Il caso Schrems- Facebook: analisi e profili di collegamento con la sentenza Google Spain

di
Andrea Puligheddu

Abstract
L'articolo esamina la sentenza Schrems e le sue implicazioni nell'ambito della giurisprudenza della Corte di giustizia in merito alla protezione dei dati personali. In particolare, si propone un parallelismo con la sentenza Google Spain, dove la Corte ha rivelato un'attitudine espansiva nell'applicazione degli articoli 7 e 8 della Carta dei diritti fondamentali dell'UE nei confronti degli operatori Internet. Alla luce di questa decisione, il caso Schrems documenta una particolare attenzione ai poteri delle autorità nazionali rispetto al trasferimento di dati personali verso paesi terzi.

The article aims at exploring the Schrems case and its implications within the context of the recent Court of Justice activism in the field of data protection. In particular, a comparison is drawn with the Google Spain judgment, where the Court of Justice has taken important steps to enforce Articles 7 and 8 of the Charter of Fundamental Rights of the European Union vis-à-vis internet service providers. In the wake of this decision, the Schrems case has focused on the powers of data protection authorities with respect to the transfer of personal data to third countries.

1. Introduzione

In questo lavoro vengono compiute alcune riflessioni riguardanti la recente vicenda che ha investito il contesto europeo in materia di trattamento dei dati online e di trasferimento dei dati dal territorio dell'Unione Europea agli Stati Uniti, ovvero il caso Schrems v. Data Protection Commissioner [1]. Intorno a questa decisione è rapidamente sorto un forte sottofondo mediatico che, se pur con le diverse sfumature, pretende di individuare all'interno della sentenza una dichiarazione di "illiceità" o una sorta di responsabilità in capo alle società che operano il trasferimento dei dati. Tali affermazioni sono

scaturite a partire dalla dichiarazione di invalidità pronunciata dalla Corte nei riguardi della Decisione 2000/520 della Commissione inerente i principi da seguire in materia di trasferimento dei dati dai due contesti territoriali e individuati all'interno di un trattato denominato Safe Harbor [2]. Un simile approccio risulta fuorviante, ed è necessario mettere in atto le dovute distinzioni del caso. Un'attenzione particolare è quella da rivolgere alle elaborazioni contenute all'interno della sentenza, soffermandosi in particolare sul ruolo e sull'indipendenza delle autorità nazionali al riguardo, e sull'alveo di effettività della Decisione. Essi saranno oggetto di una analisi autonoma, a partire dal main reasoning della Corte e soffermandosi sulle conseguenze implicite che tale decisione comporta. Affinché si possa giungere ad una proficua sintesi conclusiva, verranno presi in esame i profili di collegamento riscontrabili tra tale sentenza e la decisione Google Spain [3]. Proprio a partire dal contenuto di quest'ultima pronuncia merita infatti che sia colto il fulcro della decisione sul caso Facebook, così come rapidamente ribattezzato da una consistente parte della cronaca giornalistica, sia per ciò che concerne le prospettive future legate alla invalidità oggetto della pronuncia, sia per quanto riguarda la ritrovata titolarità potestativa degli Stati membri affinché vengano poste in essere misure specifiche a sostegno del diritto alla protezione dei dati personali in una sua forma più adeguata ai principi sanciti in materia dall'Unione Europea.

