'adeguatezza della protezione dei dati offerta dalla normativa statunitense.

Ciò pare essere reso necessario dai nuovi elementi insorti dal tempo della Decisione a tal riguardo presa dalla Commissione nel 2000. D'altra parte, comporterebbe tuttavia una violazione per l'autorità irlandese del suo dovere di rispettare ed applicare tali decisioni.

La sentenza, attesa nei prossimi anni, potrebbe portare ad importanti modifiche nei rapporti tra Europa e Stati Uniti ed in generale per la vincolatività delle Decisioni di adeguatezza della Commissione Europea.

7. Conclusioni

Una volta analizzata la situazione attuale sulla protezione dei dati personali nel trattamento da parte degli operatori esteri, non resta che fare un passo avanti e dare una visione d'insieme della disciplina attuale e del prossimo futuro.

A tal fine non ci si può esimere dal considerare gli effetti che saranno portati dal nuovo Regolamento Europeo sulla protezione dei dati personali, che sostituirà la Direttiva 95/46/CE, sarà possibilmente adottato durante il 2015 ed entrerà in vigore nel 2017.

Tra i punti più importanti vi sono i più stringenti requisiti per il trasferimento di dati personali verso Paesi terzi. Verrà infatti previsto l'obbligo di autorizzazione dei Garanti nazionali prima di inviare dati su richiesta di autorità giudiziarie o amministrative estere e sarà istituito un meccanismo di sportello unico (cd. *one-stop-shop*) per l'approvazione di BCR, che formeranno lo strumento principale di trasferimento dei dati verso società multinazionali. In ogni caso, la modifica più importante sarà la scelta dello strumento normativo del Regolamento dell'Unione Europea, con la portata generale, obbligatorietà in tutti i suoi elementi e la diretta applicabilità in ciascuno degli Stati membri che ciò comporta.

A proposito di tale scelta non si può mancare di notare che lo strumento della Direttiva, adottato nel 1995 per regolare il trattamento dei dati personali, seppure di tipo dettagliato ed avente l'obbiettivo di ravvicinare le legislazioni nazionali dei Paesi Membri, abbia talvolta fallito nel suo intento.

Le differenze tra le legislazioni comunitarie, anche quando minime, comportano confusione e complessità della materia per titolari ed interessati dal trattamento che si può considerare tra i primi fattori di criticità nella protezione dei dati personali.

Basti qui ricordare, a proposito della normativa italiana, che la figura del "Data Controller" è stata tradotta nel testo della Direttiva e nei documenti dell'Art.29 Working Part come "*responsabile*", e nel Codice in materia di protezione dei dati personali come "*titolare*", mentre la figura del "*Data Processor*" coincide in parte con l'incaricato italiano (che può tuttavia essere solo una persona fisica) ed è talvolta usata come sinonimo di responsabile, soprattutto in tema di BCR-P.[122]

Se da una parte si potranno evitare tali discrepanze legislative, dall'altra si riflette ancora sulle possibilità inesplorate della Direttiva 95/46/CE[123]

[122] Giusella Finocchiaro, "*Privacy e protezione dei dati personali. Disciplina e strumenti operativi*", Zanichelli 2012

[123] Si sostiene a tal proposito: "*It was also widely recognised that more value can still be extracted from current arrangements. A lot can be achieved by better implementation of the current rules, for instance by establishing consensus over the interpretation of several key concepts and a possible shift in emphasis in the*

e sulla preoccupazione che la materia non potrà che divenire ancora più complessa ed estesa.[124]

Ed è proprio la complessità della normativa uno degli ostacoli maggiori al consenso informato degli interessati dal trattamento, soprattutto su Internet. Era stato al riguardo proposto all'Art.7(4) del nuovo Regolamento che "*Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller*", previsione in seguito eliminata dalle versioni emendate di Consiglio Europeo e LIBE (Civil Liberties, Justice and Home Affairs). Questa si può ritenere una diretta conseguenza della "*mitologia del consenso*",[125] a cui spesso ci si affida non riconoscendo come esso sia influenzato dalle tecnologie moderne.

