Paola Piroddi

I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems *e nel nuovo regolamento generale sulla protezione dei dati*

Sommario: Considerazioni introduttive. – 1. Il quadro generale del trasferimento dei dati personali verso Stati terzi nella direttiva 95/46/CE. – 2. La decisione della Commissione relativa al «Safe Harbor» e il contesto fattuale del caso *Schrems*. – 3. La sentenza della Corte di giustizia: la 'piena indipendenza' delle autorità nazionali di controllo e la dichiarazione di invalidità della decisione della Commissione relativa al «Safe Harbor». Gli effetti della sentenza. – 4. La proposta relativa a una nuova decisione di adeguatezza della Commissione: il «Privacy Shield». – 5. I trasferimenti dei dati verso Stati terzi, le decisioni di adeguatezza della Commissione e i poteri delle autorità nazionali di controllo nel nuovo regolamento generale sulla protezione dei dati personali. – Conclusioni.

Considerazioni introduttive

Con la sentenza nel caso *Schrems c. Data Protection Commissioner*[1], la Corte di giustizia aggiunge un significativo tassello alla sua giurisprudenza volta ad adeguare alla Carta dei diritti fondamentali dell'Unione europea l'interpretazione della direttiva 95/46/CE, relativa alla tutela delle persone con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati[2].

Si tratta di una giurisprudenza evolutiva: infatti, quando è stata ema-

[1] Corte di giustizia dell'Unione europea (grande sez.), 6 ottobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, causa C-362/14, ECLI:EU:C:2015:650.

[2] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in *G.U.C.E.*, L 281 del 23 novembre 1995, p. 31 ss., modificata dall'all. II al regolamento (CE) 1882/2003 del Parlamento europeo e del Consiglio del 29 settembre 2003 recante adeguamento alla decisione 1999/468/CE del Consiglio delle disposizioni relative ai comitati che assistono la Commissione nell'esercizio delle sue competenze di esecuzione previste negli atti soggetti alla procedura prevista all'art. 251 Tr. CE, *ibid.*, L 284 del 31 ottobre 2003, p. 1 ss.

nata la direttiva, vent'anni fa, il diritto alla protezione dei dati personali non era ancora riconosciuto come diritto fondamentale nella Comunità europea. Questo diritto era tutelato soltanto nell'ambito del Consiglio d'Europa, in particolare dalla convenzione di Strasburgo n. 108 sulla protezione delle persone nel trattamento automatizzato dei dati di carattere personale[3], che all'epoca risultava già in vigore per diversi Stati membri della Comunità, e dall'art. 8 della Convenzione per i diritti dell'uomo e le libertà fondamentali («CEDU»), relativo al diritto al rispetto della vita privata e familiare[4]. Il diritto di 'ogni persona' alla protezione dei dati di carattere personale che la riguardano è stato introdotto nell'ordinamento giuridico dell'Unione europea soltanto dall'art. 8 della Carta dei diritti fondamentali[5] – peraltro inizialmente con efficacia dichiarativa e non vincolante. La Carta ha ottenuto «lo stesso valore giuridico dei trattati» solamente con il Trattato di Lisbona, che ha modificato l'art. 6, par. 1 TUE, e ha contestualmente riaffermato il diritto incondizionato alla protezione dei dati personali nell'art. 16 TFUE[6].

[3] Convenzione STCE n. 108, firmata a Strasburgo il 28 gennaio 1981, entrata internazionalmente in vigore il 1º ottobre 1985, per l'Italia il 1º luglio 1997 e per la Comunità europea il 15 giugno 1999 (v. *Amendments to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS no. 108) Allowing the European Communities to Accede*, adottati dal Comitato dei Ministri a Strasburgo il 15 giugno 1999). Si noti che la Corte europea dei diritti dell'uomo non esercita giurisdizione su questo strumento, aperto anche all'adesione di Stati non membri del Consiglio d'Europa. Cfr. anche il 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 (STCE n. 181), firmato a Strasburgo l'8 novembre 2001, entrato in vigore il 1° luglio 2004. Su altri sviluppi internazionali del diritto alla protezione dei dati personali cfr. Ch. Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future*, in *Tilburg University Legal Studies Working Papers*, No. 16/2010, p. 9 ss.; L. Bygrave, *Privacy and Data Protection in an International Perspective*, in *Scandinavian Studies in Law*, 2010, p. 165 ss.

[4] Cfr., ad es., l'affermazione della Corte di giustizia nella sentenza 20 maggio 2003, Österreichischer Rundfunk, nelle cause riunite C-465/00, C-138/01 e C-139/01, in *Racc.*, 2003, p. I-4989 ss., par. 70: «La stessa direttiva 95/46, *pur avendo come obiettivo principale quello di garantire la libera circolazione dei dati personali*, prevede, al suo art. 1, n. 1, che «[g]li Stati membri garantiscono […] la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali'».

[5] Sull'art. 8 della Carta, cfr. P. Piroddi, *Art. 8 Carta dei diritti fondamentali dell'Unione europea*, in F. Pocar, M.C. Baruffi (a cura di), *Commentario breve ai trattati dell'Unione europea*, 2° ed., Padova, 2014, p. 1682 ss.

[6] Sull'art. 16 TFUE, che ha recuperato l'art. I-51 Tr. Cost., cfr. P. Piroddi, *Art. 16 TFUE*, in F. Pocar, M.C. Baruffi (a cura di), *Commentario breve* cit., p. 189 ss. In precedenza,

La giurisprudenza della Corte di giustizia ha contribuito in modo significativo all'evoluzione del diritto alla protezione dei dati personali come diritto fondamentale della persona nell'Unione europea, applicando all'interpretazione della direttiva 95/46/CE non soltanto l'art. 8 della Carta, ma anche il più consolidato diritto alla riservatezza, salvaguardato dall'art. 7 della stessa Carta e dall'art. 8 della CEDU nel quadro del diritto al rispetto della vita privata e familiare[7]. Basti ricordare, tra le sentenze più note di questa giurisprudenza, quella nel caso *Schecke e Eifert*[8]; la sentenza nel caso *Digital Rights Ireland*[9], che ha annullato la direttiva 2006/24/CE sulla conservazione dei dati generati o trattati nell'ambito dei servizi pubblici di comunicazione elettronica e di reti pubbliche di telecomunicazione; e infine la recente pronuncia nel caso *Google Spain*[10].

La sentenza *Schrems* si inserisce in questa giurisprudenza, che ultima-

l'art. 286 Tr. CE, inserito dal Tr. Amsterdam (*ex* art. 213B Tr. CE), aveva già stabilito l'applicazione della direttiva 95/46/CE alle istituzioni e agli organismi dell'Unione, e aveva previsto la nascita del «Garante europeo della protezione dei dati», formalmente istituito dall'art. 41 del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio del 18 dicembre 2000 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, in *G.U.C.E.*, L 8 del 12 gennaio 2001, p. 1 ss.

[7] Cfr. Corte di giustizia, 9 novembre 2010, Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen, cause riunite C-92/09 e C-93/09, in Racc., 2010, p. I-11063 ss., par. 47 ss., nella quale la Corte mette in stretta relazione l'art. 8 CEDU e gli artt. 7 e 8 della Carta attraverso il riferimento all'art. 52, par. 3 e all'art. 53 della stessa Carta, creando in tal modo un anello di congiunzione tra la CEDU e il sistema di tutela dei diritti fondamentali proprio dell'ordinamento giuridico dell'Unione europea. Questo già prima dell'entrata in vigore del Trattato di Lisbona che, attraverso l'introduzione dell'art. 6, par. 3 TUE ha attribuito efficacia vincolante alla CEDU nell'Unione. Per un caso di applicazione del solo art. 8 CEDU alla direttiva 95/46/CE, v. Corte di giustizia, 20 maggio 2003, C-465/00, Österreichischer Rundfunk cit., par. 68. Per la giurisprudenza della Corte di giustizia che interpreta la direttiva 95/46/CE alla luce della Carta dei diritti fondamentali dell'Unione europea, cfr., per tutti, F. Bestagno, Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali, in Il dir. dell'Un. Eur., 2015, p. 25 ss.

[8] Corte di giustizia, 9 novembre 2010, *Schecke e Eifert* cit., spec. par. 52, 65. V. *supra*, nota 7.

[9] Corte di giustizia, 8 aprile 2014, *Digital Rights Ireland Ltd et al. c. Minister for Communications, Marine and Natural Resources*, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238.

[10] Corte di giustizia, 13 maggio 2014, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, causa C-131/12, ECLI:EU:C:2014:317, sulla quale si veda il volume monografico di *Dir. Inf.* n. 4-5 del 2014, e G. Resta, V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015.

mente sembra aver subito un'improvvisa accelerazione: la rapidità con la quale è stata decisa questa sentenza, pubblicata a pochissimi giorni di distanza dalla presentazione delle conclusioni dell'Avvocato generale[11], è inusuale per la Corte. Oltretutto, nel giro di una settimana, è stata pronunciata anche la sentenza nel caso *Weltimmo* e quella nel caso *Smaranda Bara*[12], tutte a seguito di rinvii pregiudiziali relativi all'interpretazione della direttiva 95/46/CE. Sembra che i giudici abbiano voluto affrettare la decisione dei casi ancora pendenti in questa materia, presumibilmente per approfittare dell'opportunità di poter ancora influire sul testo del nuovo regolamento generale di protezione dei dati[13]. Destinato a sostituire la direttiva nel quadro della riforma globale della disciplina relativa alla protezione ai dati personali nell'Unione europea, il regolamento si avvia infatti verso la conclusione dell'*iter* legislativo previsto per la sua approvazione. La Corte di giustizia, con la sentenza *Schrems*, sembra voler contribuire a definirne gli ultimi contorni ancora incerti.

[11] Conclusioni dell'Avv. gen. Y. Bot presentate il 23 settembre 2015, ECLI:EU:C:2015:627.

[12] Rispettivamente, sentenza 1° ottobre 2015, causa C-230/14, *Weltimmo*, ECLI:EU:C:2015:639; sentenza 1° ottobre 2015, causa C-201/14, *Smaranda Bara et al.*, ECLI:EU:C:2015:638.

[13] Cfr. la proposta relativa ad un regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, COM(2012)11 def. - 2012/0011(COD). Gli altri atti che fanno parte del «pacchetto» proposto dalla Commissione sono la comunicazione *Salvaguardare la privacy in un mondo interconnesso - Un quadro europeo della protezione dei dati per il XXI secolo*, COM(2012)9 def.; una proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati (COM(2012)10 def. – 2012/0010 (COD)), destinata a sostituire la decisione quadro 2008/977/GAI del Consiglio del 27 novembre 2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (in *G.U.U.E.*, L 350 del 30 dicembre 2008, p. 60 ss.); e infine la relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, basata sull'art. 29, par. 2, della decisione quadro 2008/977/GAI (doc. COM(2012)12, con l'allegato SEC(2012)75 def.), relativa all'attuazione di questa decisione negli Stati membri.

1. Il quadro generale del trasferimento dei dati personali verso Stati terzi nella direttiva 95/46/CE.

La direttiva 95/46/CE (nel prosieguo: la 'direttiva') definisce il quadro generale del trattamento dei dati personali nell'Unione europea, sia sotto l'aspetto relativo alla protezione dei diritti delle persone interessate, sia sotto l'aspetto relativo alla garanzia della libertà di circolazione di tali dati tra gli Stati membri dell'Unione e gli Stati membri dell'Accordo relativo allo spazio economico europeo[14]. Emanata sulla base giuridica delle norme del Trattato relative al ravvicinamento delle legislazioni[15], la direttiva persegue l'obiettivo di garantire la libertà di circolazione dei dati personali nel mercato interno attraverso l'armonizzazione delle garanzie nazionali di tutela della riservatezza rispetto al trattamento di questi dati.

Il principio generale stabilito da questo strumento è che gli Stati membri «non possono restringere o vietare la libera circolazione dei dati personali…, per motivi connessi alla tutela… dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali» (art. 1, par. 2 e 1). Il legislatore riteneva infatti che, per effetto del ravvicinamento delle legislazioni nazionali, la protezione equivalente dei diritti individuali non avrebbe più consentito agli Stati membri di ostacolare la libera circolazione di dati personali nel mercato interno per ragioni inerenti alla tutela delle persone fisiche[16].

Quando i dati delle persone residenti negli Stati membri sono trasferiti verso Stati terzi, il principio della libertà di circolazione è sostituito, nella direttiva, da un principio di autorizzazione condizionata: è consentito trasferire verso un Paese terzo i dati personali raccolti negli Stati membri dell'Unione soltanto se questo Stato garantisce un livello di protezione

[14] Infatti, la direttiva 95/46/CE è stata inserita nell'Accordo relativo allo «spazio economico europeo» («SEE/EEA») con l'art. 2 della decisione del Comitato misto SEE n. 83/1999 del 25 giugno 1999, che modifica il protocollo n. 37 e l'all. XI (servizi di telecomunicazione) dell'Accordo «SEE» (in *G.U.C.E.*, L 296 del 23 novembre 2000, p. 41 ss.). Inoltre, la direttiva è stata inclusa nell'all. B dell'Accordo del 26 ottobre del 2004 tra l'UE, la CE e la Confederazione svizzera (che non è Stato contraente dell'Accordo SEE, ma è parte dell'«Associazione europea di libero scambio», «AELS/EFTA»), riguardante l'associazione di quest'ultima all'attuazione, all'applicazione e allo sviluppo dell'*acquis* di Schengen (*ibid.*, L 53 del 27 febbraio 2008, p. 52 ss.).

[15] Art. 100A Tr. CE, ora art. 114 TFUE: v. il preambolo della direttiva.

[16] V. considerando 7, 8 e 9 della direttiva. Cfr., in proposito, le conclusioni dell'avv. gen. A. Tizzano presentate il 19 settembre 2002, nel caso *Bodil Lindqvist*, in causa C-101/01, in *Racc.*, 2003, p. I-12971 ss., par. 39.

'adeguato' dei dati stessi. Scopo di questa disposizione è evidentemente quello di evitare che la tutela garantita dal legislatore dell'Unione possa esser aggirata semplicemente trasferendo i dati verso Stati terzi con ordinamenti giuridici meno protettivi.

La direttiva tuttavia non definisce in cosa consista il 'trasferimento' di dati personali. In proposito, l'art. 25, par. 1 si limita a indicare che possono essere trasferiti tanto dati già trattati, quanto dati destinati a essere oggetto di trattamento nel Paese terzo nel quale vengono inviati. La Corte di giustizia ha apportato una significativa precisazione a questa nozione nella sentenza sul caso *Bodil Lindqvist*, che ha chiarito che l'inserimento di dati personali in una pagina di un sito *web* non configura un 'trasferimento' dall'Unione europea verso un Paese terzo ai sensi della direttiva, per il solo fatto di aver reso tali dati accessibili, attraverso un collegamento *internet*, a destinatari che si trovano fisicamente al di fuori dell'Unione europea[17]. In caso contrario, infatti, qualora cioè una pubblicazione *online,* di dati configurasse un 'trasferimento', ai sensi della direttiva, questo dovrebbe ritenersi indirizzato verso tutti quei Paesi terzi in cui esistono i mezzi tecnici per consentire di accedere alla pagina *web* attraverso un collegamento *internet*. Di conseguenza, ogni trasferimento di dati richiederebbe l'applicazione generalizzata della direttiva verso un numero indefinito di Stati (se non verso tutti), effetto certo non voluto dal legislatore. La Corte esclude quindi l'applicabilità della direttiva a quella specifica trasmissione di dati costituita dalla pubblicazione in un sito *web* accessibile anche da un Paese terzo, asserendo che non configura un 'trasferimento' di dati da un mittente a un destinatario, ai sensi della direttiva stessa.