2. Sintesi dei fatti oggetto della sentenza Schrems-Facebook.

Nel 2008 uno studente austriaco ed attivista in materia di protezione dei dati personali, Max Schrems, effettuava l'iscrizione al noto social network Facebook, di proprietà e gestione dell'omonima società, Facebook Inc., con sede principale a Palo Alto, California. All'atto dell'iscrizione, Schrems rilevava come, al fine di utilizzare i servizi proposti dalla piattaforma, fosse necessario sottoscrivere un contratto con Facebook Ireland, ovvero una controllata di Facebook Inc., sita in territorio irlandese. In particolare veniva in tale atto specificato come la politica promossa dal portale, nei confronti dei dati raccolti attraverso l'utilizzo da parte degli utenti europei registrati, fosse quello di trasferire tali dati sui server di Facebook Inc., ubicato in California. Pertanto veniva a verificarsi di fatto un trasferimento di dati dal territorio di uno stato membro dell'Unione Europea a quello statunitense. Dopo aver esaminato e discusso in varie forme di protesta pubblica la politica adottata dal social network in materia di privacy, Schrems si rivolgeva nel giugno del 2013 all'Autorità per la protezione dei dati Irlandese, invitandola ad agire nei confronti della società californiana nell'esercizio delle proprie competenze statutarie. Pertanto, egli richiedeva il diniego nei

confronti dell'operazione di trasferimento, anche a seguito delle informazioni divulgate da Edward Snowden riguardo le attività perpetrate dai servizi di intelligence statunitensi [4]. Da parte sua, l'Autorità investita della denuncia negava l'obbligo a procedere, rilevando la domanda priva di fondamento. Schrems proponeva di conseguenza ricorso di fronte all'High Court, la Corte d'appello irlandese. Quest'ultima rilevava come un effettivo accesso massiccio ed indifferenziato ai dati personali sarebbe stato "manifestamente contrario al principio di proporzionalità e ai valori fondamentali protetti dalla Costituzione irlandese" [5]. In particolare il giudice irlandese rilevava come la decisione 2000/520 non fosse più adeguata al soddisfacimento dei requisiti previsti dagli articoli 7 ed 8 della Carta dei diritti fondamentali dell'Unione Europea [6], e pertanto fosse necessario rivedere le modalità con cui potessero essere assicurate le garanzie in materia di riservatezza previste dal diritto dell'Unione. Partendo da queste premesse, la High Court decideva di sospendere il procedimento principale e sottoponeva all'attenzione della Corte di Giustizia dell'Unione Europea alcune questioni pregiudiziali. Precisamente, le richieste proposte dalla Corte d'Appello irlandese si dividevano in due partizioni. La prima richiedeva se, nell'atto di decidere in merito ad una denuncia presentata ad un'autorità indipendente, investita delle funzioni di applicazione e gestione della legislazione in materia di protezione dei dati, vi fosse implicito il rispetto di un vincolo di constatazione in senso contrario espresso dall'Unione all'interno della decisione 2000/520, anche in considerazione degli articoli 7, 8 e 47 e delle disposizioni dell'articolo 25 della Direttiva 95/46 [7]. In secondo luogo veniva domandato se detta autorità potesse condurre una propria indagine sulla questione, alla luce degli sviluppi verificatisi nel frattempo, successivamente alla prima pubblicazione della decisione 200/520.

3. Il main reasoning della Corte.

Per comprendere adeguatamente il ragionamento posto in essere dalla Corte in risposta ai quesiti sollevati, occorre procedere per punti. Innanzitutto, all'interno della pronuncia viene rilevato e riconfermato il ruolo indipendente delle Autorità nazionali di controllo, ideato appositamente affinché esse vigilino sul rispetto delle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali. Precisamente la Corte chiarisce il valore spettante al compito di verifica e controllo inerente le misure poste in atto dai titolari del trattamento, affinché esse risultino efficaci e affidabili. Sotto tale luce e rispetto a tale finalità va valutato il loro operato [8], ed in questo senso l'operazione consistente nel trasferimento dei dati personali da uno Stato membro verso un paese terzo costituisce, alla