Per l'utente internet, usufruitore dei servizi forniti da colossi multinazionali come Facebook o Google spesso c'è poco da scegliere: se si vuole utilizzare un servizio se ne devono accettare le condizioni; non cliccare sulla corrispondente "checkbox" comporta la negazione dell'accesso ad un servizio a cui nella maggior parte dei casi esistono poche o nulle alternative. A sottolineare questa situazione c'è il fatto che

---

interpretation of others", Neil Robinson and others, Review of the European Data Protection Directive, RAND 2009

[124] La Direttiva 95/46/CE conta solo 34 articoli, mentre il Regolamento proposto ne include 91, triplicando il numero di parole, da 12,500 a 35,000

[125] Bert-Jaap Koops **"***The trouble with European data protection law*", International Data Privacy Law 2014, vol. 4 n. 4

esistono in pratica un numero limitato di modelli di business per generare ricavi, se non si sceglie di sfruttare risorse quali profiling degli utenti e pubblicità. Anche se servizi a pagamento e rispettosi della protezione dei dati personali sono teoricamente possibili, il muoversi da servizi gratis a quelli a pagamento non è qualcosa che molti utenti internet sono disposti a fare.

La soluzione a cui ci si aggrappa si risolve nella praticità (attraverso testi brevi od icone) e significatività del consenso (con l'utilizzo di un linguaggio semplice o obbligando tecnicamente l'interessato a leggere il testo prima di proseguire). Questi due valori però non possono che risolversi in una dicotomia: più la procedura del consenso è resa semplice, meno ci si può aspettare una comprensione profonda da parte degli interessati; più si dà priorità all'informazione e meno l'utente si impegnerà intellettualmente nella sua cognizione.[126]

Alle difficoltà nascenti dal consenso, nella pratica se ne affiancano di altre basate sull'esercizio del controllo sui dati.

Esistono ancora piccole realtà in cui un singolo titolare del trattamento si occupa di un numero relativamente minore di dati personali, per chiare finalità ed attraverso un dialogo con l'interessato, ma nella stragrande

[126] ", Ronald E. Leenes, "*Do They Know Me? Deconstructing Identifiability"*, University of Ottawa Law & Technology Journal, Vol. 4, n. 1-2, p. 135, 2007

maggioranza dei casi, con l'evoluzione di database, cloud computing e profiling queste situazioni tenderanno a scomparire.

I trattamenti più vasti, e che mettono maggiormente a rischio i dati personali, riguardano la condivisione di dati tra multipli titolari ed incaricati e finalità non sempre precisate (si ricordi la possibilità delle società partecipanti al Safe Harbor di procedere a trattamenti per finalità diverse da quelle previste al momento della raccolta, col limite di quelle non compatibili, a meno del mero opt-out).

Come per il consenso, l'esercizio del controllo sui dati è frequentemente solo teorico.

Sostiene a tal proposito Bert-Jaap Koops sull'International Data Privacy Law Journal, "*Yes, you can be informed, if you know where to look and how to read (but who knows, looks, and reads?). Yes, you can request controllers to let you know what data they process, if you know that you have such a right in the first place (but which controller really understands and seriously complies with all such requests, particularly if exercised on an above-incidental scale?). Yes, you can request correction or erasure, if you know whom to ask (but how are you ever going to reach everyone in the chain, or mosaic, or swamp, of*

interconnected data processing?). There are simply too many ifs and buts to make data subject rights meaningful in practice".[127]

Se allora non si può fare affidamento solo sull'incremento dei diritti degli interessati dal trattamento, bisognerà cercare nuove soluzioni dal punto di vista degli operatori.

A tal fine il Regolamento europeo sulla protezione dei dati personali introdurrà, all'art.33, il dovere della valutazione d'impatto sulla protezione dei dati o *Data Protection Impact Assessment* (DPIA).

Questa valutazione avrà luogo "*quando il trattamento, per la sua natura, il suo oggetto o le sue finalità, presenta rischi specifici per i diritti e le libertà degli interessati*", indicando tra le attività rischiose un insieme aperto che comprende profiling, video sorveglianza, trattamento di dati sensibili, genetici, biometrici o dei minori. È stato sostenuto che tra tali attività rischiose debba essere incluso il trattamento attraverso cloud-computing ed il trasferimento di dati all'estero.[128]

Infatti il DPIA è il genere di strumento che permetterebbe una valutazione preventiva del trattamento dei dati, già al momento della

[127] Bert-Jaap Koops , "The trouble with European data protection law", International Data Privacy Law 2014, vol. 4 n. 4

[128] Joanna Kulesza, "*Cloud Computing Transboundary data protection and international business compliance*" International Data Privacy Law 2014, vol. 4 n. 4

sua concezione da parte dei titolari del trattamento, e che fa parte di quelle pratiche definite "*Privacy by Design*".

