Alessandro Mantelero

I flussi di dati transfrontalieri e le scelte delle imprese tra Safe Harbour *e* Privacy Shield

Sommario: Premessa. La *ratio* del «Safe Harbour» ed il suo vizio d'origine. – 1 Il post «Safe Harbour». Strategia di breve periodo. – 1.1 (*segue*). Strategia di medio periodo. – 1.2 (*segue*). Strategia di lungo periodo e valore competitivo della tutela dei dati personali. – 2. Prime conclusioni. – 3. «Privacy Shield». Quasi un epilogo

Premessa. La ratio del Safe Harbour *ed il suo vizio d'origine*

La sentenza della Corte di Giustizia dell'Unione europea sul caso Schrems[1] ha posto fine ad un compromesso, il «Safe Harbour», frutto di un'intesa politica fra Stati Uniti ed Unione europea. Non è infatti possibile ridurre il «Safe Harbour» ad un semplice programma di autocertificazione[2] adottato dal governo statunitense (Department of Commerce) al fine di individuare le imprese che si impegnavano ad offrire uno standard di tutela ritenuto dalla Commissione Europea adeguato ai sensi dell'art. 25, dir. 95/46/CE.[3] Una tale formale ed anonima costruzione, incentrata sul

[1] Cfr. Corte di Giustizia dell'Unione europea, 6 ottobre 2015, C-362/14, *Maximillian Schrems v Data Protection Commissioner, Digital Rights Ireland Ltd*, http://curia.europa.eu/juris/liste.jsf?num=C-362/14. Ad eccezione del paragrafo 3, tutti i link ipertestuali a cui è fatto rinvio nelle presenti note sono riferiti a contenuti disponibili *online* e visionati in data anteriore al 15 novembre 2015.

[2] Cfr. European Commission, *Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*, 2000/520/EC (in seguito European Commission, 2000/520/EC), Annex I e Annex II, FAQ n. 6.

[3] Con riguardo alla nozione di 'adeguatezza', la Corte precisa che «The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to

giudizio di adeguatezza, cela infatti le reali ragioni dell'accordo, ragioni che ne hanno incisivamente influenzato i contenuti.

Per comprendere l'effettiva portata giuridica e le conseguenze della decisione che ha invalidato il «Safe Harbour» e per delineare i possibili scenari futuri, occorre dunque adottare una prospettiva più ampia, superando una visione parcellizzata ed atomistica dei fenomeni giuridici. Serve quindi partire dalle origini, ovvero dai motivi che portarono all'accordo con gli Stati Uniti e dalla natura eccezionale dello stesso.[4] Perché lì risiede la *ratio* dell'anomalia che ha indotto la Corte di Giustizia alla dichiarazione d'invalidità, stante la natura genetica del vizio.

I giudici di Lussemburgo hanno rilevato come la Commissione Europea, chiamata a valutare il livello di tutela offerto dalla normativa statunitense in termini di protezione dei dati, non abbia di fatto tenuto conto del quadro regolamentare, sostituendo l'adeguatezza dello strumento («Safe Harbour»)[5] all'adeguatezza dell'ordinamento statunitense, creando un *tertium genus* non previsto dagli artt. 25 e 26 della direttiva. Tali norme delineano infatti solamente due modalità volte a garantire un livello adeguato di protezione dei dati: l'accordo fra *data importer* e *data exporter* o l'esistenza nel Paese terzo di un ordinamento giuridico che offra tale livello di protezione.[6]

La Commissione sembra dunque aver ravvisato nel «Safe Harbour» una sorta di accordo quadro fra imprese statunitensi ed europee, non è

ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter».

[4] Si vedano in proposito le considerazioni espresse da G. Resta, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE* e da S. Sica e V. D'Antonio, *I Safe Harbour Privacy Principles: genesi, contenuti, criticità*, entrambi in questo Volume.