luce dei fatti, una forma di trattamento perfettamente qualificabile come tale secondo i dettami dell'articolo 2, lettera b) della Direttiva 95/46 EC. A questo punto del reasoning, una volta riconfermata anche la competenza della Corte a decidere in merito alla validità delle decisioni poc'anzi descritte adottate dalla Commissione, il giudice europeo giunge ad affermare uno dei perni centrali dell'intera sentenza, ovvero che "una decisione della Commissione adottata sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, come la decisione 2000/520, non può impedire alle persone i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo di investire le autorità nazionali di controllo di una domanda" [9]. In altre parole le Autorità nazionali investite della questione hanno il dovere e non già la facoltà di operare una attività di vigilanza e controllo nei confronti delle operazioni di trasmissione dati da uno Stato membro ad uno Stato terzo. La Decisione in oggetto non può e non deve in alcun modo derogare a quanto contenuto nella Direttiva al riguardo[10]. Le autorità in questione devono inoltre poter svolgere tale attività d'esame dei requisiti in piena indipendenza [11], ciò anche in ragione della tutela dei diritti sanciti all'interno della Carta dei diritti fondamentali dell'Unione europea, agli articoli 7 ed 8 [12]. Per questo motivo viene ribadito in conclusione della pronuncia che sul primo quesito proposto, "si deve rispondere alle questioni sollevate che l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, quale la Decisione 2000/520, con la quale la Commissione constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, esamini la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato" [13]. Da un lato la sentenza traccia chiaramente una linea di attribuzione delle competenze in capo alle autorità nazionali, assicurando la tutela dei diritti del singolo. Infatti la Corte rimette direttamente ad esse la valutazione delle domande inoltrate dai cittadini europei, in merito alle garanzie inerenti il trasferimento dei dati. D'altro canto invece viene ricordato che benché le autorità nazionali debbano agire sotto gli auspici della piena indipendenza sostanziale, ciò non significa che possano aggirare gli atti decisionali della Commissione. In altri termini, un conto è confermare una potestà autonoma in capo alle autorità nel decidere sulle segnalazioni ricevute nella piena esplicazione dei loro compiti e nel pieno godimento di una indipendenza sostanziale; un altro è agire in stato di aperta violazione

dei principi vigenti ed approvati in materia. Per questo motivo il giudice europeo ribadisce in capo alla Corte di Giustizia dell'Unione Europea il potere di pronunciarsi sulla validità delle decisioni della Commissione, riferendosi in questo specifico caso alla Decisione 2000/520. Difatti, la seconda parte della sentenza verte su un giudizio di validità della Decisione in questione, partendo dai dubbi sul livello di protezione accordato ai dati trasferiti nei paesi terzi, così come espressi dal ricorrente in sede di domanda. Come ricordato, va ravvisato all'interno dell'articolo 25 paragrafo 6 della Direttiva una facoltà di adozione in capo alla Commissione di atti attestanti il rispetto da parte di un paese terzo di un adeguato livello di protezione dei dati. In un contesto similmente delineato, la Corte afferma che la Commissione era tenuta ad effettuare la valutazione in merito al fatto che gli Stati Uniti fossero in grado di garantire effettivamente, in considerazione della loro legislazione nazionale o dei loro impegni internazionali, un livello di protezione sostanzialmente equivalente a quello garantito dall'Unione Europea a norma della Direttiva 95/46/C. Secondo il giudice europeo, tale facoltà non è stata sostanzialmente esercitata dalla Commissione, la quale si sarebbe limitata ad un semplice esame dei principi contenuti nel regime di Safe Harbor [14]. In conclusione la Corte dichiara che il contenuto della Decisione 2000/520, e di conseguenza anche i principi [15] concordati per "l'approdo sicuro", siano da considerarsi invalidi [16].

4. Conseguenze e prospetto europeo degli effetti della sentenza

Una volta espresso in questo modo il reasoning della Corte, occorre chiedersi quale attualmente sia il quadro normativo a cui fare riferimento per le operazioni di trasferimento dei dati dall'Unione in ambito extraeuropeo. Un punto di riferimento al riguardo deve essere individuato nel documento del Working Party 29 [17] in cui viene espressa l'intenzione da parte dell'organo di operare quanto prima un'analisi dettagliata dell'impatto della sentenza sotto ogni profilo coinvolto nei sistemi di trasferimento dati [18]. Durante questo periodo viene tuttavia raccomandato che il novero delle regole da seguire debba essere considerato quello delle Binding Corporate Rules [19] e delle Standard Contractual Clauses [20]. Un ulteriore aspetto richiamato dal documento del Working Party è quello legato al sistema di sorveglianza di massa oggetto delle rivelazioni di Edward Snowden, ritenuta una questione chiave all'interno dell'analisi svolta dalla Corte e assolutamente incompatibile con il sistema di tutele predisposto dall'Unione Europea in materia di protezione dei dati [21]. Anche in considerazione dei motivi ora esposti, viene ribadita la necessità di una ulteriore discussione sui principi e le modalità che regolano il trasferimento, auspicando quanto prima