È evidente che, con questa interpretazione, la Corte intende evitare di aggravare l'onere di *compliance* accollato al responsabile del trattamento che trasferisca dati verso Stati terzi attraverso un sito *web*[18]. Tuttavia, la

[17] Corte di giustizia, 6 novembre 2003, *Procedimento penale a carico di Bodil Lindqvist*, causa C-101/01, in *Racc*., 2003, p. I-12971 ss., par. 57 ss., spec. par. 71.

[18] Cfr. Y. Poullet, *Transborder Data Flows and Extraterritoriality: The European Position*, in *Journ. Intern. Comm. Law & Techn*., 2007, p. 141 ss., , il quale osserva (a p. 149) che la Corte utilizza un argomento non corretto sotto l'aspetto tecnico: infatti, essa considera come mittente di un trasferimento di dati che avvenga attraverso un collegamento *internet* ad un sito *web* non il *webmaster* (o, comunque, il creatore del sito), cioè la persona che ha caricato effettivamente i dati personali sulla pagina, ma l'*hosting provider*, cioè il soggetto che fornisce il servizio di rete che consiste nell'allocare il sito su un *server web*. Secondo la Corte non si configura un «trasferimento» di dati dall'Unione europea verso un Paese terzo ai sensi della direttiva, poiché i dati non vengono trasmessi *direttamente* dal mittente al destinatario, ma vengono caricati sul sito *web* da un soggetto terzo, cioè dall'*hosting provider*. Pertanto, senza che rilevi il fatto che il *server* dell'*hosting provider*

decisione della Corte non è esente da critica, a causa della sua motivazione: qual è infatti la differenza sostanziale fra 'trasferire' i dati da uno Stato membro ad uno specifico destinatario che si trovi in un Paese terzo (ad esempio, attraverso l'*e-mail*) e 'rendere accessibili' gli stessi dati allo stesso destinatario via *internet*, attraverso la pagina di un sito caricato sul *web* da un responsabile del trattamento stabilito in uno Stato membro[19]? È evidente che non vi è alcuna differenza sostanziale, ma soltanto l'utilizzo di un diverso mezzo tecnico.

La differenza ci sarebbe soltanto nel caso in cui il mittente (il *webmaster* del sito, responsabile del trattamento *ex* art. 2, lett. *d* della direttiva) non avesse la possibilità tecnica di restringere l'accesso al sito ai soli destinatari del trasferimento: cioè, nel caso in cui non potesse escludere dalla ricezione dei dati tutti coloro che non sono destinatari specifici del trasferimento[20]. È stato tuttavia osservato che in questo caso (eccezionale) verrebbe tuttavia in considerazione l'art. 4, par. 1, lett. *c* della direttiva[21], che prevede l'applicazione delle legislazioni nazionali di attuazione della direttiva al trattamento di dati personali effettuato per mezzo di «strumenti, automatizzati o non automatizzati», situati nel territorio degli Stati membri, anche se il responsabile del trattamento non è stabilito nell'Unione europea. È indubbio, infatti, che l'azione consistente nel caricare dati personali su una pagina di un sito *web*, effettuata da una persona che si trova in uno Stato membro dell'Unione, configuri l'utilizzo di «strumenti, automatizzati o non automatizzati», situati in tale Stato membro, a prescindere dal fatto che il *server* dell'*hosting provider* si trovi fisicamente in uno Stato membro o in uno Stato terzo. Di conseguenza, benché la Corte di giustizia escluda che la direttiva si applichi ad una trasmissione dei dati

si trovi fisicamente in uno Stato membro o in uno Stato terzo, la Corte esclude che in questo caso si verifichi un trasferimento, ai sensi della direttiva, il quale presupporrebbe una trasmissione diretta di dati da un mittente a un destinatario. In realtà, è evidente che l'*hosting provider*, che si limita a mettere a disposizione i mezzi tecnici per effettuare il trasferimento, è soltanto incaricato del trattamento, mentre responsabile del trattamento, anche rispetto alla trasmissione dei dati verso Paesi terzi, è e resta il *webmaster*, che assume la qualità di mittente del trasferimento, ai sensi della direttiva.

[19] Y. Poullet, *Transborder Data Flows* cit., p. 147.

[20] Così il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali (Article 29 Data Protection Working Party, d'ora in avanti: «Gruppo Art. 29» o «WP29»), *Opinion 6/2002 on Transmission of Passenger Manifest Information and Other Data from Airlines to the United States*, WP66/02 del 24 ottobre 2002, p. 7; Id., *Opinion 4/2003 on the Level of Protection Ensured in the US for the Transfer of Passengers' Data*, WP 78/03 del 13 giugno 2003, p. 7.

[21] Y. Poullet, *Transborder Data Flows* cit., p. 149.

attraverso un sito *web* accessibile *online,* tuttavia, qualora il responsabile del trattamento non possa impedire l'accesso al sito a tutti coloro che non sono destinatari dei dati, questo trasferimento rientrerebbe comunque nell'ambito di applicazione della direttiva, attraverso l'art. 4, par. 1, lett. *c*.

Ai sensi dell'art. 25, par. 1 della direttiva, il trasferimento dei dati personali può avvenire soltanto a condizione che il Paese terzo verso il quale i dati sono trasmessi garantisca «un livello di protezione adeguato». L''adeguatezza' del livello di protezione dei dati esistente nello Stato terzo è dunque il requisito indispensabile per il trasferimento dei dati al di fuori dell'Unione europea. La direttiva tuttavia non definisce in cosa consista l''adeguatezza', né precisa quali siano le condizioni che consentano in concreto di ritenerla verificata. Dall'art. 25, par. 2 si evince soltanto che deve essere valutata caso per caso, in via preventiva, e «con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati». Tra le circostanze da prendere in considerazione, lo stesso par. 2 dell'art. 25 indica, in via esemplificativa e non esaustiva, «la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate».

Il Gruppo Art. 29, che ha più volte autorevolmente interpretato questa disposizione[22], ha sottolineato, nel cosiddetto *Methodology Paper*[23], come l''adeguata protezione' debba essere distinta da criteri simili, come quello di protezione 'sufficiente' o 'equivalente'. In particolare, l''equivalenza' esige la completa similarità legislativa, verificata da un rigoroso confronto analitico: richiederebbe quindi la trasposizione pura e semplice nell'ordinamento dello Stato terzo dei diritti, degli obblighi e dei meccanismi di protezione previsti nel sistema giuridico dell'Unione. L''adeguatezza', invece, si limita di per sé a richiedere soltanto la verifica che nell'ordinamento dello Stato terzo venga svolta la funzione di protezione richiesta, anche se in base ad elementi di natura diversa rispetto a quelli disposti dal

[22] WP29, *Discussion Document. First Orientations on Transfers of Personal Data to Third Countries. Possible Ways Forward in Assessing Adequacy*, WP 4/97 del 26 giugno 1997; Id., *Working Document. Judging Industry Self-Regulation: When Does It Make a Meaningful Contribution to the Level of Data Protection in a Third Country?*, WP7/98 del 14 gennaio 1998; Id., *Working Document. Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries*, WP 9/98 del 22 aprile 1998.
[23] WP29, *Working Document: Transfers of Personal Data to Third Countries: Applying Art. 25 e Art. 26 of the EU Data Protection Directive*, WP12/98 del 24 luglio 1998.

legislatore dell'Unione[24].

La valutazione dell''adeguatezza' richiede quindi un approccio funzionale, che presuppone innanzitutto l'analisi preventiva dei rischi generati dallo specifico trasferimento, tenendo conto, in particolare, delle circostanze elencate dall'art. 25, par. 2 e, in generale, di tutte le circostanze nelle quali si svolge in concreto il trasferimento. Da questa analisi preventiva, si deve ricavare un criterio di verifica della conformità dell'ordinamento giuridico del Paese terzo ai principi essenziali di protezione dei diritti della persona, nonché un criterio di valutazione dell'effettività della tutela predisposta a tale scopo da questo Paese – fermo restando che questi appaiono come fini da raggiungere da parte dello Stato terzo, e non intaccano la sua libertà rispetto ai mezzi con cui raggiungerli. Il carattere adeguato del livello di protezione garantito da questo Paese deve essere infine determinato prendendo in considerazione tutte le misure, generali o particolari, di qualsiasi natura, legislativa, regolatoria o contrattuale, che appaiano disponibili in tale Paese per evitare gli specifici rischi che si sono evidenziati in relazione al quel concreto trasferimento[25].

A differenza di un astratto principio di equivalenza normativa, l'approccio funzionale all'adeguatezza dipende quindi dall'effettività della situazione esistente nell'ordinamento dello Stato terzo complessivamente considerato, ed esclude qualsiasi valutazione aprioristica: è stato detto che persino il fatto che uno Stato terzo abbia ratificato la convenzione di Strasburgo del Consiglio d'Europa sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale non è di per sé una garanzia che questo Stato assicuri un'adeguata protezione, ai sensi della direttiva[26].

La direttiva non specifica nemmeno quale soggetto possa o debba valutare l'adeguatezza del livello di protezione riscontrabile nello Stato terzo, lasciando quindi la sua identificazione alla discrezionalità degli Stati membri in sede di implementazione della direttiva stessa. Alcuni Stati

[24] Y. Poullet, *Pour une justification des articles 25 et 26 de la directive européenne 95/46/CE en matière de flux transfrontières et de protection des données*, in *Juris-Classeur, Chronique*, 2003, p. 9 ss. (ora anche in M. Cools *et al.* (éds*), Ceci n'est pas un juriste. Liber Amicorum B. de Schutter*, Bruxelles, 2003, p. 242 ss.), a p. 10.

[25] Y. Poullet, *Pour une justification* cit., p. 12.

[26] Y. Poullet, *Transborder Data Flows* cit., p. 146. Cfr. anche, su questo metodo, Y. Poullet, B. Havelange, A. Lefebvre, *Élaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel. Rapport final* (*Centre de recherches informatique et droit, Université de Namur*, Belgium - *EU Commission*, DG XV), 1997, documento sulla base del quale il WP29 ha elaborato il «*Methodology Paper*» cit. *supra* (nota 23).

membri hanno previsto, ad esempio, che l'adeguatezza venga valutata anzitutto, con varie modalità, dallo stesso responsabile del trattamento che opera il trasferimento dei dati, talvolta sotto il controllo *ex post* dell'autorità garante nazionale. In questa prospettiva, è quindi possibile che il livello di protezione dei dati garantito dallo Stato terzo venga giudicato in modo diverso a seconda del soggetto tenuto ad effettuare la valutazione dell'adeguatezza, e a seconda dell'autorità che deve controllare tale valutazione. Tuttavia, la direttiva stabilisce che la Commissione può constatare con decisione, in conformità alla procedura istituita dall'art. 31, par. 2, che uno Stato terzo garantisce o non garantisce un livello di protezione adeguato. In entrambi questi casi, gli Stati membri sono tenuti a conformarsi alla decisione della Commissione, per espressa previsione dell'art. 25, par. 6 e par. 4 della direttiva – che, sotto questo aspetto, si limita evidentemente a confermare quanto disposto dall'art. 288 TFUE in relazione al carattere obbligatorio e vincolante della decisione come atto di diritto derivato dell'ordinamento dell'Unione europea.

Se la Commissione accerta che un Paese terzo offre un livello adeguato di protezione, il trasferimento dei dati personali dagli Stati membri verso tale Paese è consentito senza necessità di ulteriori garanzie o autorizzazioni particolari. Dall'entrata in vigore della direttiva a oggi, la Commissione ha emanato complessivamente dodici decisioni di adeguatezza *ex* art. 25, par. 6, alcune delle quali tuttavia di scarso o nullo significato economico e politico[27].

Qualora, viceversa, la Commissione dovesse constatare che uno Stato terzo non garantisca un adeguato livello di protezione (ad oggi, tuttavia, non risulta che l'abbia mai fatto), ogni trasferimento di dati personali verso il Paese terzo sarebbe vietato, in conformità al considerando 57 della direttiva.[28] Questo non è tuttavia un divieto assoluto: l'art. 26 consente, infatti, a determinate condizioni, di trasferire dati personali anche verso un Paese terzo che non garantisca un livello adeguato di tutela ai sensi dell'art. 25, par. 2[29], nonché verso un Paese terzo nei confronti del quale

[27] I Paesi interessati sono Andorra, Argentina, Canada, Fær Øer, Guernsey, Israele, Isola di Man, Jersey, Nuova Zelanda, Svizzera, Uruguay e Stati Uniti (limitatamente a *«The US Department of Commerce's Safe Harbor Privacy Principles»*, come si vedrà: cfr. *infra*, par. 3): v. l'elenco in *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*.

[28] In questo caso, ai sensi del par. 5 dell'art. 25, «la Commissione avvia, al momento opportuno, negoziati per porre rimedio alla situazione risultante dalla constatazione di cui al par. 4».

[29] Cfr. WP29, *Working Document on the Protection of Individuals with Regard to the Processing of Personal Data* cit., p. 16 ss., 26 ss.

la Commissione non abbia preso espressamente alcuna decisione, né di adeguatezza, né di inadeguatezza.

Le deroghe consentite riprendono sostanzialmente le condizioni di legittimità del trattamento che sono oggetto dell'art. 7 della direttiva[30]: innanzitutto, i dati possono essere trasferiti qualora la persona interessata abbia espresso «in maniera inequivocabile» il proprio specifico consenso al trasferimento (art. 26, par. 1, lett. *a*); quando la trasmissione dei dati è necessaria per l'esecuzione di un contratto tra il responsabile del trattamento e la persona interessata, o per l'esecuzione di misure precontrattuali prese a richiesta della persona interessata (lett. *b*), oppure 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 (lett. *c*)[31].

Una seconda categoria di deroghe prende in considerazione specifiche categorie di flussi di dati: il trasferimento può essere disposto qualora sia necessario o imposto per la salvaguardia di un «interesse pubblico rilevante», o per l'esercizio di un diritto in giudizio (lett. *d*), o per la salvaguardia dell'interesse vitale della persona interessata, qualora l'interessato si trovi nell'incapacità fisica o giuridica di dare il proprio consenso (lett. *e*); oppure, ancora, qualora il trasferimento avvenga a partire da un registro pubblico, in presenza di determinate condizioni (lett. *f*).

Un'ulteriore deroga è prevista 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» (art. 26, par. 2). È questo il caso delle «norme vincolanti d'impresa» («binding corporate rules» o «BCR»): codici di condotta, regolamenti interni e altri atti del genere, per mezzo dei quali le società si obbligano ad osservare, nell'ambito dei trasferimenti infragruppo, i principi di legittimità del trattamento. Ricadono in questa previsione, inoltre, le «clausole contrattuali tipo» («standard contractual clauses»),

[30] Ad eccezione della lett. *f* dell'art. 7, che dispone: «[Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando :] *f*) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'art. 1, par. 1».

[31] Non è quindi sufficiente l'esistenza di un contratto, o il riferimento ad un generico interesse di natura contrattuale: occorre la prova della necessità del trasferimento per concludere o per eseguire uno specifico contratto, o per adottare provvedimenti utili alla formazione del contratto.

oggetto di diverse decisioni della Commissione (par. 4 dell'art. 26)[32]. Ciascuna di queste deroghe prevede la necessità di specifiche autorizzazioni per il trasferimento di dati, che a loro volta presuppongono l'assolvimento di specifici adempimenti, tanto in sede europea, quanto in sede nazionale, ove richiesto dalle singole disposizioni legislative di attuazione della direttiva.

Sia pure con l'aggravio dovuto alle autorizzazioni richieste, i dati personali raccolti nell'Unione europea possono quindi essere trasferiti, in via di eccezione, anche verso Paesi terzi esplicitamente ritenuti inadeguati dalla Commissione, oppure verso Paesi terzi che non siano stati ritenuti né adeguati né inadeguati dalla stessa. Ma in presenza di una decisione di adeguatezza della Commissione le deroghe sono, in linea di principio, inapplicabili.