[5] Cfr. European Commission, 2000/520/EC, cit., considerando n. 5 nel preambolo della decisione ed art. 1.

[6] Nello specifico, ai sensi dell'art. 25(6) dir. 95/746/EC, la Commissione può valutare che il livello di protezione offerto dal Paese terzo sia adeguato anche in ragione «of the international commitments it has entered into», per cui il «Safe Harbour» poteva astrattamente costituire lo strumento per garantire l'adeguatezza. Il vizio, che ha portato all'invalidità dell'accordo in questione, sta però nel fatto che l'adeguatezza è stata riconosciuta sulla base della sola adesione al «Safe Harbour», senza considerare che tale accordo prevedeva ampie deroghe a favore della legislazione statunitense, in virtù delle quali quest'ultima prevaleva sugli obblighi imposti dall'accordo alle imprese aderenti. Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit., punti 83-84. In conseguenza di ciò, un giudizio corretto sull'adeguatezza della tutela offerta ai dati negli USA avrebbe dovuto tenere conto anche delle disposizioni vigenti, per la parte in cui prevalevano sull'accordo «Safe Harbour». Cfr. anche i successivi punti 87-88 e 96-97.

tuttavia questa la natura del «Safe Harbour». Occorre dunque chiedersi quali ragioni hanno indotto la Commissione a travisare consapevolmente il disposto dell'art. 26 e come sia stato possibile che per tre lustri un sistema ampio e complesso di flussi transfrontalieri si sia retto su un accordo illegittimo, senza alcuna sospensione o revoca dello stesso.[7]

In questi anni molte voci critiche si sono levate contro il «Safe Harbour», sostanzialmente in quanto la nozione di 'porto sicuro' appariva più un salvacondotto agevolmente rilasciato alle imprese statunitensi,[8] che

[7] Non sono mancate, in tempi recenti, prese di posizione critiche da parte delle istituzioni comunitarie, cfr. European Commission, *Communication from the Commission to the European Parliament and the Council. Rebuilding Trust in EU-US Data Flows*, COM(2013) 846 final, Brussels, 27 novembre 2013; European Commission, *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, Brussels, 27 novembre 2013, COM(2013) 847 final. Cfr. anche European Parliament, *Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, Strasburgo, 12 marzo 2014, P7_TA(2014)0230, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=EN&ring=A7-2014-0139. Nessuna di tale azione si è tuttavia tradotta in una sospensione dell'accordo, ma solamente le istituzioni comunitarie si sono adoperate per una rinegoziazione dello stesso. La sospensione dell'accordo è stata tuttavia richiesta dalla Commissione Civil Liberties, Justice and Home Affairs del Parlamento Europeo, cfr. LIBE Committee, *NSA snooping: MEPs table proposals to protect EU citizens' privacy Fundamental rights*, Press release 12 febbraio 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20140210IPR35501%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN. In merito all'impatto dei programmi di sorveglianza di massa statunitensi sulla dialettica fra Unione europea e Stati Uniti con riguardo al trattamento transfrontaliero di dati, si rinvia all'analisi svolta da G. Resta, *La sorveglianza di massa e il conflitto regolatorio USA/UE*, cit.

[8] Cfr. C. Connolly, *EU/US Safe Harbor – Effectiveness of the Framework in relation to National Security Surveillance. Speaking/background notes for an appearance before the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) inquiry on «Electronic mass surveillance of EU citizens»*, Strasburgo, 7 ottobre 2013, http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf. Cfr. anche le dichiarazioni rilasciate da Jeff Chester, executive director del Center for Digital Democracy, in J. Chester, *CDD Files Complaint on U.S./EU Safe Harbor for Data Privacy at FTC/ Filing Reveals Failure of U.S. Agreement to Protect European Privacy*, Center for Digital Democracy, 14 agosto 2014. https://www.democraticmedia.org/content/cdd-files-complaint-useu-safe-harbor-data-privacy-ftc-filing-reveals-failure-us-agreement («Instead of ensuring that the U.S. lives up to its commitment to protect EU consumers, our investigation found that there is little oversight and enforcement by the FTC. The Big Data-driven companies in our complaint use Safe Harbor as a shield to further their information-gathering practices