l'individuazione di una soluzione appropriata [22]. Dello stesso avviso risulta essere la Commissione Europea dopo il comunicato rilasciato successivamente, che sostanzialmente conferma ed analizza l'impatto che il giudizio ha nei confronti delle imprese operanti nel territorio europeo che raccolgono e trasferiscono dati in territorio statunitense [23]. Formale e sostanziale ricezione è inoltre quella riscontrabile da parte del Garante per la protezione dei dati personali italiano il quale ha dichiarato decaduta, attraverso specifico provvedimento, l'autorizzazione emanata a suo tempo con cui si consentivano le operazioni di trasferimento, sostanzialmente basata sull'accordo Safe Harbor e sui principi in esso contenuti [24]. Di fronte all'insieme delle risposte evidenziate, un fattore risulta essenzialmente comune: la necessità urgente di un impianto normativo adeguato. Difatti il problema evidenziato anche da parte della dottrina internazionale in merito, sposta il baricentro interpretativo dalle facoltà esercitabili da parte delle Autorità nazionali al comportamento conseguente che d'ora in avanti le società nel settore, aventi un centro d'interesse europeo, proporranno all'interno del mercato corrispondente [25]. Se da un lato infatti non viene sancita alcuna forma di responsabilità specifica in capo alla società operante attività di trasferimento [26], è anche vero che un quadro normativo così invalidato e precario non può incontrare il favore di chi operi commercialmente attraverso la raccolta e l'elaborazione dei dati [27], anche a partire dalla stessa dicitura della Corte che sembrerebbe lasciare spazio ad ulteriori problematiche, in particolare riguardo al significato della dicitura inerente un adeguato livello di protezione richiesto [28].

5. Caso Google Spain e caso Facebook: una sintesi dei valori e dei principi condivisi.

Esaminando i punti enucleati e la dinamica decisionale che caratterizza la sentenza del Caso Schrems, è possibile individuare un parallelismo ben preciso con un ulteriore caso di recente pronuncia da parte della medesima Corte, ovvero il caso Google Spain. Quest'ultima vicenda presenta infatti interessanti aspetti in comune con il caso ora esaminato, che costituiscono importanti tasselli nel quadro della giurisprudenza europea in materia di tutela dei diritti fondamentali. Un primo elemento di interesse è senza dubbio costituito dalla differenza esistente tra le due decisioni in materia di responsabilità dei fornitori di servizi della società dell'informazione. Mentre viene infatti rilevato all'interno del caso Google Spain una forma di responsabilità in capo al motore di ricerca quale soggetto titolare del trattamento dei dati per ciò che concerne l'attività di indicizzazione [29], tale assunto non viene analogamente applicato a Facebook per il quale non è