2. La decisione della Commissione relativa al «Safe Harbor» e il contesto fattuale del caso Schrems.

La vicenda che ha dato origine alla sentenza in commento prende avvio nel 2013, quando Maximillian Schrems, un cittadino austriaco utente di *Facebook*, propone un ricorso in Irlanda all'autorità garante per la protezione dei dati personali contro *Facebook Ireland* Ltd. Questa società, filiale europea della statunitense *Facebook* Inc., è responsabile del trattamento dei dati personali degli utenti del *social network* residenti o domiciliati al di fuori degli Stati Uniti e del Canada. Pertanto, *Facebook* Inc. è anche il responsabile del trattamento dei dati degli utenti residenti o domiciliati negli Stati membri dell'Unione europea. Come indica la Corte di giustizia nella sentenza[33], risulta che i dati raccolti da *Facebook Ireland* nell'Unione europea vengano abitualmente trasmessi, in tutto o in parte, alla casa madre americana. *Facebook* Inc. riceve quindi, in provenienza dall'Unione europea, un flusso continuo di dati, che sono già stati oggetto di elaborazione nel territorio di uno Stato membro, e che sono destinati ad essere oggetto di ulteriore trattamento nel territorio americano. Terminata questa attività, i dati sono archiviati per la conservazione in strutture fisi-

[32] La Commissione ha finora adottato quattro decisioni contenenti clausole contrattuali tipo (l'ultima delle quali, tuttavia, abroga e sostituisce una delle precedenti): v. tutte in http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

[33] V. par. 27 della sentenza.

camente ubicate sempre nel territorio degli Stati Uniti.

Il ricorso di Schrems non pone in questione la legittimità del trasferimento oltreoceano dei dati personali da parte di *Facebook Ireland*. Questa trasmissione, infatti, avviene in conformità ad una decisione di adeguatezza della Commissione *ex* art. 25, par. 1 e 6 della direttiva: la decisione 2000/520/CE[34], che ha dichiarato adeguato il livello di protezione dei dati personali trattati in conformità al sistema in essa previsto. Questa decisione ha dato esecuzione nell'ordinamento europeo ad un accordo concluso dopo anni di negoziati tra l'Unione e il «Department of Commerce» degli Stati Uniti, autorità equivalente ad un organo ministeriale a livello federale.

Questo accordo, denominato «Safe Harbor», o 'Approdo sicuro', stabilisce i principi sostanziali in materia di legittimità e riservatezza del trattamento dei dati applicabili nel trasferimento dei dati personali dall'Unione europea agli Stati Uniti, nonché gli orientamenti applicativi e i principi procedurali necessari per la sua esecuzione da parte degli Stati contraenti. L'accordo prevede, in sostanza, che le imprese private e le altre organizzazioni stabilite sul territorio americano che intendono ricevere dati provenienti dall'Unione europea, possano aderire volontariamente all'accordo, in pratica sulla base di un'autocertificazione, vincolandosi ad osservarne i principi alla luce degli orientamenti applicativi stabiliti nell'accordo stesso e assoggettandosi «all'autorità prevista per legge di un ente governativo degli Stati Uniti», compreso tra quelli indicati dall'accordo stesso – sostanzialmente, la *Federal Trade Commission* e l'*US Department of Transportation*. L'autocertificazione è resa esecutiva attraverso la notifica alla *Federal Trade Commission* e l'impegno relativo all'osservanza del «Safe Harbor» è pubblicizzato nelle forme previste dall'accordo stesso.

Le autorità di entrambi gli Stati sono obbligate a vigilare per garantire l'applicazione dell'accordo; negli Stati Uniti la competenza per l'esecuzione dell'accordo è attribuita sempre alla *Federal Trade Commission* e all'*US Department of Transportation*, i quali possono ricevere denunce, imporre la cessazione di eventuali violazioni dell'accordo, nonché disporre il risarcimento «di qualunque soggetto, a prescindere dal paese di residenza o dalla nazionalità, danneggiato a seguito del mancato rispetto dei

[34] Decisione della Commissione del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «*Domande più frequenti* (*FAQ*)» in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, in *G.U.C.E.*, n. L 215 del 25 agosto 2000, p. 7 ss.

principi applicati in conformità [all'accordo stesso]»[35]. I cittadini europei che intendano reclamare a causa del trattamento dei dati effettuato da un'impresa aderente al «Safe Harbor» devono quindi rivolgersi a tali enti amministrativi; soltanto in alcuni casi possono agire anche davanti a istanze giurisdizionali. Tuttavia, nel caso di uno specifico comportamento illegittimo da parte di un'impresa o di un'organizzazione aderente al «Safe Harbor», le autorità nazionali di controllo degli Stati membri dell'Unione europea possono interrompere il flusso dei dati diretto verso tale impresa o organizzazione (art. 3, par. 1 della decisione).

L'adesione all'accordo può essere limitata, da parte delle organizzazioni che vi partecipano, qualora ricorrano determinate condizioni, e in particolare: «*a*) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia; *b*) [in presenza di] disposizioni legislative o regolamentari ovvero decisioni giurisdizionali, quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione»[36].

Non vi è necessità di sottolineare l'enorme importanza economica del «Safe Harbor»: nel corso del tempo, vi hanno aderito migliaia di imprese attive in tutti i settori economici, e in particolare i principali operatori del settore delle tecnologie dell'informazione e della comunicazione, *service providers*, motori di ricerca e *social media.* Tra questi, anche *Facebook* Inc., che quindi può legittimamente ricevere, trattare e conservare presso la sua sede negli Stati Uniti i dati personali di cittadini e residenti europei che siano stati trasferiti a partire da Stati membri dell'Unione. Il ricorso di Schrems non metteva in discussione la conformità del comportamento di *Facebook* Inc. al «Safe Harbor», sotto questo aspetto.

Quello che Schrems contestava nel suo ricorso, in realtà, era il giudizio reso dalla Commissione relativamente al livello di adeguatezza della protezione garantita dagli Stati Uniti nel quadro del «Safe Harbor». Il motivo erano le rivelazioni relative al cosiddetto scandalo «Datagate», effettuate da Edward Snowden, che aveva denunciato all'opinione pubblica l'attività di sorveglianza elettronica di massa perpetrata dai servizi di sicurezza americani, in particolare dalla *National Security Agency* («NSA»), nel quadro di un programma di intercettazioni denominato *PRISM*, attuato

[35] Art. 1, par. 2, lett. *b* della decisione della Commissione cit.
[36] All. I alla decisione della Commissione cit.

su larga scala e per lungo tempo negli Stati Uniti. Come si rileva dalle conclusioni della commissione d'inchiesta istituita dal Parlamento europeo e dalla risoluzione adottata dallo stesso Parlamento europeo alla chiusura dell'indagine[37], il programma *PRISM* aveva consentito alle autorità americane di *intelligence* di accedere in modo generalizzato e indiscriminato al contenuto di dati e metadati di traffico elettronico conservati nel territorio degli Stati Uniti, compresi i dati di cittadini europei, o di persone residenti nel territorio di Stati membri dell'Unione europea. Schrems rilevava nel suo ricorso che, poiché non era contestato che anche *Facebook* Inc. avesse collaborato a questo programma, i dati personali del suo *account* sul *social network*, una volta trasferiti in territorio americano, non erano e non sarebbero stati al riparo da gravissime forme di intercettazione, non consentite negli Stati membri dell'Unione europea. Doveva quindi ritenersi che gli Stati Uniti non fossero più in grado di garantire l''adeguata' protezione dei dati personali, contrariamente a quanto ritenuto dalla Commissione nella decisione relativa al «Safe Harbor».

La Commissione, in realtà, aveva riconosciuto, in alcune sue comunicazioni successive allo scoppio del «Datagate»[38], che l'applicazione del «Safe Harbor» da parte delle autorità americane era stata insufficiente sotto più punti di vista, e aveva quindi avviato trattative con le autorità americane per la rinegoziazione dell'accordo. Benché tali negoziati procedessero con lentezza, la Commissione si era astenuta dal sospendere la decisione di attuazione del «Safe Harbor», ritenendo che l'abrogazione *tout court* dell'accordo si sarebbe risolta in un danno per gli interessi degli operatori economici, tanto negli Stati Uniti, quanto nell'Unione. Malgrado la pendenza di tali negoziati, il «Safe Harbor» era quindi formalmente in vigore

[37] Cfr., rispettivamente, la relazione sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell'UE, e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni (2013/2188(INI)), condotta dalla Commissione per le libertà civili, la giustizia e gli affari interni (rel. Moraes), doc. A7-0139/2014 del 21 febbraio 2014; e la risoluzione del Parlamento europeo del 4 luglio 2013 sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sulla vita privata dei cittadini dell'Unione europea e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni (2013/2682(RSP)) – P7_TA(2013)0322, entrambe in http://www.europarl.europa.eu.

[38] Cfr. le due comunicazioni della Commissione al Parlamento europeo e al Consiglio, l'una intitolata «Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA», COM(2013) 846 def. del 27 novembre 2013, par. 3.2; e l'altra, relativa al funzionamento del regime 'Approdo sicuro' dal punto di vista dei cittadini dell'Unione europea e delle società ivi stabilite, COM(2013)847 def., sempre del 27 novembre 2013, spec. par. 7 e 8.

nell'ordinamento europeo nel momento in cui Schrems presentava il suo ricorso all'autorità irlandese di controllo dei dati.

L'*authority* rigettava tuttavia il ricorso, osservando, da un lato, che non vi era prova di uno specifico accesso da parte delle autorità americane ai dati personali del ricorrente, e rilevando, dall'altro lato, che la decisione della Commissione relativa al «Safe Harbor» era un atto obbligatorio e vincolante *ex* art. 288 TFUE, che richiedeva alle autorità nazionali di controllo degli Stati membri di conformarsi ad essa, finché fosse rimasta in vigore.

Schrems impugnava la decisione di rigetto davanti alla *High Court* irlandese. Quest'ultima osservava che, poiché non risultava che *Facebook* avesse trasgredito i suoi obblighi di osservanza del «Safe Harbor», l'autorità irlandese di controllo non avrebbe potuto interrompere il trasferimento dei dati verso gli Stati Uniti: infatti, come si è visto, l'art. 3, par. 1 della decisione della Commissione consente di sospendere l'accordo nei confronti di un soggetto che abbia aderito al «Safe Harbor» soltanto in presenza di uno specifico comportamento illegittimo.

Ciononostante, la *High Court* esprimeva forti dubbi sul fatto che il trasferimento dei dati verso gli Stati Uniti potesse ancora esser ritenuto compatibile con la direttiva. L'intercettazione dei dati da parte dell'autorità pubblica può infatti rispondere a legittimi obiettivi di interesse generale, quali la salvaguardia della sicurezza nazionale, della difesa, della pubblica sicurezza, o la prevenzione del terrorismo e di altri crimini. Queste eccezioni possono effettivamente giustificare una restrizione al diritto fondamentale alla tutela dei dati personali, come prevede anche l'art. 13, par. 1 della direttiva[39], ricalcando in buona parte i limiti consentiti dall'art. 8, par. 2 CEDU al diritto al rispetto della vita privata. Tuttavia, l'attività di sorveglianza praticata su larga scala dalle autorità americane sembrava aver ecceduto, secondo la Corte irlandese, la necessaria proporzionalità nel perseguimento di tali obiettivi, senza che oltretutto agli interessati fosse stata concessa un'adeguata garanzia di tutela giurisdizionale o amministrativa.

La *High Court* chiedeva quindi alla Corte di giustizia di pronunciarsi in via pregiudiziale sulla questione se, in presenza di una decisione della Commissione che dichiara 'adeguato' il livello di protezione dei dati personali garantito da uno Stato terzo, le autorità nazionali di controllo siano «assolutamente vincolate» a tale valutazione, o se possano discostarsene, ai fini dell'esame del ricorso di un cittadino europeo che asserisce che il livello di protezione in detto Stato terzo, nel quale sono stati trasferiti i suoi

[39] Cfr. in particolare le lett. *a, b, c* ed f dell'art. 13, par. 1.

dati, è inadeguato, alla luce di sviluppi fattuali e giuridici successivi alla decisione della Commissione[40]. Nell'ambito di tali sviluppi, la *High Court* includeva anche l'entrata in vigore della Carta dei diritti fondamentali dell'Unione europea, che tutela sia il diritto alla riservatezzaa e il diritto alla protezione dei dati personali (artt. 7 e 8), sia il diritto ad un ricorso effettivo e a un giudice imparziale (art. 47).

3. La sentenza della Corte di giustizia: la 'piena indipendenza' delle autorità nazionali di controllo e la dichiarazione di invalidità della decisione della Commissione relativa al «Safe Harbor». Gli effetti della sentenza

In conformità ad una giurisprudenza che può ritenersi ormai consolidata, come si è osservato, la Corte di giustizia risponde al rinvio pregiudiziale interpretando la direttiva alla luce degli artt. 7, 8 e 47 della Carta[41]. In base a questa interpretazione, i giudici dichiarano che una decisione di adeguatezza della Commissione *ex* art. 25, par. 6 della direttiva non può impedire alle autorità nazionali di controllo dei dati di esaminare, «con tutta la diligenza richiesta», la domanda proposta da una persona fisica a motivo della violazione dei suoi diritti relativi al trattamento dei dati personali, qualora i suoi dati siano stati trasferiti verso uno Stato terzo nel quale di fatto non venga garantito un appropriato livello di tutela. Inoltre, malgrado la questione non fosse oggetto di rinvio[42], la Corte dichiara invalida la decisione della Commissione relativa al «Safe Harbor». Su entrambi i punti della decisione, la sentenza aderisce alle conclusioni esposte dall'Avvocato generale, pur discostandosene occasionalmente nella motivazione.

La decisione sul primo punto, relativo all'obbligo delle autorità di controllo di ricevere i ricorsi individuali che contestano una decisione di adeguatezza della Commissione, è motivata dalla Corte in base alla 'piena indipendenza' delle autorità nazionali di controllo dei dati, indipendenza volta a consentire a tali autorità di esercitare effettivamente le funzioni

[40] V. par. 36 della sentenza.

[41] Sugli artt. 7, 8 e 47 della Carta v., rispettivamente, C. Campiglio, *Art. 7*, P. Piroddi, *Art. 8* e M. Castellaneta, *Art. 47*, tutti in F. Pocar, M.C. Baruffi (a cura di), *Commentario breve* cit., rispettivamente a p. 1678 ss., 1682 ss., 1770 ss.

[42] Per un precedente nel quale la Corte ha trasformato di fatto un rinvio pregiudiziale di interpretazione in rinvio pregiudiziale anche di validità, occorre risalire a Corte di giustizia, 1° dicembre 1965, *Schwarze*, causa 16/65, in *Racc.*, 1965, p. 910 ss.

loro attribuite dall'art. 28 della direttiva[43]. Afferma la Corte che lo *status* di indipendenza delle autorità di controllo nell'esercizio delle rispettive funzioni è una componente essenziale del regime europeo di protezione dei dati, non soltanto ai sensi dell'art. 28, par. 1 della direttiva, che prevede l'istituzione di tali autorità[44] ma, come la Corte ha costantemente ritenuto, anche ai termini dell'art. 8, par. 3 della Carta e dell'art. 16, par. 2 TFUE, che assoggettano il rispetto dei diritti delle persone interessate dal trattamento dei dati al controllo di 'autorità indipendenti'[45].