una garanzia per i cittadini europei circa il trattamento dei propri dati oltreoceano.[9] I princìpi del «Safe Harbour»,[10] cui le imprese statunitensi dovevano aderire per ricevere informazioni personali dall'EEA senza dover porre in essere adempimenti ulteriori, erano già in sé una 'riduzione' delle disposizioni chiave della normativa comunitaria in materia. A ciò si aggiunga una prassi in cui molte delle imprese aderenti al «Safe Harbour» non risultavano di fatto nemmeno conformarsi ai requisiti richiesti dall'accordo stesso.[11]

Sino a qui dunque, e per sommi capi, i caratteri distintivi dell'accordo; per cogliere le ragioni dell'anomalia del «Safe Harbour» occorre però guardare altrove, al disposto dell'art. 25 della dir. 95/46/CE ed alla *ratio* ispiratrice di tale disposizione. La logica sottostante risiede nell'intento di non vanificare gli sforzi posti in essere dagli Stati europei nel dotarsi di uno standard in gran parte uniforme in materia di protezione dei dati personali, attestato su un livello di più elevato di quello offerto dagli altri modelli esistenti.[12]

Creata, non senza difficoltà, questa comune area di circolazione sicura dei dati, in termini di tutela offerta, l'Unione europea non poteva veder vanificata la propria opera ammettendo che processi di delocalizzazione delle risorse informative potessero sottrarre i dati personali alla disciplina comunitaria. La ragione ultima delle dinamiche che hanno portato al

without serious scrutiny. Companies are relying on exceedingly brief, vague, or obtuse descriptions of their data collection practices, even though Safe Harbor requires meaningful transparency and candor. Our investigation found that many of the companies are involved with a web of powerful multiple data broker partners who, unknown to the EU public, pool their data on individuals so they can be profiled and targeted online»). Meno critici a riguardo S. Sica e V. D'Antonio, *I Safe Harbour Privacy Principles: genesi, contenuti, criticità*, cit., i quali rilevano come i Safe Harbour Principles abbiano rappresentato «una sorta di by-pass tra la tutela dei dati personali di stampo comunitario e il diverso approccio adottato negli Stati Uniti».

[9] Cfr. Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein, *Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015*, C-362/14, 14 October 2015, punto 4, https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html («the CJEU argued that the Commission did not make any statement about the level of data protection in the US, but instead chose with the Safe Harbour principles, an inapt construction as compensation for an inadequate level of protection»).

[10] Per una disamina di tali principi si rinvia a S. Sica e V. D'Antonio, *I «Safe Harbour» Privacy Principles: genesi, contenuti, criticità*, cit.

[11] Cfr. supra n. 5 e 6.

[12] Cfr. anche Corte di Giustizia dell'Unione europea, C-362/14, cit., punto 73.

«Safe Harbour» risiede dunque nella tensione cui è sottoposta la nozione di territorialità del diritto in relazione alle tecnologie digitali ed alla diffusione delle reti elettroniche di comunicazione.[13]

Abbandonati i dati cartacei e l'età dei *mainframe*, in cui per ragioni diverse lo spostamento di banche dati da un luogo all'altro risultava non solo complesso, ma anche facilmente monitorabile, nell'era della rete internet in cui terabyte di dati possono fluire agevolmente da un qualsiasi computer di un cittadino europeo verso qualsiasi punto del globo, appare estremamente fragile l'idea di creare mura a difesa dei propri standard di protezione. Non a caso la stessa Cina, che molto ha investito nella protezione dei propri confini informatici sia in termini tecnologici che normativi, conosce non pochi casi di aggiramento del proprio sistema.