menzionata alcuna forma di responsabilità per l'adeguatezza del trattamento, e per il quale viene spostato il fulcro sull'appropriatezza dei parametri entro i quali la società avrebbe dovuto agire. Certamente le domande proposte e gli oggetti di doglianza sono nettamente differenti; tuttavia sotto il profilo del comportamento posto in essere, in particolare sul versante del trattamento dei dati personali, le due società californiane possiedono elementi in comune di non poca rilevanza. Meritano di essere menzionati in modo specifico due aspetti: la rinnovata importanza della tutela dei diritti fondamentali della personalità e la questione della territorialità del dato. In entrambi i casi citati, uno dei punti chiave è senza alcun dubbio rappresentato dall'interpretazione da accordare agli articoli 7 ed 8 della Carta dei diritti fondamentali dell'Unione Europea, rispettivamente riguardanti il rispetto della vita privata e familiare e la protezione dei dati di natura personale. Sul tema la giurisprudenza europea sembra essere rimasta sostanzialmente concorde, rinvenendo in entrambi gli articoli la fonte prima da cui attingere per aggiornare ed estendere l'adeguatezza delle tutele del singolo e dei suoi diritti fondamentali [30]. Risulta interessante infatti notare come sia nel caso Google Spain che nel caso Schrems si sia data assoluta rilevanza all'esigenza di tutela dei diritti fondamentali del singolo, da un lato per quanto concerne il diritto all'oblio e le modalità predisposte per la sua integrazione nell'insieme dei servizi proposti, dall'altro nella dichiarazione di necessario controllo da parte delle autorità nazionali di fronte alle richieste di coloro i quali desiderino informazioni relative all'adeguatezza delle tutele predisposte per l'attività di trasferimento. Proprio tale operazione richiama un ulteriore aspetto trattato all'interno di entrambe le decisioni, ovvero la questione della territorialità. Anche se la problematica affrontata in Google Spain verteva sull'applicazione del principio di territorialità, enucleabile dall'articolo 4 della Direttiva 95/46 EC, nei confronti del trattamento effettuato nel contesto delle attività di stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, la similitudine riscontrabile con il caso oggetto dell'analisi sino ad ora proposta risulta evidente sul piano della essenzialità nell'individuare il territorio a cui fare riferimento per collegare l'attività di trattamento e le relative garanzie. In altre parole, si deve ritenere esteso anche al territorio extraeuropeo il novero di garanzie individuali a tutela dei diritti fondamentali, e tale sussistenza prescinde anche in questo dal luogo in cui il trattamento viene effettuato qualora la società che operi il trattamento eserciti la propria attività nel contesto europeo. Ancora una volta il contesto geografico si rivela non semplicemente rilevante, ma assolutamente decisivo.

6. Conclusioni

A parere di chi scrive, il caso Schrems sembra collocarsi a piena ragione in una ottica di riconferma, da parte della Corte, dell'esigenza di autonomia potestativa da ripartirsi in capo ai singoli Stati membri. Nonostante da un lato essa sia foriera di una rinnovata sensibilità sul tema e sull'impellente necessità di una tutela conforme alle garanzie europee dei loro diritti, dall'altro lato desta perplessità sul fronte della politica del diritto, sollevando interrogativi circa l'adeguatezza degli strumenti normativi che succederanno al trattato e circa la risposta messa in campo dalle società operanti attraverso controllate all'interno dell'Unione, pur avendo centrale dei propri interessi in USA [31]. Per ciò che concerne il versante europeo, risulta particolarmente interessante la chiarezza espressa dalla Corte riguardo il comportamento delle autorità nazionali ed il loro ruolo di entità indipendente nel valutare le domande poste da una persona "riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato". Seguendo il dettato stabilito dall'art. 25 paragrafo 6 della direttiva, interpretato alla luce della Carta dei diritti fondamentali dell'Unione Europea ed in particolare degli articoli 7,8 e 47. Sarebbe lecito dunque attendersi dopo questa pronuncia un maggiore interesse in materia in capo alle autorità garanti e preposte al controllo, ed una maggior attenzione riguardo le richieste debitamente motivate [32]. Certamente una riforma che aggiorni nel più breve tempo possibile la normativa in materia è la soluzione auspicabile per ogni operatore del settore. Sicuramente sono inoltre da attendersi importanti sviluppi conseguenti questa pronuncia e i vari provvedimenti adottati dalle istituzioni europee, in particolare per ciò che concerne il profilo della sorveglianza di massa così come eccepita dal documento del Working Party 29 [33]. Un'interessante fattore di novità potrebbe essere quello apportato dalla proposta del progetto di regolamento per la protezione dei dati personali attualmente al vaglio delle istituzioni europee [34]. Una sintesi dei principi implicati certo non di facile attuazione, ma quanto prima necessaria affinché si rigeneri un clima di reciproca affidabilità verso il quadro normativo del settore.