È evidente che le autorità nazionali di controllo non possono pronunciarsi in contrasto con una decisione della Commissione indirizzata agli Stati membri, atto obbligatorio in tutti i suoi elementi e vincolante per tutti gli organi degli Stati che ne sono i destinatari. Tuttavia, e questo è il punto chiave della pronuncia della Corte, una decisione della Commissione *ex* art. 25, par. 6 della direttiva non può eliminare o restringere i poteri espressamente accordati alle autorità nazionali di controllo dall'art. 8, par. 3 della Carta e dall'art. 28 della direttiva, che sono funzionali all'esercizio da parte di tali autorità della competenza relativa alla sorveglianza nell'applicazione delle disposizioni nazionali di attuazione della direttiva.

Elencati in modo indicativo e non esaustivo dall'art. 28, par. 3, tali poteri comprendono innanzitutto il diritto di accedere ai dati oggetto di trattamento e il diritto di raccogliere qualsiasi informazione necessaria all'esercizio della funzione di controllo; in secondo luogo essi comprendo-

[43] Sull'indipendenza delle autorità di controllo la giurisprudenza della Corte di giustizia è costante: v. sentenze 9 marzo 2010, *Commissione c. Germania*, C-518/07, in *Racc.*, 2010, p. I-1885 ss., par. 23; 16 ottobre 2012, *Commissione c. Austria*, C-614/10, ECLI:EU:C:2012:631, par. 36; 8 aprile 2014, *Commissione c. Ungheria*, C-288/12, ECLI:EU:C:2014:237, par. 47.

[44] Cfr. anche il considerando 62 della direttiva stessa, secondo il quale «la designazione di autorità di controllo che agiscano in modo indipendente in ciascuno Stato membro è un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali».

[45] Si noti, tuttavia, che né l'art. 8, par. 3 della Carta, né l'art. 16, par. 2 TFUE affermano che le 'autorità indipendenti' di controllo dei dati debbano essere anche autorità «nazionali». Stando a queste norme, potrebbe benissimo trattarsi di un organo indipendente istituito a livello europeo. In realtà, l'esistenza di autorità 'nazionali' di protezione dei dati non è altro che è il risultato del fatto che l'attuale sistema europeo di protezione dei dati è basato su una direttiva, che è uno strumento che deve essere implementato a livello nazionale dai singoli Stati membri. Pertanto, lo *status* di indipendenza delle autorità presenti a livello nazionale non è coperto dal diritto primario dell'Unione europea, ma soltanto dall'art. 28, par. 1 della direttiva: cfr. G. Thüsing, J. Traut, *The Reform of European Data Protection Law: Harmonisation at Last?*, in *Intereconomics*, 2013, p. 271 ss., a p. 273.

no poteri effettivi di decisione e di intervento, come quello di ordinare il congelamento, la cancellazione e la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento; da ultimo, il potere di promuovere azioni giudiziarie e di agire in giudizio in caso di violazione delle disposizioni nazionali di attuazione della direttiva. Osserva la Corte che l'art. 28, par. 3 non esclude dalla sfera di competenza delle autorità nazionali di controllo la vigilanza sui trasferimenti di dati verso Stati terzi che siano stati oggetto di una decisione di adeguatezza della Commissione[46]. Pertanto, in linea con le conclusioni dell'Avvocato generale[47], la Corte dichiara che il potere di verificare l'adeguatezza del livello di protezione esistente in uno Stato terzo deve ritenersi condiviso dalla Commissione con le autorità nazionali di controllo.

Si noti che la Corte di giustizia abbandona tutti i distinguo che aveva avanzato nella sentenza *Bodil Lindqvist* per circoscrivere i trasferimenti di dati ai quale è applicabile la direttiva da quelli sottratti alle sue garanzie. E si noti anche che il par. 2 dell'art. 25 non indica che la valutazione dell'adeguatezza del livello di protezione garantito da uno Stato terzo debba spettare alle autorità nazionali di controllo. In effetti, come si è visto, la direttiva non specifica a quale soggetto competa la valutazione dell'adeguatezza: l'individuazione di tale soggetto rientra nel margine di discrezionalità degli Stati membri, che possono attribuire tale potere anche al responsabile del trattamento, come è avvenuto in diversi casi.

Ciò non toglie che, se la Commissione ha constatato, a norma della direttiva, che un paese terzo garantisce un livello di protezione adeguato», l'art. 25, par. 6 stabilisce che «gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione». L'obbligo degli Stati membri di applicare la decisione di adeguatezza della Commissione non è altro che una specificazione dell'art. 288 TFUE, come aveva già osservato il *Data Protection Commissioner*. Del resto, anche il principio del primato del diritto dell'Unione europea, sviluppato nella stessa giurisprudenza della Corte di giustizia, induce a escludere che gli organi di uno Stato membro possano adottare atti non conformi a un obbligo contenuto in una valida decisione della Commissione[48].

Da questo punto di vista, lascia perplessi la conclusione della Corte di

[46] V. par. 54 della sentenza.
[47] V. par. 71 e 85 delle conclusioni.
[48] Sull'effetto preclusivo del principio del primato del diritto dell'Unione v., per tutti, A. Arena, *Il principio della* preemption *in diritto dell'Unione europea. Esercizio delle competenze e ricognizione delle antinomie tra diritto derivato e diritto nazionale*, Napoli, 2013, p. 9 ss..

giustizia, secondo la quale le autorità nazionali di controllo hanno l'obbligo di valutare la legittimità del trasferimento dei dati verso un determinato Stato terzo, in 'piena indipendenza' rispetto alla decisione di adeguatezza della Commissione[49]. Ci si può chiedere infatti quale carattere obbligatorio e vincolante residui per la decisione della Commissione, intesa come atto di diritto derivato, se le autorità degli Stati membri possono valutare la situazione esistente nello Stato terzo indipendentemente dal disposto della decisione stessa. Ci si può chiedere, inoltre, se la pronuncia della Corte valga anche per le decisioni di non adeguatezza, che la Commissione può emanare *ex* art. 25, par. 4, e se anche rispetto ad esse i garanti nazionali abbiano un autonomo potere di valutazione. Ci si può chiedere, ancora, se questo autonomo potere di valutazione possa essere esteso anche alle decisioni della Commissione che hanno approvato *binding corporate rules* o *standard contractual clauses*. Potrebbero essere giudicate inadeguate anche le garanzie che hanno giustificato le decisioni della Commissione riferite all'applicazione di queste deroghe nei trasferimenti verso gli Stati Uniti, considerato che, nella fattispecie, non può escludersi una possibile ingerenza delle autorità americane anche sui dati personali trasferiti in forza di tali strumenti?

Infine, ci si può chiedere se, oltre a «verificare, in piena indipendenza, se il trasferimento [dei dati personali] rispetti i requisiti fissati dalla direttiva»[50], le autorità nazionali di controllo possano anche sospendere o vietare, se del caso, i trasferimenti di tali dati verso il Paese terzo che ritengano inadeguato, malgrado l'esistenza di una decisione di adeguatezza della Commissione riferita a quello Stato terzo. L'Avvocato generale ha ritenuto che alle autorità nazionali di controllo spetta, in questo caso, «il potere di sospendere il trasferimento di dati in parola, e ciò a prescindere dalla valutazione generale effettuata dalla Commissione nella sua decisione»[51]. Sembra difficile, tuttavia, giungere a una simile conclusione senza attribuire sostanzialmente una portata extraterritoriale ai poteri delle autorità di controllo, poteri che, per espressa previsione della direttiva, hanno efficacia esclusivamente limitata al territorio dello Stato membro nel quale tali autorità sono state istituite (art. 28, par. 6). La territorialità dei poteri delle autorità nazionali di controllo è stata espressamente riaffermata dalla Corte di giustizia nella sentenza *Weltimmo*, emanata a ridosso della sentenza *Schrems*, che ha escluso che l'autorità di controllo di uno Stato mem-

[49] Par. 58 della sentenza; v. anche la pronuncia della Corte di giustizia, 8 aprile 2014, *Digital Rights Ireland* cit., par. 68.
[50] Par. 57 della sentenza.
[51] Par. 81 delle conclusioni.

bro possa esercitare i «poteri effettivi d'intervento» che le sono attribuiti dalla direttiva sul territorio di un altro Stato membro[52]. Ma se le autorità nazionali di controllo non possono sospendere o vietare i trasferimenti dei dati verso il Paese che ritengano inadeguato, quale effettività ha il potere di valutazione che tali autorità devono esercitare 'in piena indipendenza'?

Stando a quanto si limita ad affermare esplicitamente la Corte, le autorità nazionali di controllo, in presenza di una decisione di adeguatezza della Commissione, hanno l'obbligo di 'esaminare la domanda' di una persona relativamente alla tutela dei suoi diritti con riferimento al trattamento di dati personali che la riguardano. Sembra, quindi, che tali autorità siano tenute soltanto a ricevere i ricorsi individuali *ex* art. 28, par. 4 della direttiva, proposti a seguito di asserite violazioni del diritto alla protezione dei dati personali, verificatesi a seguito di un trasferimento internazionale dei dati. Qualora l'autorità nazionale di controllo respinga il reclamo, l'interessato potrà accedere al ricorso giurisdizionale che gli Stati membri sono obbligati a predisporre avverso le decisioni di rigetto di tale autorità, in conformità all'art. 28, par. 3 della direttiva. In quella sede, l'interessato potrà sollecitare l'autorità giudiziaria ad effettuare un rinvio pregiudiziale di validità alla Corte di giustizia avverso la decisione di adeguatezza della Commissione – rinvio pregiudiziale che, peraltro, rientra esclusivamente nella discrezionalità del giudice adito, e risulta obbligatorio soltanto per gli organi giurisdizionali di ultima istanza, *ex* art. 267 TFUE[53].

Qualora invece l'autorità nazionale di controllo consideri fondato il reclamo che le è stato proposto, e ritenga inadeguato il livello di protezione esistente nello Stato verso il quale sono stati trasferiti i dati, è incerto, sulla base della sentenza *Schrems*, se questa autorità, oltre ad 'esaminare la domanda', possa anche accogliere il ricorso ed emettere i conseguenti provvedimenti, provvisori o definitivi, relativi alla sua esecuzione. Infatti, la Corte si limita a dichiarare che, qualora ritenga fondato il reclamo, l'autorità nazionale di controllo dovrà adire l'autorità giudiziaria, *ex* art. 28, par. 3 della direttiva, sollecitando un rinvio pregiudiziale sulla validità della decisione della Commissione.

[52] In questo caso, l'autorità in questione dovrà limitarsi a chiedere l'intervento dell'autorità di controllo dello Stato membro sul territorio del quale dovrebbe aver luogo l'esecuzione: cfr. Corte di giustizia, 1° ottobre 2015, causa C 230/14, *Weltimmo* cit., par. 60.

[53] Giurisprudenza costante: cfr., ad es., Corte di giustizia, 7 dicembre 2010, *VEBIC VZW*, causa C-439/08, in *Racc.*, 2010, p. I-12471 ss., par. 41; Corte di giustizia, 2 aprile 2009, *Pedro IV Servicios*, causa C260/07, *ibid.*, p. I-2437 ss., par. 28; 14 dicembre 2006, *Confederación Española de Empresarios de Estaciones de Servicio*, causa C 217/05, *ibid.*, 2006, p. I-11987 ss., par. 16.

La Corte sembra implicitamente escludere che le autorità nazionali di controllo dei dati possano proporre autonomamente il rinvio pregiudiziale alla Corte di giustizia. Si potrebbe sostenere che tali autorità non presentino i requisiti di «*organi giurisdizionali* degli Stati membri» che, a norma dell'art. 267 TFUE, devono obbligatoriamente riscontrarsi nell'autorità remittente[54]. Tuttavia, l'accento posto dalla Corte di giustizia sulla 'completa indipendenza' di tali autorità, l'aver attribuito loro l'obbligo di tutelare diritti fondamentali della persona, il fatto che esse esercitino una funzione contenziosa in senso stretto, destinata a risolversi in una pronuncia di carattere giurisdizionale, pone seriamente la questione della legittimazione delle autorità nazionali di controllo dei dati a sollevare il rinvio pregiudiziale, anche in vista del fatto che il nuovo regolamento, come si vedrà, aumenterà i poteri e l'indipendenza delle *authorities*.

Nella sentenza *Schrems*, inoltre, la Corte di giustizia interpreta la nozione di 'adeguatezza'. In proposito, la Corte limita innanzitutto la discrezionalità della quale può disporre la Commissione nel valutare questo requisito, tenuto conto, da un lato, del carattere fondamentale del diritto alla protezione dei dati personali e, dall'altro, dell'elevato numero di persone i cui diritti sarebbero a rischio se i loro dati fossero trasferiti verso Paesi dal livello di protezione inadeguato[55]. In secondo luogo, malgrado la direttiva non imponga alla Commissione un obbligo di revisione periodica delle sue decisioni di adeguatezza,[56], la Corte afferma esplicitamente che la

[54] Per costante giurisprudenza, la Corte di giustizia accerta la qualità di «organo giurisdizionale di uno Stato membro», *ex* art. 267 TFUE, che costituisce una nozione autonoma di diritto dell'Unione, verificando l'esistenza, presso l'organo remittente, di una serie di elementi, quali l'origine legale dell'organo, il suo carattere permanente, l'obbligatorietà della sua giurisdizione, la natura contraddittoria del procedimento, il fatto che l'organo applichi norme giuridiche e che sia indipendente: cfr., ad es., Corte di giustizia, 17 settembre 1997, causa C-54/96, *Dorsch Consult*, in *Racc.*, 1997, p. I-4961 ss., par. 23; 30 novembre 2000, causa C-195/98, Österreichischer Gewerkschaftsbund, *ibid.*, p. I-10497 ss., par. 24; 30 maggio 2002, causa C-516/99, *Schmid*, *ibid.*, 2002, p. I-4573 ss., par. 34; 22 dicembre 2010, *Koller*, causa C-118/09, *ibid.*, 2010, p. I-13627 ss., par. 22 s.; 22 dicembre 2010; *RTL Belgium*, causa C-517/09, *ibid.*, p. I-14093 ss., par. 36 ss.; 14 giugno 2011, *Miles et al.*, causa C-196/09, *ibid.*, 2011, p. I-5105 ss., par. 37 ss. Inoltre, i giudici nazionali possono adire la Corte soltanto se dinanzi ad essi sia pendente un procedimento destinato a risolversi in una pronuncia di carattere giurisdizionale: v. Corte di giustizia, 19 ottobre 1995, *Job Centre*, causa C-111/94, in *Racc.*, 1995, p. I-3361, par. 9; 31 maggio 2005, C-53/03, *Syfait*, *ibid.*, 2005, p. I-4609 ss., par. 29.

[55] In questo senso v. anche la sentenza della Corte di giustizia dell'8 aprile 2014, *Digital Rights Ireland* cit., par. 48.

[56] E malgrado la decisione relativa al «*Safe Harbor*» impegnasse la Commissione ad un'unica valutazione della sua applicazione, tre anni dopo l'entrata in vigore: cfr. art. 4 della

Commissione è tenuta a verificare periodicamente che l'adeguato livello di protezione garantito dallo Stato terzo si mantenga giustificato nel tempo, da un punto di vista fattuale e legale[57]. La Corte accolla alla Commissione un vero e proprio obbligo: può quindi ritenersi che, qualora questa istituzione ometta di adempiervi, in presenza di circostanze sopravvenute che giustifichino dubbi sulla persistenza delle garanzie assicurate dallo Stato terzo, si possa prospettare la proposizione di un ricorso in carenza avverso la Commissione, *ex* art. 265 TFUE.