Come potevano dunque gli stati europei pensare di aver successo in una simile opera 'difensiva', seppur animata dall'intento di offrire maggior tutela ad un diritto fondamentale? La chiave di volta del modello europeo, che ne ha segnato l'indubbio successo in termini di circolazione e recezione ad opera di Paesi terzi,[14] non è stata né la forza politica, né quella tecnologica, bensì quella economica, intesa non come forza intrinseca delle imprese europee, bensì come sfruttamento dei legami di interdipendenza esistenti in un contesto di economia globalizzata.

Non i Paesi terzi, bensì le imprese europee sono state nel contempo il *target* e gli alfieri della diffusione del modello europeo. Ponendo la regola secondo cui i dati personali non possono essere inviati al di fuori dell'EEA verso Paesi che non offrano adeguati livelli di tutela,[15] si è in concreto fatto leva sulla dipendenza reciproca esistente fra imprese commerciali europee ed imprese dei Paesi terzi, in un contesto di economia dell'informazione.

Come dimostrato *ex post* dalle reazioni che hanno fatto seguito alla decisione della Corte di Giustizia, il valore assunto dai dati in tutti gli aspetti della vita economica ha reso impensabile che, da un lato, le imprese europee potessero decidere di circoscrivere la loro operatività entro i confini dello spazio economico europeo che, d'altro canto, che, per non

[13] Cfr. in proposito la più ampia disamina sul rapporto fra regolamentazione e sovranità digitale nelle reti globali elaborata da V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in questo Fascicolo.

[14] Cfr. G. Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108, in International Data Privacy Law*, 2012, 2(2), 68 ss.; G. Greenleaf, *Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority, in Privacy Laws & Business International Report*, 2015, 133.

[15] Cfr. art. 25 dir. 95/46/CE.

adempiere alle norme in materia di *data protection*, i *partners* commerciali delle imprese europee decidessero di rinunciare agli accordi negoziali in essere con esse.

Non solo, sotto il profilo organizzativo, una volta che le suddette ragioni hanno indotto le imprese dei Paesi terzi ad adottare standard simili a quelli comunitari, si è in molti casi generata una sorta di propagazione spontanea di questi ultimi. In un contesto dominato dall'elaborazione aggregata delle informazioni originate da fonti diverse, è risultato infatti sovente impossibile od inefficiente, per i *partners* degli operatori comunitari, separare i dati provenienti da questi ultimi dai dati propri.

Infine, gli stati stessi, spesso a ciò indotti dalle proprie imprese, hanno ritenuto vantaggioso adottare delle norme in materia di *data protection* che fossero conformi al modello comunitario, onde ridurre gli oneri in capo alle imprese locali in termini di negoziazione ed adeguamento al livello di tutela richiesto dall'Unione.[16]

Una simile forma di circolazione del modello europeo, incentrata sulle dinamiche proprie delle relazioni commerciali, non poteva di certo operare pienamente nei confronti dell'attuale maggiore potenza economica ovvero gli USA. Questo non solo in ragione della forza delle società nordamericane, ma soprattutto in conseguenza della forza politica del governo e delle istituzioni statunitensi.

In quest'ottica, il «Safe Harbour» viene alla luce come compromesso, come soluzione figlia di accordi politici. L'accordo in questione viene poi accolto favorevolmente da parte degli operatori economici di entrambe le sponde dell'Atlantico, essendo ancora lontana una cultura diffusa della *data protection* come valore di impresa e fattore competitivo, prevalendo invece una lettura che ravvisa nella tutela dei dati una mera voce di costo.

[16] Si veda in proposito il caso emblematico dell'India e dell'interesse all'adozione di un modello simile a quello europeo al fine di attrarre la delocalizzazione dei servizi di outsourcing informatico, su cui volendo A. Mantelero, *La nuova normativa indiana in materia di* data protection*: la protezione dei dati declinata in maniera funzionale all'*outsourcing, in *Contratto e impr. Europa*, 2011, 728 ss. Cfr. anche G. Greenleaf, *Promises and illusions of data protection in Indian law*, in *International Data Privacy Law*, 2011, 1 (1), 47 ss.