Note:

[*] Il presente contributo è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente del Comitato di Referee secondo il Regolamento adottato da questa Rivista.

[1] Sentenza C-362/14, Schrems v. Data Protection Commissioner,

[2] Si fa riferimento alla Decisione 2000/520/EC, Official Journal L 215, 2000 P. 0007- 0047

[3] Si fa riferimento alla sentenza C-131/12 Google Spain SL,Google Inc. V. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 13 Maggio 2014. La decisione della Corte rappresenta un vero e proprio milestone case in materia di diritto all'oblio. In particolare, con riferimento al tema trattato in questo elaborato, tale sentenza è stata decisiva per delineare l'orientamento della Corte riguardo all'interpretazione degli articoli 7 ed 8 della Carta dei diritti fondamentali dell'Unione Europea e sulla applicazione estensiva del principio di territorialità.

[4] In particolare veniva rilevato come simili dinamiche avessero pregiudicato in maniera grave i diritti inviolabili dei cittadini europei coinvolti in tali programmi di sorveglianza di massa. Il meccanismo di spionaggio evidenziato dalle rivelazioni di Snowden e mutato ora in un programma di sorveglianza di massa collegabile alla NSA, ha generato una vera e propria ondata di sensibilizzazione nei confronti della sicurezza informatica globale.

[5] Sentenza C-362/14, Schrems v. Data Protection Commissioner, par. 33

[6] Carta dei Diritti Fondamentali dell'unione Europea, 2000/C 364/01

[7] In particolare viene ribadita dalla Corte la necessità di corretta interpretazione del par. 6 ove viene riportato che "La Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona. Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione"

[8] Sentenza C-362/14, Schrems v. Data Protection Commissioner, par. 41

[9] Sentenza C-362/14, Schrems v. Data Protection Commissioner, par. 53

[10] Si fa qui riferimento precisamente al contenuto dell'Art. 28 par 4 della Direttiva 95/46 EC "Qualsiasi persona, o associazione che la rappresenti, può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali. La persona interessata viene informata del seguito dato alla sua domanda. Qualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali

adottate a norma dell'articolo 13 della presente direttiva. La persona viene ad ogni modo informata che una verifica ha avuto luogo"
[11] Sentenza C-362/14, Schrems v. Data Protection Commissioner, par. 57
[12] Sentenza C-362/14, Schrems v. Data Protection Commissioner, par. 63
[13] Sentenza C-362/14, Schrems v. Data Protection Commissioner, par. 66
[14] Si veda al riguardo all'interno della pronuncia C-362/14, Schrems v. Data Protection Commissioner, il paragrafo 97, in cui si evince che la Commissione, nella decisione 2000/520, non ha affermato che gli Stati Uniti d'America «garantiscono» effettivamente un livello di protezione adeguato in considerazione della loro legislazione nazionale o dei loro impegni internazionali ; ciò viene riaffermato anche nel comunicato emanato dalla stessa Corte, ove si afferma che "le esigenze afferenti alla sicurezza nazionale, al pubblico interesse e all'osservanza delle leggi statunitensi prevalgono sul regime del Safe Harbor, cosicché le imprese americane sono tenute a disapplicare, senza limiti, le norme di tutela previste da tale regime laddove queste ultime entrino in conflitto con tali esigenze"(comunicato stampa n.117/15 della Corte di Giustizia)
[15] I principi in oggetto sono così riassumibili: 1) Gli utenti devono essere avvertiti sulla raccolta e l'utilizzo dei propri dati personali; 2) Ciascuno deve essere libero di rifiutare la raccolta dei dati e il loro trasferimento a terzi; 3) I dati possono essere trasferiti solo a organizzazioni che seguono principi adeguati di protezione dei dati; 4) Le aziende devono fornire garanzie contro il rischio che i dati vengano smarriti.
[16] In particolare il ragionamento della Corte ruota attorno alla valutazione degli articoli da 1 al 4 della decisone, considerati inseparabili e dei relativi allegati.
[17] Il Gruppo è stato istituito dall'art. 29 della direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione.
[18] Ove è previsto all'interno del document del W.P. Art.29 che "In the meantime, the Working Party will continue its analysis on the impact of the CJEU judgment on other transfer tools. During this period, data protection authorities consider that Standard Contractual Clauses and Binding Corporate Rules can still be used. In any case, this will not prevent data protection authorities to investigate particular cases, for instance on the basis of complaints, and to exercise their powers in order to protect individuals. If by the end of January 2016, no appropriate solution is found with the US authorities and depending on the assessment of the transfer tools by the Working Party, EU data protection authorities are committed to take all