Per quanto riguarda il merito della definizione di 'adeguatezza', la Corte riconosce innanzitutto che 'adeguato' non significa 'identico', secondo quanto già evidenziato dal Gruppo Art. 29. È ammissibile, quindi, secondo la Corte, che il livello di protezione assicurato dal Paese terzo presenti delle differenze rispetto a quello garantito nel diritto dell'Unione europea. Lo Stato terzo, tuttavia, deve assicurare 'effettivamente' ai diritti della persona interessata una tutela 'sostanzialmente equivalente' a quella garantita nell'ordinamento dell'Unione dalla direttiva e dalla Carta dei diritti fondamentali[58]. Inutile sottolineare quanto questa richiesta da parte della Corte appaia intrinsecamente contraddittoria: una protezione 'effettiva' ed 'equivalente' a quella assicurata dall'Unione europea non è altro, infatti, che una protezione sostanzialmente identica a quella esistente nell'Unione europea. L'espressione adoperata dalla Corte ricorda da vicino l'endiadi dell'«effettività ed equivalenza di tutela», da tempo utilizzata dalla Corte di giustizia per limitare l'autonomia procedurale *degli Stati membri* nella predisposizione della tutela di diritti spettanti ai singoli in forza del diritto dell'Unione[59]. In questa sentenza, tuttavia, questi principi sono applicati dalla Corte *nei confronti di Stati terzi rispetto all'Unione*. Se la premessa della motivazione della Corte è analoga a quello del Gruppo Art. 29, le conclusioni non potrebbero essere più distanti.

In applicazione di questo rigoroso *test* di effettività ed equivalenza, la Corte prende dunque in esame la decisione della Commissione relativa al «Safe Harbor» e osserva, innanzitutto, che questo atto non certifica l'adeguatezza del livello di protezione dei dati relativo all'ordinamento degli Stati Uniti complessivamente considerato, ma soltanto quella del sistema istituito dall'accordo negoziato dalla Commissione. Il «Safe Harbor» infatti è applicabile soltanto alle imprese e alle organizzazioni che

decisione.

[57] Par. 76 della sentenza.

[58] Par. 73-74 della sentenza.

[59] Giurisprudenza consolidata: v. già Corte di giustizia, 16 dicembre 1976, *Rewe*, causa 33/76, in *Racc.*, 1976, p. 1989 ss.; 16 dicembre 1976, *Comet*, causa 45/76, *ibid.*, 2043 ss.

vi abbiano specificamente aderito, ma non vincola le autorità pubbliche e le istituzioni americane, che non risultano tenute ad osservarne i principi.

La Corte riscontra, in secondo luogo, che il «Safe Harbor» è carente relativamente all'effettività delle misure e delle procedure di vigilanza, peraltro particolarmente necessarie per un sistema del genere, sostanzialmente basato sull'autocertificazione di un impegno volontariamente assunto dai partecipanti.

In terzo luogo, questo accordo, come si è visto, non soltanto consente alle autorità statunitensi di derogare ai principi di legittimità del trattamento, e quindi di accedere ai dati per esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia[60], ma permette altresì agli aderenti di sottrarsi legittimamente alla sua applicazione, in presenza di atti legislativi, amministrativi o giurisprudenziali che li obblighino o li autorizzino a disapplicare l'accordo per finalità di tutela dell'interesse pubblico[61].

Infine, secondo la Corte, il «Safe Harbor» non predispone sufficienti presidi giuridici per limitare questa ingerenza, né prevede concreti controlli amministrativi o rimedi giurisdizionali per le persone interessate che siano cittadine europee o residenti negli Stati membri dell'Unione, qualora i loro dati personali siano stati oggetto, da parte delle autorità americane, di accessi illegittimi, determinando così una disparità di trattamento rispetto ai cittadini americani. La Corte ricorda anche che tutte queste insufficienze, già evidenziate a suo tempo dal Gruppo Art. 29[62], possono considerarsi dimostrate, poiché sono state esplicitamente ammesse dalla stessa Commissione, che ha riconosciuto che il «Safe Harbor» non ha di fatto salvaguardato i dati personali dei cittadini europei dagli accessi ingiustificati effettuati delle autorità degli Stati Uniti[63].

Tali restrizioni sono illegittime, secondo la Corte, non perché un diritto fondamentale, qual è quello alla protezione dei dati personali, non

[60] Cfr. all. I alla decisione cit., par. 4, lett. a).
[61] Cfr. all. I alla decisione cit., par. 4, lett. b).
[62] V., in proposito, WP29, *Opinion 7/99 On 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*, WP 27/99 del 3 dicembre 1999, spec. p. 11 ss.; Id., *Opinion 1/99 Concerning the Level of Data Protection in the United States And the Ongoing Discussions Between the European Commission and the United States Government*, WP15/99 del 26 gennaio 1999, p. 2-4.
[63] V. la comunicazione della Commissione «Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA» cit., par. 2 e 3.2; e la relazione della Commissione stessa sul «Funzionamento del regime *'Approdo sicuro'*» cit., par. 7 e 8.

possa ammettere limitazioni giustificate da esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia. Lo stesso art. 8, par. 2 CEDU, sulla base del quale deve essere interpretato il diritto alla protezione dei dati personali contenuto nell'art. 8 della Carta, ammette che possano esservi ingerenze dell'autorità pubblica nell'esercizio del diritto alla riservatezza, a condizione che ciascuna di esse sia prevista dalla legge e costituisca «una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui». Tuttavia, la Corte, richiamando la sua giurisprudenza nel caso *Digital Rights Ireland*[64], afferma che tali restrizioni devono essere contenute «entro i limiti dello stretto necessario». E i principi di necessità e di proporzionalità risultano violati quando l'autorità pubblica può effettuare accessi indiscriminati e generalizzati al contenuto dei dati, «senza alcuna differenziazione, limitazione o eccezione in funzione degli obiettivi perseguiti».[65] Una simile ingerenza viola il diritto fondamentale al rispetto della vita privata e alla riservatezza dei dati personali, nonché il diritto ad un effettivo rimedio giurisdizionale, *ex* art. 7, 8 e 47 della Carta. Su questa base, la Corte dichiara quindi invalido l'art. 1 della decisione della Commissione relativa al «Safe Harbor».

[64] Corte di giustizia, 8 aprile 2014, *Digital Rights Ireland* cit., par. 32-37 e 65 della sentenza. La sentenza aveva dichiarato invalida la direttiva 2006/24/CE riguardante la conservazione di dati nei servizi di comunicazione elettronica accessibili al pubblico e nelle reti pubbliche di comunicazione. La direttiva, in particolare, obbligava i fornitori di questi servizi a conservare per un certo periodo i metadati relativi al traffico, all'ubicazione e ad altre informazioni, che possono consentire l'identificazione dell'abbonato o dell'utente; inoltre, permetteva l'accesso delle autorità nazionali al contenuto dei dati, senza che vi fosse obbligo di informare la persona interessata; infine, non imponeva che i dati fossero conservati sul territorio degli Stati membri e pertanto non garantiva, secondo la prospettiva allora espressa dalla Corte, il pieno controllo da parte delle autorità indipendenti del rispetto delle esigenze di protezione e di sicurezza, che è stato esplicitamente richiesto dall'articolo 8, par. 3, della Carta quale elemento essenziale della protezione dei diritti delle persone relativi al trattamento dei dati personali. La Corte aveva concluso che tutte queste carenze costituivano un'ingerenza grave nel diritto fondamentale alla protezione dei dati di carattere personale, sancito dall'art. 7 e dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea. Trattandosi di ingerenza non proporzionata, né limitata allo stretto necessario, così seria da violare la sostanza stessa del diritto fondamentale alla tutela dei dati personali, la Corte aveva quindi annullato la direttiva. V. anche le conclusioni dell'Avv. gen. Cruz Villalón del 12 dicembre 2013, ECLI:EU:C:2013:845, in particolare par. 39-40, 77, 80.

[65] Par. 93 della sentenza.

La Corte dichiara invalido anche l'art. 3 di tale decisione. Come si è visto, questa norma consente alle autorità nazionali di controllo di sospendere i trasferimenti di dati diretti verso un'impresa o un'organizzazione aderente al «Safe Harbor», qualora siano stati violati i principi di legittimità del trattamento, applicati in conformità agli orientamenti applicativi contenuti nella decisione, o qualora «sia molto probabile che i principi vengano violati», senza che venga posto effettivo rimedio a questo inadempimento. Tuttavia, le condizioni richieste per l'applicazione dell'art. 3 sono così restrittive, da convincere la Corte che questa disposizione in realtà sottrae alle autorità nazionali di controllo una parte dei poteri di intervento che sono stati loro attribuiti dall'art. 28 della direttiva. Poiché tuttavia la Commissione non poteva restringere i poteri conferiti dalla direttiva alle autorità di controllo, la Corte dichiara l'invalidità anche dell'art. 3 della decisione. Infine, considerata l'inseparabilità dell'art. 1 e dell'art. 3 dal resto dell'atto, dichiara invalida tutta la decisione relativa al «Safe Harbor»[66].

Gli effetti dell'invalidità retroagiscono al momento nel quale la decisione della Commissione è entrata in vigore[67]. Infatti, la Corte sceglie di non avvalersi della facoltà di limitare nel tempo gli effetti della sentenza, esponendo consapevolmente gli operatori alle gravi ripercussioni economiche causate dall'invalidità retroattiva del «Safe Harbor». La retroattività della dichiarazione di invalidità appare come un'arma della quale la Corte si serve per costringere la Commissione ad accelerare la rinegoziazione del «Safe Harbor». Al momento della pronuncia della sentenza *Schrems*, infatti, la conclusione delle trattative con gli Stati Uniti appariva ancora lontana, benché i negoziati fossero stati avviati prima della proposizione del rinvio pregiudiziale alla Corte di giustizia. Alle pressioni da parte della Corte si sono aggiunte, all'indomani della sentenza *Schrems*, quelle del

[66] Si noti che la decisione relativa al «*Safe Harbor*» non avrebbe potuto essere oggetto di un autonomo ricorso dinanzi alla Corte di giustizia per annullamento ex art. 263 TFUE, considerato che il termine perentorio di proposizione del ricorso è di due mesi a decorrere dalla pubblicazione dell'atto nella Gazzetta Ufficiale dell'Unione europea, o dalla notificazione al destinatario, oppure, in mancanza di pubblicazione o di notifica, dal momento in cui il ricorrente è venuto a conoscenza dell'atto stesso: cfr. art. 263 TFUE, ult. comma.

[67] Talvolta, la Corte di giustizia, al fine di evitare che la retroattività di principio delle sentenze dichiarative dell'invalidità (risalente al momento in cui l'atto è entrato in vigore) possa pregiudicare diritti acquisiti in buona fede, ha attribuito alle proprie decisioni di annullamento, in via di eccezione e sulla base del principio generale del legittimo affidamento e della certezza del diritto, un effetto ex nunc. Sulla possibilità di limitare nel tempo gli effetti delle sentenze dichiarative dell'invalidità degli atti cfr. già Corte di giustizia, 8 aprile 1976, causa 43/75, *Defrenne II*, in *Racc.*, 1976, p. 455.

Gruppo Art. 29, che ha dichiarato che le autorità garanti nazionali non avrebbero escluso 'azioni coordinate', nel caso in cui la Commissione, entro la fine di gennaio 2016, non avesse trovato 'un'appropriata soluzione' con il governo degli Stati Uniti per rimediare al vuoto normativo creatosi con l'invalidità del «Safe Harbor»[68].

Prendendo atto dell'orientamento della Corte di giustizia e dell'avvertimento, neanche troppo velato, proveniente dal Gruppo Art. 29, la Commissione ha accelerato le trattative per sostituire il «Safe Harbor» – pur rammentando agli operatori che, nel frattempo, avrebbero potuto proseguire i trasferimenti oltreoceano dei dati utilizzando le deroghe previste dall'art. 26 della direttiva, sia pure con l'obbligo di richiedere le relative autorizzazioni caso per caso[69]. Tuttavia, come subito precisato dal Gruppo Art. 29, i trasferimenti in deroga non offrono alcuna protezione contro l'accesso ai dati da parte dell'autorità pubblica per ragioni di sicurezza nazionale[70].

4. La proposta relativa a una nuova decisione di adeguatezza della Commissione: il «Privacy Shield»

Il 29 febbraio 2016 la Commissione ha annunciato di aver finalmente raggiunto l'intesa con gli Stati Uniti sul nuovo quadro giuridico per lo scambio di dati destinato a sostituire il «Safe Harbor»[71] e ha presentato, con una sua comunicazione, la proposta relativa alla decisione di adeguatezza dell'«EU-US Privacy Shield» (o «Scudo per la riservatezza»). Così come nel caso del «Safe Harbor», anche in questo caso oggetto di valu-

[68] Cfr. «Statement of the Article 29 Working Party» del 16 ottobre 2015: «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.»

[69] Si veda la comunicazione della Commissione al Parlamento europeo e al Consiglio relativa al trasferimento di dati personali dall'UE agli Stati Uniti, in applicazione della direttiva 95/46/CE a seguito della sentenza della Corte di giustizia nella causa C-362/14, (*Schrems*), COM(2015)566 def. del 6 novembre 2015, p. 6 ss.

[70] Cfr. «*Statement of the Article 29 Working Party*» cit., e l'analogo «*Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment*» del 3 febbraio 2016.

[71] Cfr. comunicazione della Commissione al Parlamento europeo e al Consiglio *Trasferimenti transatlantici di dati – Ripristinare la fiducia attraverso solide garanzie* (COM(2016)117 def. del 29 febbraio 2016, spec. p. 8 ss.

tazione non è il complesso dell'ordinamento giuridico degli Stati Uniti, ma soltanto lo specifico sistema di protezione istituito appositamente dal governo americano per il trattamento dei dati trasferiti a partire dall'Unione europea. Questo comprende un elenco di principi che le organizzazioni aderenti saranno tenute a rispettare nell'ambito dell'accordo, l'istituzione di specifici organismi tenuti a vigilare sul rispetto di tali principi, e la predisposizione di una serie di mezzi di ricorso individuale per l'applicazione di sanzioni in caso di violazione dell'accordo. Tuttavia, con una significativa novità rispetto al «Safe Harbor», il governo degli Stati Uniti rilascerà impegni scritti e dichiarazioni ufficiali sull'applicazione dell'accordo che, a conferma della loro vincolatività, saranno pubblicati nell'*U.S. Federal Register*.

I pilastri del «Privacy Shield» sono rappresentati, innanzitutto, dall'imposizione alle organizzazioni aderenti di precisi obblighi giuridicamente vincolanti, e non più soltanto volontariamente assunti. Tali organizzazioni risulteranno responsabili anche qualora trasferiscano dati di cittadini dell'Unione a soggetti terzi, esterni all'accordo, che si trovino negli Stati Uniti o in Paesi terzi (c.d. 'trasferimenti successivi', ad esempio per attività di trattamento dei dati in subfornitura).

In secondo luogo, le autorità governative degli Stati Uniti rilasceranno specifiche garanzie in relazione alle condizioni per l'accesso ai dati effettuato ai fini di amministrazione della giustizia, di sicurezza nazionale e per altri scopi di interesse pubblico. Tali garanzie riguarderanno sia l'apposizione di precisi limiti all'accesso da parte delle autorità pubbliche di sicurezza (verrà impedito, tra l'altro, l'accesso indiscriminato ai dati), sia l'azionabilità dei diritti individuali sanciti dall'ordinamento americano sulla tutela della vita privata, in particolare attraverso l'estensione ai cittadini dell'Unione europea di alcuni diritti di ricorso giudiziario finora esercitabili soltanto dai cittadini statunitensi e dai residenti permanenti. All'interno dell'*US Department of State* verrà inoltre istituito un mediatore indipendente, che avrà l'incarico di trattare i ricorsi di cittadini dell'Unione relativamente all'accesso effettuato per motivi di sicurezza nazionale da parte dell'autorità pubblica. La competenza del mediatore dovrebbe estendersi, in linea di principio, a tutti i dati personali trasferiti negli Stati Uniti per fini commerciali, e non soltanto a quelli trasferiti nel quadro del «Privacy Shield».