Tale concetto è un approccio all'ingegneria dei sistemi di trattamento dei dati che tiene in considerazione i diritti degli interessati durante l'intero procedimento.

Esso ha origine da un report su "*privacy-enhancing technologies*" da parte di un team formato delle autorità di protezione dei dati di Canada ed Olanda.[129]

Il successo di tale sistema l'ha portato ad essere scelto nel 2012 dall'US Federal Trade Commission come una delle pratiche raccomandate per la protezione dei dati, [130] e ad essere incorporato nel piano della Commissione Europea per la stesura del Regolamento europeo sulla protezione dei dati personali.

Ciò dimostra una condivisione di valori transatlantica nel settore, basata su 7 principi fondanti:[131]

1) *Proactive, not reactive; preventive, not remedial*: la PbD anticipa e previene eventi invasivi della privacy nello stato iniziale del trattamento,

[129] Hes, R. "*Privacy Enhancing Technologies: the path to anonymity*"

[130] Federal Trade Commission Report, "*Protecting Consumer Privacy in an Era of Rapid Change – a major validation of its significance*", Marzo 2012

[131] Ann Cavoukian, "*Privacy by Design, The 7 Foundational Principles*"

senza attendere che il rischio per la protezione dei dati personali si materializzi.

2) *Privacy as the default setting*: per mantenere la protezione dei dati personali non è richiesta nessuna azione da parte degli individui, essendo ciò previsto automaticamente.

3) *Privacy embedded into design*: la protezione dei dati personali è un elemento essenziale delle funzionalità base dei servizi progettati ed offerti all'utente finale.

4) *Full functionality, positive-sum, not zero-sum*: la PbD cerca di accomodare tutti i legittimi interessi e gli obbiettivi del trattamento, piuttosto che effettuare compromessi non necessari tra i diversi aspetti.

5) *End-to-end security, full lifecycle protection*: forti misure di sicurezza sono essenziali per la protezione dei dati personali, dall'inizio alla fine del ciclo dei dati.

6) *Visibility and trasparency*: i componenti di ogni operazione sui dati devono rimanere visibili e trasparenti. Sono essenziali per stabilire *accountability* e fiducia.

7) *Respect for user privacy*: la PbD richiede il mantenimento degli interessi degli individui come obbiettivo chiave nell'offrire misure come la "*privacy by default setting*", comunicazioni semplici ed efficienti e opzioni user-friendly per gli interessati dal trattamento.

Per ottenere una protezione dei dati personali che unisca i cittadini di Paesi diversi non si può quindi che operare sulla base di una prospettiva comune, e questa deve necessariamente essere considerata ancora prima del trattamento, ossia nella sua ideazione. Come affermato nell'introduzione, la tecnologia tende ad unire, mentre la legislazione a dividere. Tuttavia normative di Paesi differenti, aventi alla base una tavola di valori condivisi, non possono che accrescere ed arricchire le possibilità offerte dall'evoluzione tecnologica.

Bibliografia

Normativa

Art.29 Working Party, Opinione 03/2013 del 2 Aprile 2013 "*purpose limitation*", WP 203

Art.29 Working Party, Opinione 3/2010 del 13 Luglio 2010 "*the principle of accountability*", WP 173

Legge austriaca sulla protezione dei dati (Datenschutzgesetz), Federal Law Gazette No. 165/1999, par. 46

Risoluzione del Consiglio d'Europa (74) 29 "*the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*", 20 September 1974

Risoluzione del Consiglio d'Europa (73) 22 "*the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*", 26 September 1973

Consiglio d'Europa, "*Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*" CETS n. 108/1981

Raccomandazione del Consiglio *d'Europa R (95) 4 "the protection of personal data in the area of telecommunication services, with particular reference to telephone services"*

Consiglio d'Europa, "*Emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*", 15 Giugno 1999