necessary and appropriate actions, which may include coordinated enforcement actions" (http://ec.europa.eu/justice/data- protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf)

[19] Si tratta di uno strumento volto a consentire il trasferimento di dati personali dal territorio dello Stato verso Paesi terzi (extra-UE) tra società facenti parti dello stesso gruppo d'impresa.
Si concretizzano in un documento contenente una serie di clausole (rules) che fissano i principi vincolanti (binding) al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo (corporate). Le Bcr costituiscono un meccanismo in grado di semplificare gli oneri amministrativi a carico delle società di carattere multinazionale con riferimento ai flussi intra-gruppo di dati personali. (Così secondo quanto riportato dal Garante e liberamente consultabile all'indirizzo: http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi#3)

[20] La Commissione europea, ai sensi dell'articolo 26(4) della Direttiva 95/46/CE, può stabilire che determinati strumenti contrattuali consentono di trasferire dati personali verso Paesi terzi. Si tratta di una delle deroghe (stabilite nel comma 2 dell'articolo 26 della Direttiva 95/46/CE) al divieto di effettuare il trasferimento verso Paesi che non offrono garanzie "adeguate" in materia di protezione dei dati personali. Utilizzando il testo delle clausole contrattuali in questione in un contratto utilizzato per il trasferimento, l'esportatore dei dati garantisce che questi ultimi saranno trattati conformemente ai principi stabiliti nella Direttiva anche nel Paese terzo di destinazione

[21] "It recalls that it has consistently stated that such surveillance is incompatible with the EU legal framework and that existing transfer tools are not the solution to this issue. Furthermore, as already stated, transfers to third countries where the powers of state authorities to access information go beyond what is necessary in a democratic society will not be considered as safe destinations for transfers. In this regard, the Court's judgment requires that any adequacy decision implies a broad analysis of the third country domestic laws and international commitments."

[22] Il termine indicato all'interno del documento del WP29 è temporaneamente fissato entro la fine Gennaio 2016

[23] Si fa riferimento alla COM(2015) 566, on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems) Per una consultazione dettagliata si invita a consultare la versione integrale

del documento reperibile all'indirizzo: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf

[24] Si fa riferimento al Provvedimento del 22 Ottobre 2015, Trasferimento dati personali verso gli USA: caducazione provvedimento del Garante del 10.10.2001 di riconoscimento dell'accordo sul c.d. "Safe Harbor". In esso viene sinteticamente annunciata la ricezione dell'invalidità del Safe Harbor e dichiarata l'urgenza di una normativa necessaria di sostituzione, con la massima cooperazione da parte dell'Autorità affinché ciò avvenga quanto prima.

[25] "The ruling could have a significant impact on the way American companies can store and transfer data on European citizens. In addition to potentially stricter privacy requirements, American companies may have to navigate more than 20 different policies adopted by European member states, rather than a single E.U. wide policy. In the meantime, U.S. and E.U. officials are continuing ongoing negotiations over the so-called "Safe Harbor 2.0," which would create a more privacy-protective transatlantic agreement. The ruling has also prompted renewed calls for further surveillance reform in the United States". (Così D. Kehl European Court of Justice invalidates key part of EU-USA Safe Harbor agreement, 4/11/2015 e reperibile all'indirizzo: http://jolt.law.harvard.edu/digest/privacy/european-court-of-justice-invalidates-key-part-of-u-s-e- u-safe-harbor-agreement)

[26] In capo a Facebook non è stata riscontrata alcun tipo di responsabilità specifica per le modalità di trattamento dei dati degli utenti, e ciò è da ritenersi analogicamente conseguente per la categoria di società assimilabili da un punto di vista operativo.