Terzo, sarà garantita l'effettività della protezione dei diritti dei cittadini dell'Unione europea attraverso l'istituzione di organismi di vigilanza, con il potere di infliggere sanzioni, che potranno arrivare fino all'esclusione

dei soggetti inadempienti dall'applicazione del «Privacy Shield». Verranno inoltre istituiti mezzi di ricorso individuale, accessibili e di costo sostenibile, tra i quali, in particolare, alcuni organi di risoluzione alternativa delle controversie, e un comitato, che appare come una forma di arbitrato, la cui decisione in ultima istanza sarà vincolante ed esecutiva nei confronti degli operatori aderenti al sistema. Alle organizzazioni americane che trattano dati di cittadini europei relativi alle risorse umane sarà inoltre imposto il rispetto delle decisioni delle autorità garanti europee.

Infine, il «Privacy Shield» prevede un meccanismo annuale di riesame congiunto, che consentirà alla Commissione di monitorare il funzionamento dell'accordo, insieme con il *Department of Commerce* degli Stati Uniti, per verificare che le garanzie in materia di protezione dei diritti individuali fornite al momento del trasferimento dei dati restino equivalenti a quelle in forza nell'Unione europea. Qualora gli operatori economici o le autorità pubbliche americane non tengano fede agli impegni assunti, la Commissione potrà avviare la procedura per la sospensione dell'accordo. La Commissione sarà tenuta a presentare annualmente una relazione al Parlamento europeo e al Consiglio basata sui risultati di tale riesame congiunto.

L'*iter* previsto per l'approvazione della proposta relativa al «Privacy Shield» ha già subito tuttavia una battuta d'arresto, a seguito del parere non del tutto positivo del Gruppo Art. 29, che renderà necessarie sostanziali modifiche al contenuto della decisione.

Il Gruppo ha ravvisato infatti una mancanza di chiarezza e di trasparenza del testo, che lo rende di difficile consultazione, dispersivo, e talvolta incoerente. In particolare, alcune definizioni relative ai principi chiave della *privacy* non combaciano con quelle già adottate negli atti dell'Unione in materia, rischiando di rendere inutilmente complicata l'interpretazione e la futura applicazione di questo strumento.

Il Gruppo Art. 29 sottolinea inoltre che l'accordo, che è stato stilato in riferimento alla direttiva, dovrà esser armonizzato con il nuovo regolamento, e in generale con tutto il pacchetto di riforma dei dati personali che sta per essere emanato. Questo implica la necessità di una revisione a breve dell'accordo; in caso contrario, il Gruppo ritiene che il «Privacy Shield» potrebbe non rispondere al requisito di fornire una protezione 'essenzialmente equivalente', considerato che la riforma garantirà un livello di tutela dei diritti e delle libertà individuali più elevato rispetto alla direttiva. Ad esempio, il Gruppo Art. 29 osserva che il fondamentale diritto relativo alla cancellazione dei dati non è espressamente menzionato nel

testo dell'accordo, e non può essere inferito senza incertezze dal principio relativo all'integrità dei dati e alla limitazione dello scopo della raccolta, poiché quest'ultimo non obbliga i soggetti aderenti alla rimozione dei dati, nel caso in cui la conservazione non risulti più necessaria.

Inoltre, i limiti posti dal «Privacy Shield» all'azione delle autorità pubbliche statunitensi restano suscettibili di essere interpretati con eccessiva discrezionalità. In particolare, il Gruppo Art. 29 ritene che l'allegato VI al «Privacy Shield» non consenta di escludere del tutto che l'autorità governativa degli Stati Uniti possa continuare l'accesso indiscriminato su vasta scala ai dati personali trasferiti dall'Unione europea, in evidente contasto con la pronuncia della Corte di giustizia.

Un ulteriore aspetto riguarda il meccanismo di reclamo che dovrebbe far capo alla figura del mediatore. Benché debba senz'altro essere approvata l'istituzione di un'istanza di ricorso indipendente, in vista di un effettivo esercizio dei diritti individuali, il Gruppo Art. 29 osserva che la figura descritta nell'accordo non sembra esser dotata di poteri sufficienti per vigilare efficacemente e impedire eventuali abusi, anche in considerazione del rinnovato impulso politico alla sorveglianza di massa causato dal timore nei confronti del terrorismo. Inoltre, possono esprimersi legittimi dubbi sull'effettiva terzietà e indipendenza di tale autorità (incardinata all'interno dell'*US Department of State*, come si è visto). Gli altri rimedi previsti dall'accordo sembrano a loro volta troppo complessi per poter essere azionati dai singoli senza eccessive difficoltà, inducendo così a dubitare della loro effettività.

Ancora, poiché il «Privacy Shield» è suscettibile di essere utilizzato per trasferire i dati anche in Paesi terzi rispetto agli Stati Uniti, il Gruppo Art. 29 insiste affinché i trasferimenti esterni rispondano agli stessi requisiti di protezione dei dati personali stabiliti per i trattamenti effettuati nei Paesi oggetto dell'accordo, poiché, in caso contrario, questo genere di trasferimento extraterritoriale rischia di costituire un mezzo per aggirare i principi relativi alla protezione dei dati dell'Unione europea.

Infine, il meccanismo annuale di revisione congiunta, che a parere del Gruppo Art. 29 costituisce un fattore chiave per la credibilità complessiva del «Privacy Shield», soffre di scarsa chiarezza relativamente alle sue modalità di svolgimento, sotto l'aspetto della pubblicità da riservare alla relazione conclusiva dell'esame, delle possibili conseguenze in caso di risultato negativo, e della mancata indicazione dei mezzi di finanziamento. Il Gruppo Art. 29 ritiene inoltre che la revisione dell'accordo dovrebbe coinvolgere anche rappresentanti delle autorità garanti nazionali.

Considerata la gravità dei rilievi mossi dal Gruppo Art. 29, dei quali la Commissione non può non tenere conto, il testo della proposta appare quindi ancora lontano dall'essere definitivo.

Nel frattempo, però, è stato posto un altro tassello per la tutela dei dati dei cittadini europei nei confronti delle autorità americane. Infatti, l'8 settembre 2015, dopo quattro anni di trattative, iniziate quasi in parallelo all'avvio della riforma della direttiva, è stato firmato un accordo quadro tra l'Unione europea e gli Stati Uniti per la protezione dei dati personali in materia penale[72]. L'accordo, chiamato «the Umbrella Agreement» si propone di di assicurare un elevato grado di protezione dei dati personali – prevalentemente giudiziari e comunque pertinenti a tali finalità – scambiati tra magistratura, autorità giudiziarie e organismi di polizia, nel quadro della cooperazione transatlantica per la lotta al terrorismo e alla criminalità organizzata.

5. I trasferimenti dei dati verso Stati terzi, le decisioni di adeguatezza della Commissione e i poteri delle autorità nazionali di controllo nel nuovo regolamento generale sulla protezione dei dati personali

Lo scenario di riferimento, per quanto riguarda la protezione dei dati personali nell'Unione europea, è destinato a cambiare a breve. Infatti, il nuovo regolamento generale di protezione dei dati, che dovrà sostituire la direttiva, sta per concludere l'*iter* relativo alla sua approvazione definitiva. L'insistenza da parte della sentenza *Schrems* su determinati argomenti sembra spiegarsi proprio con la volontà della Corte di giustizia di incidere su alcuni aspetti del nuovo regolamento che possono ancora essere modificati.

Per quanto riguarda specificamente i trasferimenti dei dati verso Stati terzi, il nuovo regolamento, nel testo provvisorio attualmente disponibile,[73] ricalca nelle sue linee fondamentali la struttura prevista dalla direttiva:

[72] *Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses*, in http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf. La decisione di attuazione dell'accordo verrà adottata dal Consiglio dopo l'approvazione del Parlamento europeo.

[73] Il testo provvisoriamente disponibile consolida gli emendamenti apposti dal Parlamento europeo in prima lettura: cfr. risoluzione legislativa del Parlamento europeo del 12 marzo 2014 sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente

il principio generale è ancora quello dell'autorizzazione condizionata alla verifica della conformità del trasferimento ai principi di legittimità del trattamento (art. 40). Ancora una volta, il trasferimento non richiede una specifica autorizzazione, qualora la Commissione decida con un atto delegato – previa acquisizione del parere obbligatorio, ma non vincolante, del Comitato europeo per la protezione dei dati – che lo Stato terzo, o l'organizzazione internazionale ove il trasferimento è diretto, assicuri un adeguato livello di protezione (art. 41).[74] Tuttavia, a differenza della direttiva, il nuovo regolamento precisa nel dettaglio una lunga lista di elementi che la Commissione è tenuta a prendere in considerazione per verificare l'adeguatezza[75], restringendo quindi la sua discrezionalità nell'effettuare tale valutazione, così come richiesto dalla Corte di giustizia nella sentenza *Schrems*.

È anche possibile identificare una traccia dell'approccio funzionale proposto dal Gruppo Art. 29 nella sezione del regolamento che prevede che, per verificare l'adeguatezza del livello di protezione dei dati, il

la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), P7_TA(2014)0212.

[74] Art. 41, par. 1 e 3 del testo provvisorio del regolamento: «1. Il trasferimento è ammesso se la Commissione ha deciso che il paese terzo, o un territorio o settore di trattamento all'interno del paese terzo, o l'organizzazione internazionale in questione garantisce un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche. […] 3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'art. 86, al fine di decidere che un paese terzo, o un territorio o settore di trattamento all'interno del paese terzo, o un'organizzazione internazionale garantisce un livello di protezione adeguato ai sensi del par. 2. […]».

[75] Art. 41, par. 2, del testo provvisorio del regolamento: «2. Nel valutare l'adeguatezza del livello di protezione la Commissione prende in considerazione i seguenti elementi: *a)* lo stato di diritto, la pertinente legislazione generale e settoriale vigente, anche in materia penale, di pubblica sicurezza, difesa e sicurezza nazionale, come anche l'attuazione di tale legislazione, le regole professionali e le misure di sicurezza osservate nel paese terzo o dall' organizzazione internazionale in questione, la giurisprudenza precedente nonché i diritti effettivi e azionabili, compreso il diritto degli interessati a un ricorso effettivo in sede amministrativa e giudiziaria, in particolare quelli che risiedono nell' Unione e i cui dati personali sono oggetto di trasferimento; *b)* l' esistenza e l' effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o nell' organizzazione internazionale in questione, incaricate di garantire il rispetto delle norme di protezione dei dati, anche con sufficienti poteri sanzionatori, assistere e consigliare gli interessati in merito all' esercizio dei loro diritti e cooperare con le autorità di controllo dell' Unione e degli Stati membri, e *c)* gli impegni internazionali assunti dal paese terzo o dall' organizzazione internazionale in questione, in particolare ogni convenzione o strumento giuridicamente vincolante in relazione alla protezione dei dati personali».

responsabile del trattamento – o, se del caso, l'incaricato – avrà l'obbligo di effettuare un'analisi preventiva dei rischi generati dal trattamento sui diritti e sulle libertà della persona interessata, nonché una valutazione di impatto e una revisione di conformità delle procedure adoperate nel trattamento stesso, prendendo in esame tutte le circostanze concrete, con specifica attenzione all'effettività della situazione, ed evitando qualsiasi valutazione aprioristica (art. 32 *bis* ss.).

Il regolamento riflette le richieste della Corte di giustizia anche sotto l'aspetto dell'obbligo, esplicitamente accollato alla Commissione, di monitorare continuativamente gli sviluppi della situazione esistente nello Stato terzo (o nell'organizzazione internazionale) ove sono stati trasferiti i dati, allo scopo di individuare eventuali cambiamenti nelle circostanze che potrebbero giustificare modifiche alla decisione di adeguatezza[76]. In particolare, qualora nel Paese terzo non dovesse più riscontrarsi il livello di protezione inizialmente esistente nella tutela dei diritti delle persone residenti nell'Unione, la Commissione avrà l'obbligo di revocare la decisione di adeguatezza, e potrà anche adottare una decisione di non adeguatezza, attraverso atti delegati o di esecuzione[77].

In mancanza di una decisione di adeguatezza della Commissione, o qualora vi sia una decisione di non adeguatezza, il regolamento riconferma, in continuità con la direttiva, il divieto di trasferire dati personali verso lo Stato o l'organizzazione internazionale che siano stati ritenuti inadeguati (art. 42, par. 1).

Ancora una volta, tuttavia, il divieto cade, e il responsabile o l'incaricato del trattamento può trasferire dati verso uno Stato terzo (o verso un'organizzazione internazionale) senza dover essere specificamente autorizzato, a condizione che offra garanzie adeguate contenute in uno strumento giuridicamente vincolante che sia stato approvato dall'autorità

[76] Cfr. art. 41, par. 3, *in fine* e, rispettivamente, par. 4 *bis* del testo provvisorio del regolamento: «3. […] Tali atti delegati prevedono una clausola di estinzione se riguardano un settore di trattamento e sono revocati a norma del par. 5 qualora non sia più garantito un livello adeguato di protezione in conformità del presente regolamento. […] 4 *bis*. La Commissione controlla, su base continuativa, gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sugli elementi di cui al par. 2 [v. nota precedente] qualora sia stato adottato un atto delegato ai sensi del par 3 [v. *supra*, nota 74]».

[77] Art. 41, par. 5 del testo provvisorio del regolamento. La Commissione sarà obbligata inoltre a rivedere tutte le decisioni di adeguatezza adottate dalla Commissione sulla base della direttiva. Queste resteranno in forza soltanto per cinque anni dopo l'entrata in vigore del regolamento, se non modificate, sostituite o abrogate prima dalla Commissione: v. art. 41, par. 8 del testo provvisorio del regolamento.

nazionale di controllo[78]. Questi strumenti, elencati in via esemplificativa e non esaustiva dall'art. 42, par. 2 del regolamento, sono ancora costituiti dalle norme vincolanti d'impresa; le clausole *standard* di protezione dei dati, che siano state dichiarate di validità generale dalla Commissione[79]; le clausole contrattuali tra il responsabile o l'incaricato del trattamento e il destinatario dei dati; e infine, con una novità introdotta dal regolamento, il «sigillo europeo di protezione dei dati» (art. 39, par. 1, lett. *aa*). Questo costituisce una sorta di marchio di conformità, un contrassegno concesso dall'autorità nazionale di controllo a conclusione di una procedura amministrativa volta a certificare che il trasferimento dei dati è effettuato in conformità con le norme del regolamento, allo scopo di segnalare al pubblico l'adozione volontaria, da parte del responsabile o dell'incaricato del trattamento, di una serie di misure, procedure e controlli a garanzia della legittimità del trasferimento.

Non è stata invece ricompresa, tra gli strumenti giuridicamente vincolanti, una *best practice* che, con l'avallo del Gruppo Art. 29, inizia a svilupparsi a livello interno, costituita dalla certificazione indipendente effettuata da un ente di standardizzazione, che verifichi, da una prospettiva di terzietà, la conformità del trattamento agli obblighi e agli adempimenti posti a carico del responsabile del trattamento[80].

Anche il nuovo regolamento prevede, in via di eccezione, la possibilità di derogare al divieto di trasferire dati verso uno Stato terzo o un'organizzazione internazionale che non garantiscano un livello adguato di protezione (o che non siano stati oggetto di una decisione di adeguatezza della Commissione).

Le deroghe, previste dall'art. 44 del regolamento, sono sostanzialmente le stesse consentite dalla direttiva: il consenso informato e specifico della persona interessata; la necessità di concludere o eseguire un contratto tra la persona interessata e il responsabile del trattamento, oppure tra questi e

[78] Se del caso, in conformità al meccanismo di coerenza di cui all'art. 57 del regolamento: v. *infra* nel testo.