1. Il post «Safe Harbour». Strategia di breve periodo

Se questi sono gli antecedenti storici della situazione attuale, occorre chiedersi quali siano le attese per il futuro in termini di tutela delle informazioni provenienti dall'Unione europea ove trattate dalle imprese statunitensi. A tal proposito pare opportuno distinguere fra scenari e soluzioni giuridiche di breve, medio e lungo periodo. Questo poiché le prospettive di un nuovo accordo, come gli strumenti legali per legittimare il flusso transfrontaliero di dati, hanno tempi di realizzazione ed oneri variabili, ragion per cui è immaginabile che gli operatori economici possano elaborare scelte differenziate nel tempo, anche in ragione della loro dimensione organizzativa e della natura e complessità dei flussi transfrontalieri cui danno origine.

Va in primo luogo rilevato come l'invalidità del «Safe Harbour» non escluda, in teoria, un giudizio positivo sull'adeguatezza della tutela offerta dall'ordinamento statunitense, tanto è vero che sul punto, a seguito della decisione della High Court irlandese successiva al rinvio pregiudiziale,[17] spetterà al garante irlandese pronunciarsi sul caso posto all'esame dei giudici lussemburghesi e valutare se il flusso transfrontaliero verso gli USA originato da Facebook sia tale da esporre i dati dei cittadini europei ai rischi derivanti da un livello di tutela che non sia «essentially equivalent» a quello goduto nell'Unione.

Poiché tuttavia nella pronuncia della Corte di Giustizia sono già presenti molti indici per concludere in senso negativo suddetta valutazione, ben si spiega come sin da subito la macchina politica si sia mossa su entrambe le sponde dell'Atlantico al fine di raggiungere quanto prima una nuova soluzione compromissoria basata su un accordo bilaterale. Non solo, le stesse autorità garanti - cui la Corte di Giustizia ha riconosciuto un ruolo decisivo nella valutazione della legittimità dei flussi transfrontalieri verso gli USA – hanno sposato una strategia attendista.

Se si eccettua infatti la posizione del garante dello Schleswig-Holstein, le autorità nazionali, attraverso l'Article 29 Data Protection Working Party, hanno ribadito l'illegittimità dei trattamenti effettuati sulla base dell'accordo dichiarato invalido, ma nello stesso tempo hanno concesso più di tre mesi alle parti in gioco (imprese e governi) per addivenire ad una soluzione. Pronta in tal senso la reazione della Commissione Europea che ha spinto per una rapida rinegoziazione del «Safe Harbour».

[17] Cfr. a riguardo Europe-v-facebook, *Irish High Court: DPC to investigate Facebook's PRISM participation*, 21 ottobre 2010, http://www.europe-v-facebook.org/MU_HC.pdf.

Fino a qui dunque, per alcuni aspetti, un copione che si ripete, con lo scivolamento dal piano giuridico, rappresentato dal baluardo del giudizio di adeguatezza di cui all'art 26 della dir. 95/46/CE, verso il piano politico, basato su accordi bilaterali. La sensazione è che però, dopo la decisione della Corte di Giustizia ed in ragione delle motivazioni addotte dai giudici, non sia possibile una replica di quanto accaduto in passato.[18]

La conclusione in tempi rapidi di un nuovo accordo è tuttavia fortemente voluta dagli USA e dalla Commissione Europea, nonché dalle imprese interessate ai flussi transfrontalieri, laddove gli attori politici guardano al buon andamento dei rapporti bilaterali, mentre gli operatori commerciali alla semplificazione degli adempimenti in materia di tutela dei dati. Al raggiungimento di questo obiettivo pare però frapporsi il *decisum* della Corte, che ha fortemente limitato i margini di manovra (e di deroga) della Commissione.