Consiglio d'Europa, "*Protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri*", CETS n. 181/2001

Garante per la protezione dei dati personali, doc. 1728496 "*Autorizzazione al trasferimento di dati personali del territorio dello Stato verso Paesi non appartenenti all'Unione europea, effettuati in conformità alle clausole contrattuali tipo*"

Garante per la protezione dei dati personali, doc. 1717863 "*Trasferimento di dati personali relativi ai dipendenti e alla clientela verso paesi non appartenenti all'Ue mediante Bcr - provvedimento di autorizzazione nazionale (gruppo Hyatt)"*

Art.29 Working Party, Working Document 74 del 3 Giugno 2003 "*Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*", WP74

Art.29 Working Party, Explanatory Document del 19 Aprile 2013 "*The Processor Binding Corporate Rules*" WP 204

Decisione 94/1/CECA "r*elativa alla conclusione dell'accordo sullo Spazio economico europeo tra le Comunità europee, i loro Stati membri e la Repubblica d'Austria, la Repubblica di Finlandia, la Repubblica d'Islanda, il Principato del Liechtenstein, il Regno di Norvegia, il Regno di Svezia e la Confederazione elvetica*", 13 dicembre 1993, OJ 1994 L 1

Direttiva 95/46/CE "*relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*", OJ Vol 38, 23 Novembre 1995, L. 281, p. 31

Direttiva 2002/58/CE "*relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche",* OJ Vol 45, 31 Luglio 2002 L. 201, p. 37

Direttiva 2006/24/CE "*riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi e comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione*", OJ Vol 49, 13 Aprile 2006 L. 105, p. 54

Personuppgiftslag (1998:204), legge sulla protezione dei dati

OECD Council Recommendation "*concerning guidelines governing the protection of privacy and transborder flows of personal data*", 23 Settembre 1980

Risoluzione ONU 45/95 "*Guidelines for the Regulation of Computerized Personal Data Files*", 14 Dicembre 1990

Public Law 100-618, "*Video Privacy Protection Act*", 5 Novembre 1988

Commissione Europea 2002, Decisione 2002/2/CE del 20 Dicembre 2001 conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio "*riguardante l'adeguatezza della protezione fornita dalla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (Canadian Personal Information Protection and Electronic Documents Act)*".

Accordo USA-UE riguardo il trasferimenti di PNR, OJ 2012 L 215, pp. 5–14

Accordo USA-UE riguardo trattamento e trasferimento di Financial Messaging Data dall'Unione Europea agli Stati Uniti d'America utilizzati per il Terrorist Finance Tracking Program, OJ 2010 L 8, pp. 11–16

Commissione Europea COM(2003) 265 "*First report on the implementation of the Data Protection Directive (95/46/CE)*", 15 Maggio 2003

Art.29 Working Party, Working Document 12 del 24 Luglio 1998 "Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive", WP 12

Decisione del Consiglio Europeo 2004/496/CE del 17 Maggio 2004 "*conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection*", OJ 2004 L 183, p. 83.

Decisione della Commissione 2004/535/CE del 14 Maggio 2004 "*adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection*", OJ 2004 L 235, pp. 11-22

Decisione del Consiglio 2012/472/UE del 26 Aprile 2012 "*conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security*" OJ 2012 L 215/4.

Comunicazione della Commissione del 21 Settembre 2010 "*global approach to transfers of Passenger Name Record (PNR) data to third countries*", COM(2010)492.

Art.29 Working Party, Opinione 7/2010 "*European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries"*, WP 178.

Proposta per una Direttiva del Parlamento Europeo e del Consiglio del 2 Febbraio 2011 "*use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*", COM(2011)32.

European Union Agency for Fundamental Rights (FRA) "*Opinione 1/2011 "Passenger Name Record""*", 14 Giugno 2011

Memorandum of understanding between the ministry of the interior or the Czech Republic and the Department of Homeland Security of the United States of America regarding the United States Visa Waiver Program and related enhanced security measures, 27 Febbraio 2008

Art.29 Working Party, Opinione 14/2011 del 13 Giugno 2011 "*data protection issues related to the prevention of money laundering and terrorist financing"*, WP 186

Art.29 Working Party, Opinione 10/2006 del 22 Novembre 2006 "*processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT)"*, WP 128

Autorità per la protezione dei dati personali del Belgio (Commission de la protection de la vie privée) Decisione del 9 Dicembre 2008, "*Control and recommendation procedure initiated with respect to the company SWIFT scrl"*

Decisione del Consiglio 2010/412/EU del 13 Luglio 2010 "*conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program",* OJ 2010 L 195, pp. 3 e 4.