[79] Cfr. art. 62, par. 1, lett. *b* del testo provvisorio del regolamento. Le clausole contrattuali approvate dall'autorità di controllo sulla base dell'art. 26, par. 2 della direttiva resteranno valide per due anni dopo l'entrata in vigore del nuovo regolamento, se non modificate, sostituite o abrogate dall'autorità entro questo periodo di tempo: art. 42, par. 5 del testo provvisorio del regolamento.

[80] Cfr., ad es., la norma ISO 27018 per *public cloud*, pubblicata nel 2014 dall'ente di certificazione internazionale ISO quale standard specifico per garantire il rispetto della direttiva 95/46/CE da parte di *providers* che gestiscono infrastrutture informatiche distribuite seguendo il modello del *cloud* pubblico (benché l'adozione di contratti e accordi vincolanti non sia obbligatoria, ma lasciata alla discrezionalità del *service provider*).

un terzo, a condizione che il contratto sia a favore della persona interessata (escluso il caso delle attività svolte dalla pubblica autorità nell'esercizio dei suoi poteri); il pubblico interesse, in quanto ammesso dalla legge di uno Stato membro al quale il responsabile del trattamento è assoggettato, o dalla legislazione dell'Unione; la proposizione o l'esercizio di un'azione o di una difesa in giudizio; la necessità di salvaguardare interessi vitali della persona interessata o di un terzo, qualora la persona interessata sia fisicamente o giuridicamente incapace di prestare il consenso; la provenienza dei dati trasferiti da un registro pubblico aperto alla consultazione. Il Comitato europeo per la protezione dei dati – organismo istituito dal regolamento, composto da tutte le autorità nazionali di controllo insieme con il Garante europeo[81] – dovrà tuttavia emanare linee guida, raccomandazioni e migliori pratiche per consentire un'effettiva conformità dei trasferimenti in deroga.

Il nuovo regolamento, inoltre, rafforza considerevolmente la 'piena indipendenza' delle autorità nazionali di controllo dei dati che, come si è osservato, costituisce il perno attorno al quale ruota la motivazione della Corte di giustizia nella sentenza *Schrems*. L'art. 47, par. 1 stabilisce chiaramente che «l'autorità di controllo esercita le sue funzioni e i suoi poteri in piena indipendenza e imparzialità». Specifiche garanzie sono previste nel regolamento dal punto di vista delle prerogative che garantiscono lo *status* di indipendenza dell'*authority* rispetto allo Stato che l'ha istituita.

Resta tuttavia l'incertezza relativa alla possibile contraddittorietà delle decisioni che, nell'esercizio della loro 'piena indipendenza', le autorità nazionali di controllo possono emanare, e la questione dei termini nei quali esse devono ritenersi assoggettate alla Commissione. Basti pensare che quest'ultima, all'indomani della sentenza *Schrems*, preannunciava già l'invio di linee direttive a dette *autorithies*, per evitare applicazioni difformi in sede nazionale dei principi stabiliti dalla Corte[82].

La Corte di giustizia non sembra preoccuparsi troppo, nella sua pronuncia, della possibile contraddittorietà delle decisioni delle autorità nazionali di controllo. D'altra parte, la direttiva non si proponeva un'armonizzazione completa, ma soltanto un ravvicinamento delle legislazioni nazionali, e ammetteva quindi l'eventualità di differenze nella sua applicazione a livello nazionale. È chiaro invece che l'uniforme

[81] Cfr. artt. 64 ss. del testo provvisorio del regolamento.

[82] Cfr. il comunicato stampa della Commissione n. 15/5782 del 6 ottobre 2015: *First Vice-President Timmermans and Commissioner Jourová 's press conference on Safe Harbour following the Court ruling in case C-362/14 (Schrems)*, in, in http://europa.eu/rapid/press-release_STATEMENT-15-5782_it.htm.

applicazione del regolamento non potrà essere raggiunta mantenendo l'assoluta indipendenza delle autorità di controllo. Oltre al rischio di decisioni difformi, che contrastano con la finalità stessa del regolamento, si potrebbe incentivare il «forum shopping» da parte di responsabili del trattamento non europei che, a fronte di prassi amministrative differenti a livello nazionale, potrebbero scegliere di stabilirsi in un determinato Stato membro per assoggettarsi all'autorità di controllo più compiacente o più mite. Inoltre, l'indipendenza delle autorità nazionali di controllo nell'esercizio dei loro poteri non dovrebbe impedire il loro assoggettamento all'indirizzo della Commissione. L'indipendenza delle autorità nazionali deve quindi essere necessariamente controbilanciata, in applicazione del regolamento, da una stretta cooperazione reciproca tra tutte le autorità, e tra queste e la Commissione[83].

Per quanto riguarda il coordinamento reciproco delle autorità nazionali di controllo, il nuovo regolamento stabilisce il principio definito dello «sportello unico», che prevede che, quando ad un determinato trasferimento verso Stati terzi siano applicabili le leggi di più Stati membri, o quando siano coinvolti i dati personali di interessati residenti in più Stati membri, l'autorità nazionale di controllo dello Stato nel quale si trova lo stabilimento principale del responsabile o dell'incaricato del trattamento agisca come autorità capofila per la sorveglianza delle attività di trattamento effettuate dal responsabile o dall'incaricato del trattamento *in tutti gli Stati membri*. L'autorità capofila «è l'unica autorità autorizzata a decidere in merito a misure volte a sortire effetti giuridici per quanto riguarda le attività di trattamento del responsabile del trattamento o dell'incaricato del trattamento di cui è responsabile».[84] La *leading autorithy* potrà adottare provvedimenti produttivi di effetti giuridici soltanto dopo essersi consultata con le altre autorità, sforzandosi di raggiungere un consenso comune su tali misure. A questo scopo sono previsti obblighi di assistenza reciproca tra le autorità nazionali, consistenti essenzialmente in richieste di informazioni e in misure di controllo, quali richieste di autorizzazione o di consultazione preventiva, ispezioni e indagini.

Lo specifico strumento attraverso il quale il nuovo regolamento si propone invece di coordinare le autorità nazionali di controllo con la Commissione è il cosiddetto «meccanismo di coerenza». Introdotto dall'art. 57, è un sistema che deve essere instaurato innanzitutto quando un'autorità nazionale intenda determinare *standard protection clauses*,

[83] V. Art. 46, par. 1 del testo provvisorio del regolamento.
[84] Art. 54 *bis*., par. 2 del testo provvisorio del regolamento.

autorizzare clausole contrattuali o approvare *binding corporate rules*[85]. In secondo luogo, il meccanismo di coerenza può essere attivato a richiesta della Commissione, del Comitato europeo o di un'autorità nazionale di controllo nel caso in cui l'autorità di un altro Stato membro debba affrontare 'questioni di applicazione generale', relative all'uniforme applicazione del regolamento (art. 58, par. 3). È anche prevista, in via residuale, la possibilità di instaurare un meccanismo di coerenza qualora l'autorità nazionale di controllo che assume il ruolo di capofila debba adottare misure vincolanti in casi individuali (art. 58 *bis*). Questo meccanismo prevede che, prima dell'approvazione di quasiasi misura, l'autorità nazionale di controllo ne comunichi una bozza alla Commissione, al Comitato europeo per la protezione dei dati e alle altre autorità nazionali. Il Comitato dovrà o potrà, a seconda dei casi, esprimere un parere preventivo, che verrà reso pubblico e potrà diventare vincolante sull'autorità nazionale di controllo (par. 7 dell'art. 58 *bis*). È espressamente stabilito che, qualora un'autorità nazionale di controllo violi il meccanismo di coerenza, le misure da essa adottate a seguito della violazione non saranno valide né eseguibili negli Stati membri (art. 63, par. 2).

In continuità con la direttiva, il nuovo regolamento riconferma che, in linea di principio, ciascuna autorità nazionale di controllo esercita i poteri che le sono attribuiti «sul territorio del proprio Stato membro» (art. 51, par. 1). Tuttavia, con una novità di significativo rilievo rispetto alla direttiva, come interpretata dalla Corte nel caso *Weltimmo*[86], il regolamento prevede che una misura esecutiva legittimamente adottata da un'autorità di controllo possa essere attuata in qualsiasi Stato membro, quindi anche in uno Stato diverso da quello nel quale siede l'autorità di controllo che ha preso tale decisione (art. 63, par. 1). Non è del tutto chiara, tuttavia, l'eventuale interazione di questa previsione con le condizioni per il riconoscimento e l'esecuzione delle decisioni stabilite nel regolamento «Bruxelles I *bis*».[87]

[85] V. art. 58 lett. *d, e, f* e art. 42, par. 2, lett. *c* e *d* e art. 43 del testo provvisorio del regolamento.

[86] Corte di giustizia, 1° ottobre 2015, *Weltimmo* cit., par. 60.

[87] L'art. 1, par. 1 del regolamento stabilisce che esso «si applica in materia civile e commerciale, indipendentemente dalla natura dell'autorità giurisdizionale», ma «non si estende, in particolare, alla materia […] amministrativa»: v. regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio del 12 dicembre 2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (c.d. «Bruxelles I *bis*», in *G.U.U.E.* n. *L* 351 del 20 dicembre 2012, p. 1 ss.), modificato dal regolamento (UE) n. 542/2014 del Parlamento europeo e del Consiglio, del 15 maggio 2014, per quanto riguarda le norme da applicare con riferimen-

Resta ovviamente esclusa qualsiasi efficacia extraterritoriale dei poteri delle autorità nazionali di controllo rispetto a Stati terzi. In questa prospettiva, il regolamento prevede che, fatti salvi eventuali trattati internazionali di reciproca assistenza giudiziaria che vincolano l'Unione o un singolo Stato membro, non potranno essere riconosciute o dichiarate esecutive nell'Unione decisioni giurisdizionali o misure amministrative di Stati terzi, che ingiungano a un responsabile o a un incaricato del trattamento stabilito nell'Unione di divulgare il contenuto di dati personali trattati nel territorio di uno Stato membro (art. 43 *bis*) – che esigano, in definitiva, di trasferire tali dati nello Stato terzo che ha preso il provvedimento. Qualora il responsabile o l'incaricato del trattamento stabilito nell'Unione riceva un'intimazione del genere dovrà notificarla all'autorità di controllo e attendere la sua autorizzazione preventiva. Questa verrà concessa soltanto se il trasferimento può avvenire in conformità al regolamento, e se è necessario e obbligatorio per la proposizione, l'esercizio o la contestazione di azioni in giudizio (art. 44, par. 1, lett. *d* e lett. *e*) o «per importanti ragioni di interesse pubblico» , non meglio specificate. Resta fermo che l''interesse pubblico' deve essere riconosciuto dal diritto dell'Unione o dello Stato membro al quale è assoggettato il responsabile del trattamento (art. 44, par. 5).

Se sono coinvolte persone interessate che si trovano in altri Stati membri, l'autorità di controllo applicherà il meccanismo di coerenza, e in ogni caso la persona interessata dovrà essere informata dell'autorizzazione concessa dall'autorità di controllo[88]. È evidente la volontà del legislatore di evitare che i trasferimenti internazionali consentano alle autorità pubbliche di Stati terzi l'accesso ai dati senza le adeguate garanzie, esigenza ribadita dal Gruppo Art. 29, che ha già proposto un'interpretazione restrittiva di questa parte del regolamento[89].

Parallelamente, il nuovo regolamento promuove la cooperazione con Stati terzi e organizzazioni internazionali, specialmente se la Commissione

to al Tribunale unificato dei brevetti e alla Corte di giustizia del Benelux (in G.U.U.E. n. L 163 del 29 maggio 2014, p. 1 ss.).

[88] In questo senso cfr. anche la sentenza della Corte del 1° ottobre 2015, causa C 201/14, *Smaranda Bara* cit., par. 28 ss., nella quale la Corte ha stabilito che uno Stato membro non può legittimamente consentire , senza prevedere appropriate garanzie, misure che consentono a un'amministrazione pubblica di questo Stato di trasmettere dati personali a un'altra amministrazione pubblica dello stesso Stato, a fini di trattamento, senza che le persone interessate siano state informate di tale trasmissione o del successivo trattamento, in conformità ai principi stabiliti dagli artt. 10, 11 e 13 della direttiva.

[89] WP 29, *Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing*, WP 232/15 del 22 settembre 2015, p. 7 s.

ritenga che essi assicurino un adeguato livello di protezione dei dati *ex* art. 41, par. 3. Tanto la Commissione, quanto le autorità di controllo dovranno sviluppare effettivi meccanismi di cooperazione internazionale per assicurare l'applicazione dei diritti e delle libertà fondamentali relativamente alla protezione dei dati personali, e offrire reciproca assistenza internazionale nell'applicazione delle relative disposizioni, comprese quelle riguardanti le notifiche, il deposito dei ricorsi, l'assistenza per l'attività istruttoria e lo scambio di informazioni (art. 45, par. 1, lett. *a* e *b*). Questo costituisce uno sviluppo innovativo, specialmente per quanto riguarda il coinvolgimento diretto nelle relazioni internazionali di organismi interni, quali sono le autorità nazionali di controllo[90].

Infine, un emendamento apposto dal Parlamento europeo al considerando 90 della proposta di regolamento vorrebbe che, qualora uno Stato terzo richieda ai responsabili del trattamento requisiti di conformità contrastanti rispetto a quelli stabiliti dal regolamento, la Commissione abbia l'obbligo di garantire che, nel conflitto di giurisdizione con lo Stato terzo interessato, il diritto dell'Unione prevalga 'in ogni circostanza'[91]. Un obbligo difficile da adempiere, tuttavia, poiché la necessaria applicazione delle norme del regolamento non può che dipendere dal tenore del diritto

[90] Inoltre, la Commissione e gli Stati membri dovranno coinvolgere le parti interessate nel dibattito e nelle attività relative alla promozione della cooperazione internazionale, promuovere lo scambio e la documentazione relativa tanto alla legislazione quanto alla prassi, fornirsi informazioni e consultarsi su conflitti di giurisdizione con Stati terzi (lett. *c, d* e *da* del par. 1 dell'art. 45 del testo provvisorio del regolamento).

[91] Cfr. risoluzione legislativa del Parlamento europeo del 12 marzo 2014 cit., emendamento n. 63 al considerando 90 del regolamento (in corsivo nel testo): «90. Alcuni paesi terzi adottano leggi, regolamenti e altri strumenti legislativi finalizzati a disciplinare direttamente le attività di trattamento dati di persone fisiche e giuridiche poste sotto la giurisdizione degli Stati membri. L'applicazione extraterritoriale di tali leggi, regolamenti e altri strumenti legislativi potrebbe essere contraria al diritto internazionale e ostacolare il conseguimento della tutela delle persone garantita nell'Unione con il presente regolamento. I trasferimenti dovrebbero quindi essere consentiti solo se ricorrono le condizioni previste dal presente regolamento per i trasferimenti a paesi terzi. Ciò vale tra l'altro quando la divulgazione è necessaria per un motivo di interesse pubblico rilevante riconosciuto dal diritto dell'Unione o dello Stato membro cui è soggetto il responsabile del trattamento. Occorre che la Commissione precisi le condizioni in cui sussiste un motivo di interesse pubblico rilevante con un atto delegato. *Laddove i responsabili del trattamento o gli incaricati del trattamento si trovino di fronte a requisiti di conformità contrastanti tra la giurisdizione dell'Unione, da una parte, e quella di un paese terzo, dall'altra, la Commissione deve garantire che il diritto dell'Unione prevalga in ogni circostanza. La Commissione ha il compito di fornire consulenza e assistenza al responsabile del trattamento e all'incaricato del trattamento nonché di cercare di risolvere il conflitto di giurisdizione con il paese terzo interessato*.»

internazionale privato dello Stato che esercita la giurisdizione nella relativa controversia. Se, nella fattispecie, fosse giurisdizionalmente competente lo Stato terzo, è evidente che difficilmente la Commissione potrebbe influire sull'obbligo dell'autorità amministrativa o dell'organo giudicante dello Stato terzo di determinare la legge applicabile al trattamento sulla base delle regole di applicabilità, o del diritto internazionale privato, in forza nello Stato terzo nel quale tale autorità o tale giudice siede.