In primo luogo va ricordato che, come correttamente evidenziato dalla Corte di Giustizia,[19] un accordo internazionale può fornire uno standard adeguato di tutela a condizione che non contenga deroghe in favore di disposizioni nazionali la cui adeguatezza in termini di tutela non è accertata o non sussiste. Nello specifico dunque, o si addiviene ad un nuovo accordo ove si prevede che le imprese aderenti non siano vincolate dalle disposizioni nazionali USA in conflitto con gli obblighi in materia di protezione dei dati personali previsti da tale accordo, oppure la riproposizione di deroghe in favore delle norme in materia di sorveglianza governativa esistenti negli USA implica necessariamente una valutazione dell'adeguatezza di quest'ultime. Valutazione che, in ragione dell'ampio spettro di intervento di tali disposizioni,[20] difficilmente pare ipotizzarsi come positiva.

Alla luce di tali punti fermi posti dalla decisione sul caso Schrems non sembra dunque più possibile per la Commissione addivenire ad un accordo sui flussi transfrontalieri verso gli USA senza che vengano meno i limiti esistenti con riguardo alla tutela offerta dall'ordinamento statunitense.

[18] Sulla valenza politica delle decisioni assunte dalla stessa Corte di Giustizia, si veda G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a* Schrems, in questoVolume.

[19] Cfr. supra nota 6

[20] Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit., punto 93. Sulla natura ancora estesa della sorveglianza realizzata negli USA ad opera delle agenzie governative, anche dopo le riforme del 2013, cfr. T. Edgar, *Focusing PRISM: An Answer to European Privacy Concerns?*, in *Lawfare*, 2 novembre 2015, https://www.lawfareblog.com/focusing-prism-answer-european-privacy-concerns.

In tal senso, le autorità americane paiono aver colto il problema, come dimostrato dall'accelerazione avutasi nell'*iter* del Judicial Redress Act, che dovrebbe garantire la tutela giurisdizionale in favore dei soggetti europei interessati dal trattamento, in linea con quanto richiesto dalla Corte di Giustizia.[21] Rimane però il nodo dell'esteso ambito di operatività riconosciuto dalle leggi statunitensi alle agenzie investigative nell'accesso ai dati. Tali poteri, come rilevato dalla Corte di Giustizia, non sono compatibili con un generalizzato riconoscimento di un sufficiente livello di adeguatezza della tutela offerta dall'ordinamento statunitense.

Un accordo onnicomprensivo come il «Safe Harbour», con la previsione di ampie deroghe in favore della legislazione nazionale ed a discapito della tutela prevista per i dati personali,[22] può dunque solamente essere sostituito con un diverso accordo che ammetta solo eccezionalmente ipotesi di deroga rispetto al livello di protezione accordato.[23] Questo però richiederebbe la contemporanea riforma delle vigenti norme statunitensi che riconoscono poteri ispettivi alle agenzie governative nordamericane.[24] Per tale motivo una reale rinegoziazione dell'accordo UE-USA pare costituire più che altro una strategia di medio-lungo periodo.[25]

Quanto sopra non toglie tuttavia che le ragioni della politica possano

[21] Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit., punto 95. Cfr. *infra* § 1.2.
[22] Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit., punto 84.
[23] Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit., punto 92 («above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary»). Cfr. in tal senso Corte di Giustizia dell'Unione europea, 8 aprile 2014, *Digital Rights Ireland* e altri, cause riunite C-293/12 e C-594/12, punto 52, http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=404932; Corte di Giustizia dell'Unione europea, 7 novembre 2013, *Institut professionnel des agents immobiliers (IPI) contro Geoffrey Englebert e altri*, C-473/12, punto 39, http://curia.europa.eu/juris/liste.jsf?num=C-473/12; Corte di Giustizia dell'Unione europea, 16 dicembre 2008, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, C-73/07, punto 56, http://curia.europa.eu/juris/liste.jsf?language=en&num=C-73/07; Corte di Giustizia dell'Unione europea, 9 novembre 2010, *Volker und Markus Schecke e Eifert contro Land Hessen*, C-92/09 e C-93/09, punti 77 e 86, http://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=406004.
[24] Cfr. Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein, *Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015*, C-362/14, cit. («the US can currently show no effective means to ensure protection essentially equivalent to the level of protection guaranteed within the European Union»).
[25] Cfr. *infra* § 1.2.