Consiglio d'Europa, Comitato consultivo della Convenzione 108/81 (2002), "*Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data*".

Garante per la protezione dei dati personali italiano, doc. web n. 42156, "*Autorizzazione al trasferimento verso Paesi senza adeguato livello di protezione*", 10 ottobre 2001

Garante per la protezione dei dati personali italiano, doc. web n. 1151949, "*Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso paesi terzi*", 9 Giugno 2005

Garante per la protezione dei dati personali, doc. web n. 1728496, "*Autorizzazione al trasferimento di dati personali del territorio dello Stato verso Paesi non appartenenti all'Unione europea, effettuati in conformità alle clausole contrattuali tipo, di cui all'allegato alla decisione della Commissione europea del 5 febbraio 2010, n. 2010/87/UE*", 27 maggio 2010

Art.29 Working Party, Opinione 1/2010 del 16 Febbraio 2010 "*the concepts of "controller" and "processor"",* WP 169

Garante per la protezione dei dati personali, Relazione annuale 2012

Art.29 Working Party, Raccomandazione 1/2007 del 10 Gennaio 2007 "*Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data*", WP133

[1] Art.29 Working Party, Working Document 107 del 14 Aprile 2005 "*Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"", WP107*

Art. 29 Working Party, Working Document 02/2012 del 6 Giugno 2012 "*Setting up a table with the elements and principles to be found in Processor Binding Corporate Rules",* WP195

EU Parliament policy department C citinzens' rights and constitutional affairs, "The US surveillance programmes and their impact on EU citizens' fundamental rights", 2013

Art. 29 Working Party, Opinione 1/99 del 26 Gennaio 1999 "*Level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government"*, WP15

Art. 29 Working Party, Opinione 2/99 del 3 Maggio 1999 "*Adequacy of the "International Safe Harbor Principles" issued by the US Department of Commerce on 19th April 1999*", WP19

Art.29 Working Party, Opinione 4/99 del 7 Settembre 1999 "*Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed*

"Safe Harbor Principles" on the Adequacy of the "International Safe Harbor Principles"", WP21

Code of Laws of the United States of America

Report del Consiglio europeo A5- 0177/2000 "*on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles (C5-0280/2000 – 2000/2144(COS))"*

Commission Staff Working Paper SEC(2002)196 "*The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*"

Commission Staff Working Document SEC(2004)1323 "*The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*"

US Department of Commerce, "*Safe Harbor Privacy Principles*", 21 Luglio 2000, visionabile su http://export.gov/safeharbor/eu/eg_main_018475.asp (visitato il 10 Febbraio 2015)

Art.29 Working Party, Opinione 7/99 del 3 Dicembre 1999 "*The Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce",* WP27

Düsseldorfer Kreis, Decisione 28/29 Aprile 2010

Report del Parlamento Europeo 2013/2188(INI), "*US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*"

Federal Trade Commission report, "*Protecting Consumer Privacy in an Era of Rapid Change – a major validation of its significance*" Marzo 2012

Giurisprudenza

Supreme Court of the United States, Griswold v. Connecticut, 381 U.S. 479, 1965

Corte Europea dei Diritti dell'Uomo, Amann v. Switzerland [GC], N. 27798/95, 16 Febbraio 2000

Corte Europea dei Diritti dell'Uomo, Kopp v. Switzerland, N. 23224/94, 25 Marzo 1998

Corte Europea dei Diritti dell'Uomo, Iordachi and Others v. Moldova, N.25198/02, 10 Febbraio 2009

Corte Europea dei Diritti dell'Uomo, Malone v. the United Kingdom, N. 8691/79, 2 Agosto 1984

Corte Europea dei Diritti dell'Uomo, Silver and Others v. the United Kingdom, N. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 Marzo 1983