[27] In particolare il problema verterebbe sulle modalità con cui garantire la qualità del trattamento. Un'ipotesi possibile potrebbe essere quella di richiedere il semplice consenso per il trattamento dei dati personali all'estero direttamente agli utenti, modificando così le condizioni dei servizi offerti. Resta da vedere se alla luce dei procedimenti descritti nella COM(2015) 566 della Commissione ciò sia concretamente attuabile.

[28] "La Corte[...] non esclude che l'Autorità di controllo di uno Stato membro[...] esamini la richiesta di una persona circa la tutela dei suoi diritti e delle libertà in materia di trattamento dei dati personali a fronte del trasferimento dei suoi dati personali da uno Stato membro a un Paese terzo, quando si ritenga che la legge e la prassi del Paese terzo non garantiscano un adeguato livello di protezione" In particolare risulta complesso poter determinare, data l'assenza di parametri adeguati, quale sia l'asse di riferimento per determinare l'adeguatezza delle misure inerenti le operazioni di trasferimento dati.

[29] Si veda il par. 41 della sentenza google spain in cui viene riconosciuta la responsabilità in capo al gestore di un motore di ricerca qualora l'attività di trattamento si concretizzi "nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza" (Corte di Giustizia Europea, 13 Maggio 2014, C- 131/12 par. 41)

[30] In Google Spain l'interpretazione corretta degli articoli 7 ed 8 della Carta è risultata essenziale per sancire il riconoscimento del diritto all'oblio come diritto fondamentale della persona e come manifestazione strumentale del diritto alla riservatezza in contemperanza con la libertà di espressione (si veda paragrafo 81 della sentenza Google Spain). Similmente anche all'interno della sentenza Schrems il fattore interpretativo degli articoli in oggetto è risultato di fondamentale importanza nella interpretazione dell'articolo 25 paragrafo 6 della Direttiva 95/46/CE, così come ricordato dal giudice europeo in sede conclusiva.

[31] Va ricordato qui qualora non si dovesse addivenire ad una soluzione politicamente condivisa, sarà cura della Corte stessa provvedere all'individuazione di un novero di principi attuabili in materia. Come già ricordato nel documento (metti coordinate) del WP 29, il termine attualmente concordato è la fine del mese di gennaio 2016. Un altro fattore di non scarsa rilevanza è costituito dal giudizio tuttora in corso tra Microsoft ed il governo statunitense (United States v. Microsoft Corporation 253 F.3d 34), che verte sulla soggezione della società al warrant federale anche per dati degli utenti conservati nel suolo UE. Se dovesse infatti permanere il criterio di prevalenza della nazionalità dell'impresa sulla territorialità del dato, saranno favorite le imprese stabilmente residenti all'interno dell'Unione Europea per i dati in essa trattati; mentre se dovesse prevalere il criterio della territorialità su quello della nazionalità dell'impresa, le imprese dominanti resteranno in territorio statunitense e tratteranno il dato all'interno dell'Unione ed attraverso strutture proprie site in territorio europeo.

[32] il testo della pronuncia riporta chiaramente la necessità di una congrua struttura che dimostri la lesione della qualità del trattamento quando dice "qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato"

[33] Al riguardo si veda qui: http://www.nytimes.com/2015/11/07/technology/europe-wants-to-reach-data-transfer-pact-by-early-2016.html?_r=0

[34] In January 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU. The completion of this reform is a policy priority for 2015. The objective of this new set of rules is to give

citizens back control over of their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritised. The reform will allow European citizens and businesses to fully benefit from the digital economy. (http://ec.europa.eu/justice/data-protection/)