indurre ad un nuovo accordo bilaterale, anche in difformità delle indicazioni della Corte di Giustizia. Certamente la validità dello stesso potrebbe essere contestata di fronte alle autorità garanti nazionali e poi posta all'attenzione della Corte di Giustizia che necessariamente dovrebbe giungere alla declaratoria di invalidità. Nell'ottica di una strategia dilatoria, questo porterebbe tuttavia a guadagnare un paio di anni e, considerata anche la congiuntura politica statunitense (elezioni presidenziali) e le trattative in corso sul fronte della Transatlantic Trade and Investment Partnership, questo potrebbe essere un tempo utile per conseguire una riforma dell'esistente quadro normativo statunitense in materia di *data protection* e di poteri delle forze di intelligence.

Nelle more di un eventuale nuovo accordo, potrebbe dunque prevalere una logica attendista, specie fra le piccole e medie imprese, in considerazione dei costi dell'eventuale adozione degli strumenti volti a legittimare i flussi transfrontalieri di dati.[26]

1.1 (segue). Strategia di medio periodo

Sebbene prevalga un certo immobilismo, in attesa di vedere cosa accadrà allo scadere dell'*ultimatum* posto dalle autorità garanti,[27] molti operatori economici si stanno interrogando su quali siano le soluzioni più idonee per offrire un'adeguata base giuridica ai flussi transfrontalieri di dati cui danno vita nel corso dello svolgimento delle proprie attività.[28] Questo anche alla luce del fatto che, come precisato dalla Corte di Giustizia, un nuovo «Safe Harbour» non sarà comunque immune dal sindacato delle autorità garanti.[29]

[26] Cfr. paragrafo successivo.

[27] Cfr. Article 29 Data Protection Working Party, *Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case* (C-362-14), Brussels, 16 ottobre 2015, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf, in cui i garanti europei hanno chiarito che «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».

[28] Ad oggi infatti solo le imprese più lungimiranti, che avevano affiancato l'adozione delle *standard contractual clauses* ai benefici del «Safe Harbour», risultano essere in una posizione di vantaggio competitivo potendo ostentare la conformità alla legge dei propri servizi.

[29] Cfr. anche Corte di Giustizia dell'Unione europea, 1 ottobre 2015, C-230/14,

Standard contractual clauses, *binding corporate rule*s, clausole contrattuali *ad hoc*, consenso dell'interessato, sono dunque stati prontamente riscoperti dai consulenti legali ed esperti di *privacy* in tutto il mondo. Soluzioni prima accantonate perché onerose e limitanti, a fronte della maggior semplicità dell'adesione ai «Safe Harbour» Principles, sono ora prese nuovamente in considerazione dalle imprese statunitensi e dai loro *partners* europei.

Rispetto alle diverse alternative, che possono offrire non solo una pronta risposta nell'intermezzo fra il vecchio ed il nuovo «Safe Harbour», ma anche una maggior garanzia di tutela stabile per il futuro, occorre però fare dei distinguo in termini di onerosità ed efficacia.