Corte di Giustizia dell'Unione europea, Procedimenti riuniti C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 Novembre 2011

Corte di Giustizia dell'Unione europea, C-317/04 e C-318/04 European Parliament v Council of the European Union and Commission of the European Communities, 30 Maggio 2006

Corte di Giustizia dell'Unione europea, C- 131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), 13 Maggio 2014

Corte di Giustizia dell'Unione europea, C-101/01 Criminal proceedings against Bodil Lindqvist, 6 Novembre 2003

Corte di Giustizia dell'Unione europea, C-362/14 Schrems, causa pendente

Dottrina

Michael Bogdan, "*Dataflykt over gränserna och den svenska datalagstiftningen*", Svensk Juristtidning 1978

Christopher Kuner, "*The (data privacy) law hasn't even checked in when technology takes off",* International Data Privacy Law 2014 vol. 4 n. 3

Christopher Kuner, "*Systematic Government Access to Private-Sector Data Redux",* International Data Privacy Law 2014 vol. 4 n. 1

Ira Rubinstein, New York University School of Law, Greg Nojeim, Center for Democracy & Technology, Ronald Lee, Arnold & Porter LLP, "*Systematic Government Access to Personal Data: A Comparative Analysis*" 13 Novembre 2013

Dan Svantesson, "*Fundamental policy considerations for the regulation of Internet cross-border privacy issues*", Policy & Internet 2011

Palfrey, "*Born Digital"*, 2008

Christopher Kuner, Fred H. Cate, Christopher Millard, e Dan Jerker B. Svantesson "*The extraterritoriality of data privacy laws — an explosive issue yet to detonate"*, International Data Privacy Law 2013 vol. 3 n. 3

Donald C. Dowling, Jr, "*International Data Protection and Privacy Law*", White & Case, Agosto 2009

Statewatch, Marzo 2008

"*Report on the value of TFTP Provided Data*" 27 Novembre 2013

Paul M. Schwartz , "*The EU-US Privacy collision: a turn to institutions and procedures*", 126 Harvard Law Review 1966, Maggio 2013 Vol 3

European Centre for International Political Economy, "*The Economic Importance of Getting Data Protection Right*", Marzo 2011

Galexia "*Electronic mass surveillance of EU citizens*", 7 Ottobre 2013

European Telecommunications Network Operators, "*ETNO consideration*" 4 Ottobre 2013

Galexia, "*The US Safe Harbor - Fact or Fiction?*", 2008

Giusella Finocchiaro, "*Privacy e protezione dei dati personali. Disciplina e strumenti operativi*", Zanichelli 2012

Neil Robinson and others, "*Review of the European Data Protection Directive*", RAND 2009

Joanna Kulesza, "*Cloud Computing Transboundary data protection and international business compliance*" International Data Privacy Law 2014, vol. 4 n. 4

Hes, R. "Privacy Enhancing Technologies: the path to anonymity"

Ronald E. Leenes, "*Do They Know Me? Deconstructing Identifiability"*, University of Ottawa Law & Technology Journal, Vol. 4, n. 1-2

Bert-Jaap Koops **"***The trouble with European data protection law*", International Data Privacy Law 2014, vol. 4 n. 4

Ann Cavoukian, "*Privacy by Design, The 7 Foundational Principles*"

Altro

New York Times, "*Big Brother is Us*", James Gleick, 29 Settembre 1996

Conferenza stampa "Facebook to Establish International Headquarters in Dublin, Ireland", Facebook, 2 Ottobre 2008

Wall Street Journal, "*For Your Eyes Only, Europe's New High-Tech Role: Playing Privacy Cop to the World*", David Scheer, 10 Ottobre 2003

Certificazione Safe Harbor Facebook Inc. 05/10/2007, http://safeharbor.export.gov/companyinfo.aspx?id=23019, visitato il 10 Febbraio 2015

Certificazione Safe Harbor di Google Inc. 10/15/2005, http://safeharbor.export.gov/companyinfo.aspx?id=25007, visitato il 10 Febbraio 2015

The Washington Post, "*NSA slides explain the PRISM data-collection program*", pubblicato il 6 Giugno 2013, aggiornato il 10 Luglio 2013

Documentario "*Inside the Mind of Google*", CNBC 3 Dicembre 2009