Conclusioni

La sentenza *Schrems* riflette con chiarezza le preoccupazioni della Corte di giustizia a causa dell'inefficacia di fatto del sistema predisposto dall'Unione per la protezione dei dati personali trasferiti verso Stati terzi.

L'aspetto sconcertante di questa vicenda è che non vi sono stati inadempimenti formali rispetto agli obblighi di legge incombenti sul *service provider,* eppure gravissime violazioni del diritto fondamentale alla protezione dei dati personali hanno potuto verificarsi, senza che questo incidesse sulla continuità del flusso dei dati verso gli Stati Uniti. L'inefficacia del sistema di tutela è tanto più grave, in quanto non riguarda soltanto la decisione relativa al «Safe Harbor» o la direttiva 95/46/CE, ma lo stesso diritto primario relativo alla protezione dei dati personali, cioè il Trattato sul funzionamento dell'Unione europea e la Carta dei diritti fondamentali dell'Unione europea.

E se la principale responsabilità per tale situazione dev'essere addebitata alla decisione relativa al «Safe Harbor», che ha meritato di essere dichiarata invalida, tuttavia anche le altre decisioni di adeguatezza emanate dalla Commissione risultano discutibili, per motivi diversi. Infatti, anche a voler prescindere dal merito della valutazione relativa all'adeguatezza sostanziale della protezione garantita dai vari Stati, queste decisioni si sono rivelate di scarsissimo rilievo pratico, ai fini della promozione della libertà di circolazione internazionale dei dati, che pure dovrebbe rappresentare un obiettivo prioritario per la Commissione, come evidenziano tanto il piano d'azione per l'attuazione dell'«Agenda digitale europea», quanto la strategia «Europa 2020»[92]. Pertanto, tutto il sistema relativo

[92] Cfr. Commissione, doc. COM(2012)11 def. - 2012/0011(COD) cit., p. 2, par. 1, in riferimento alla Comunicazione della Commissione *Un'agenda digitale europea*, COM(2010) 245 def. del 19 maggio 2010; Comunicazione della Commissione *EUROPA 2020. Una strategia per una crescita intelligente, sostenibile e inclusiva*, COM(2010)2020 def. del 3 marzo 2010.

al trasferimento dei dati personali dall'Unione europea verso Stati terzi sembra aver fallito l'una o l'altra delle proprie finalità, e cioè la tutela delle persone quanto al trattamento dei dati personali e il rafforzamento della libertà di circolazione dei dati come strumento per la promozione della competitività delle imprese europee nel mercato interno e nel commercio internazionale.

A fronte delle falle del sistema, tuttavia, il nuovo regolamento non introduce apparentemente modifiche sostanziali alla disciplina del trasferimento dei dati verso Stati terzi. Il principio generale resta sempre quello dell'autorizzazione condizionata, con la dichiarazione di adeguatezza della Commissione relativa al livello di protezione garantito dallo Stato terzo, oppure con la decisione di non adeguatezza; sono ancora consentiti gli strumenti giuridici vincolanti per trasferire i dati verso Stati terzi che non assicurino un adeguato livello di protezione; ed è ancora prevista la possibilità di trasferimenti in deroga.

Andando oltre le apparenze, tuttavia, la prospettiva è rovesciata: se la direttiva istituiva un rapporto da regola a eccezione tra i trasferimenti effettuati sulla base della decisione di adeguatezza della Commissione, e quelli effettuati sulla base di strumenti giuridici vincolanti, il nuovo regolamento stabilisce, tra questi e i trasferimenti basati sulle decisioni di adeguatezza, una relazione che si avvia a diventare paritaria. Il punto di vista del legislatore è chiaro: la garanzia della protezione dei dati nei trasferimenti internazionali non può più essere assicurata esclusivamente da un processo di conformità con il sistema normativo, isolatamente considerato, come ha evidenziato peraltro anche il caso *Schrems*. Gli obblighi legislativi devono trovare necessariamente corrispondenza negli obblighi vincolanti di autoregolamentazione imposti al responsabile del trattamento: in altri termini, la protezione dei dati personali nei trasferimenti internazionali deve essere il risultato di una cooperazione tra l'azione del legislatore, che resta ancora il principale soggetto sul quale grava la responsabilità di garantire la legittimità del trasferimento, e l'azione del responsabile del trattamento, in assolvimento di obblighi di *self-regulation* posti direttamente in capo ad esso, sotto la vigilanza delle autorità di controllo.

In questa prospettiva, quasi in risposta alle richieste della Corte di giustizia, il regolamento rafforza considerevolmente l'indipendenza delle autorità nazionali di controllo. Tuttavia, per quanto piena e completa possa essere l'indipendenza delle *authorities*, questa non le esime dalla necessità di coordinarsi reciprocamente, né dall'obbligo di assoggettarsi all'autorità della Commissione, al fine di non vanificare l'applicazione uniforme del

regolamento a livello nazionale. L'esigenza di conciliare questi aspetti potenzialmente conflittuali è ben conosciuta dal legislatore dell'Unione che, in altri casi – ad esempio, nell'applicazione del diritto della concorrenza[93] – ha risolto il problema attraverso la creazione di una rete europea di cooperazione tra la Commissione e le autorità garanti degli Stati membri. Il regolamento, pur senza istituire una formale rete di cooperazione, interviene con modalità analoghe a quelle previste per l'*enforcement* della concorrenza: da un lato estende anche alla materia del trasferimento dei dati il principio del cosiddetto 'sportello unico', con un'autorità capofila, qualora più autorità nazionali di controllo rivendichino una competenza nello stesso caso; dall'altro, istituisce un 'meccanismo di coerenza', nel quale sono coinvolte tanto le autorità nazionali e il Comitato europeo per la protezione dei dati, quanto la Commissione – la cui funzione di guida peraltro non appare ancora del tutto chiara[94].

Ma la questione forse più critica riguarda l'eventuale esecutività dei provvedimenti delle autorità nazionali di controllo nel territorio di Stati diversi da quello nel quale siedono le autorità che li hanno emanati. In applicazione della direttiva, questo effetto è stato esplicitamente respinto dalla Corte di giustizia nella sentenza *Weltimmo*, che ha preceduto di pochi giorni la sentenza *Schrems*. Il testo provvisorio del regolamento, invece, stabilisce espressamente che le decisioni esecutive delle autorità nazionali di controllo possano avere efficacia in tutti gli Stati membri dell'Unione europea. Resta esclusa, ovviamente, la portata extraterritoriale di tali provvedimenti al di fuori dell'Unione. Allo stato attuale del diritto internazionale[95], non sembra possibile ottenere questo risultato se non attraverso la conclusione di specifici accordi con gli Stati interessati. Tuttavia, con un'omissione che è stata già evidenziata dal Garante europeo per la protezione dei dati, il regolamento non impone la revisione degli accordi internazionali conclusi dall'Unione nella materia del trasferimento dei dati, allo scopo di allinearli al regolamento[96].

[93] Cfr. la Comunicazione della Commissione sulla cooperazione nell'ambito della rete delle autorità garanti della concorrenza, in *G.U.U.E.*, C 101 del 27 aprile 2004, p. 43 ss.

[94] Peraltro, il ruolo di guida attribuito alla Commissione non è del tutto chiaro, poiché sembra che la Commissione si limiti, nella fase iniziale, ad attivare il ricorso al Comitato (art. 58, par. 4) e, in una fase successiva, abbia soltanto il potere di adottare pareri.

[95] Anche l'Assemblea delle Nazioni Unite ha recentemente sottolineato che il diritto umano alla privacy deve godere anche nello spazio digitale dell'identica tutela che gli è offerta nel mondo reale: cfr. risoluzione dell'Assemblea ONU 68/17 del 18 dicembre 2013, intitolata «*The Right to Privacy in the Digital Age*» (A/RES/68/167 -A/68/456/Add.2), in http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167).

[96] Cfr. Garante europeo della protezione dei dati, Parere del 7 marzo 2012 sul

Tra gli accordi conclusi dall'Unione, vi è, in particolare, quello firmato con gli Stati Uniti nel 2012, recante *Trade Principles for Information and Communication Technology Service*[97]. Questo accordo, avente valore dichiarativo e non vincolante, trova applicazione nel settore delle reti e dei servizi per le tecnologie dell'informazione e della comunicazione, sia nell'ambito delle relazioni commerciali bilaterali tra Unione europea e Stati Uniti, sia nel quadro dei negoziati internazionali eventualmente aperti da questi con Stati terzi, senza pregiudizio degli obblighi internazionali sanciti dal WTO e dal GATS. Ispirati ai *Principles on Internet Policymaking* dell'OCSE[98], gli orientamenti stabiliti da questo accordo impegnano gli Stati contraenti, in particolare, a non ostacolare i trasferimenti internazionali di dati effettuati da *service providers* stabiliti in altri Paesi o dai loro clienti, e a non bloccare l'accesso, da parte degli stessi *service providers* o dei loro clienti, alle informazioni pubblicamente disponibili, o alle informazioni di loro proprietà conservate in altri Paesi.

Questo accordo è tuttavia destinato ad essere superato dal discusso accordo di libero scambio tra Unione europea e Stati Uniti, attualmente è in corso di negoziazione («Transatlantic Trade and Investment Partnership» o «TTIP»)[99]. Le perplessità suscitate presso una larga parte dell'opinione pubblica dalle trattative relative a questo accordo dipendono dal fatto che il testo sembra consentire, nelle materie che ne sono oggetto, un'applicazione significativamente attenuata delle disposizioni dell'Unione relative alla protezione dei dati personali.

Si noti, in proposito, che il GATS non vieta, in linea di principio, di apporre barriere allo scambio internazionale di servizi giustificate dalla

pacchetto di riforma della protezione dei dati (2012/C 192/05), in G.U.U.E., C 192 del 30 giugno 2012, p. 7 ss., a proposito del considerando 79 del regolamento.

[97] *European Union-United States Trade Principles for Information and Communication Technology Service*, accordo concluso in data 4 aprile 2012, in http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc_147780.pdf : «*3. Cross-Border Information Flows: Governments should not prevent service suppliers of other countries, or customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in other countries.*»

[98] OECD (*Organization for Economic Cooperation and Development* – Organizzazione per la Cooperazione e lo sviluppo economico), *Recommendation of the OECD Council on Principles for Internet Policy Making*, C(2011)154 del 13 dicembre 2011, in http://www.oecd.org/internet/ieconomy/49258588.pdf (pubblicati nel 2014 in versione finale: OECD *Principles on Internet Policy Making*, in http://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf). In dottrina, cfr. R.H. Weber, *Principles for Governing the Internet: A Comparative Analysis*, 6th ed., Paris, 2015.

[99] V. la pagina dedicata alle trattative in corso sul sito della Commissione: http://ec.europa.eu/trade/policy/in-focus/ttip/.

protezione dei dati personali[100]. Da questo punto di vista, l'Unione europea non infrangerebbe quindi alcun obbligo internazionale, se assicurasse, anche nei rapporti commerciali con Stati terzi, il diritto fondamentale delle persone alla protezione dei propri dati.

Tuttavia, al di là dell'aspetto formale, è evidente che un livello di tutela così elevato come quello richiesto dalla Corte di giustizia nella sentenza *Schrems* comporta un rischio di frammentazione del mercato globale dell'informazione, che può effettivamente tradursi in un concreto ostacolo alla competitività internazionale delle imprese stabilite nell'Unione europea.

Il punto di equilibrio tra queste opposte esigenze non dovrebbe tuttavia essere ricercato abbassando il livello di protezione dei dati personali negli scambi commerciali con Stati terzi. Al contrario, come indicato anche dal nuovo regolamento, la strada da seguire non può che essere quella di instaurare iniziative a livello internazionale per estendere il diritto alla protezione nel trattamento dei dati personali, come *standard* non più rinunciabile da parte del legislatore[101].

[100] Il General Agreement on Trade in Services («GATS») ammette, tra le eccezioni generali all'applicazione delle sue disposizioni, «the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts»: v. l'Art. XIV(*c*)(*ii*), entrato in vigore il 1° gennaio 1995 (in https://www.wto.org/english/docs_e/legal_e/26-gats.pdf): «Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures: […]; c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: […]; (*ii*) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; […]». Nessuna decisione del Panel ha finora interpretato l'Art. XIV(c)(ii). Invece, nel quadro del WTO (*World Trade Organization*), esiste un *Work Programme on Electronic Commerce*, adottato dal General Council il 25 settembre 1998, (doc. WT/L/274, 30 September 1998, 98-3738 in https://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm, adottato a seguito della *Geneva Ministerial Declaration on Global Electronic Commerce* del 20 maggio 1998 (WT/MIN (98)/DEC/2, 92-2148, 25 May 1998, in https://www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm), che elenca, tra le questioni che il *Council for Trade in Services* dovrà esaminare, *«protection of privacy and public morals and the prevention of fraud (Article XIV)»* (par. 2.1). In dottrina, cfr., per tutti, M.V. Pérez Asinari, *Is There Any Room for Privacy and Data Protection Within the WTO Rules?, in The Electr. Commun.* Law Rev., 2002, p. 249 ss.

[101] Sull'influenza della disciplina europea sulle iniziative promosse a livello internazionale in relazione alla protezione dei dati personali, cfr. G. Greenleaf, *The Influence*

Abstract

This paper examines the EU Court of justice's judgment in the case Maximillian Schrems v. Data Protection Commissioner. In this landmark ruling, the Court declares that the European Commission's decision enforcing the «Safe Harbor» agreement between the US Department of Commerce and the European Union, read in the light of Articles 7, 8 and 47 of the EU Charter of Fundamental Rights, is invalid. Although the Commission found that the American legal system affords an adequate level of protection of personal data, the Court holds that the law and practices in force in the USA at the time of the facts of the case did not ensure a protection sufficient to comply with the requirements of the EU legislation on the protection of such data. The Court further determines that national supervisory authorities of Member States may examine claims concerning violation of an individual's rights in regard to the processing of his personal data which has been transferred to a third country.

The analysis of the judgement is conducted in two parts. The first briefly presents the basic elements of the case and outlines the fundamental requirements of directive 95/46/CE (the «General Data Protection Directive») and its mechanism of transfers of personal data to third countries. The second part identifies the reasons of the Court's decision and discusses some of the problematic consequences raised by the case. These include the effective functioning of the EU data protection law and the Charter of Fundamental Rights; the «complete independence» of functions of Member States' national supervisory authority; the Commission's power to adopt adequacy decisions regarding third States; the legal effects of the declaration of invalidity of the «Safe Harbor» decision and its disruptive practical consequences on transatlantic data transfers.

The issues raised by the Court's ruling are also examined under the new General Data Protection Regulation's draft text, since the European institutions have reached agreement on this important measure, which is due to abrogate and substitute the directive.

A further scrutiny is devoted to the new Commission's proposal for a «EU-US Privacy Shield», which is intended to substitute the «Safe Harbor» decision.

The comment concludes with a brief general assessment of the questions that the judgment of the Court leaves open, and some observations regarding the tense relationships with the USA because of the tentative assertion by the EU legislator of its data protection legal framework as a model legislation at a global level.

of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108, in *Intern. Data Privacy Law*, 2012, p. 68 ss.