L'opzione più semplice appare certamente quella di avvalersi del disposto dell'art 26 (a), dir. 95/46/CE, laddove si prevede che il consenso dell'interessato possa validamente legittimare il flusso di dati verso un Paese terzo. La norma, in linea con l'art. 7(a) della direttiva, richiede però che il consenso dell'interessato sia prestato «unambiguously». Posto che, ai sensi dell'art. 2(h) il consenso dell'interessato consiste nella «freely given specific and informed indication of his wishes»,[30] ne consegue che il soggetto dovrebbe ricevere adeguate informazioni circa le modalità e finalità del trattamento connesso ai flussi transfrontalieri, nonché circa gli eventuali ulteriori trattamenti posti in essere da terze parti successivamente al trasferimento dei dati. Non solo, poiché l'art. 26(a) prevede la possibilità di invio di informazioni personali verso un Paese terzo che non offre un adeguato livello di protezione in virtù del consenso dato «unambiguously», ne consegue che l'interessato dovrà quanto meno essere informato circa tale carenza di protezione ed in cosa questo si concretizzi, in termini di rischio per i dati che lo riguardano.

Questo contesto normativo esclude in primo luogo la possibilità del ricorso esteso al consenso dell'interessato al fine di legittimare una molteplicità pressoché indistinta di trattamenti.[31] Ma soprattutto, relativamente all'invio dei dati verso gli USA, implica che l'interessato dovrebbe essere consapevole dei poteri propri delle agenzie investigative statunitensi, delle

Weltimmo s. r. o. contro Nemzeti Adatvédelmi és Információszabadság Hatóság, http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=406747.

[30] Cfr. riguardo D. Beyleveld-R. Brownsword, *Consent in the law*, Oxford-Portland, 2007, 126.

[31] Cfr. Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 13luglio 2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

conseguenze in termini di trattamento dati e delle lacune che affliggono l'ordinamento statunitense con riguardo ad un'effettiva tutela dei dati personali.[32]

A ciò si aggiunga che l'idea del consenso dell'interessato come espressione di una volontà consapevole ed informata è sempre più oggetto di critiche da parte della dottrina giuridica, stante la complessità dei trattamenti dati realizzati e la difficoltà di fornire un'adeguata e comprensibile informativa all'interessato.[33] Posto che ad oggi risultano ancora in parte oscure le articolate modalità di trattamento realizzate negli USA attraverso l'interazione fra attori pubblici e privati,[34] pare dunque viepiù improbabile che queste possano essere oggetto di un'adeguata informativa, che è il presupposto per un consenso consapevole.

Come poi correttamente sottolineato dal garante dello Schleswig-

[32] Cfr. anche Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein, *Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015*, C-362/14, cit.

[33] Cfr. L. Brandimarte, A. Acquisti e G. Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, 2010, Ninth Annual Workshop on the Economics of Information Security, http://www.heinz.cmu.edu/~acquisti/papers/acquisti-SPPS.pdf; J. Turow, C. J. Hoofnagle, D. K. Mulligan e N. Good, *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, in *ISJLP*, 2007, 3, 723 ss., http://scholarship.law.berkeley.edu/facpubs/935; Federal Trade Commission, *Data brokers. A Call for Transparency and Accountability*, 2014, 42, http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; R. M. Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, in *Notre Dame L. Rev.*, 2013, 87(3), 1027 ss.; D. J. Solove, *Introduction: Privacy Self-management and The Consent Dilemma*, in *Harv. L. Rev.*, 2013, 126, 1883 ss.

[34] Cfr. European Parliament, *Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy*, Strasburgo, 4 luglio 2013, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//EN; European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, *The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens*, 2013, 14 ss., http://info.publicintelligence.net/EU-NSA-Surveillance.pdf; European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, *National Programmes for Mass Surveillance of Personal data in EU Member States and Their Compatibility with EU Law*, 2013, 12 ss., http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf.

Holstein,[35] l'ampiezza delle deroghe previste dall'ordinamento statunitense in favore dei servizi governativi è tale da minare significativamente i diritti fondamentali dell'individuo,[36] ragion per cui l'eventuale consenso dell'interessato si tradurrebbe nella rinuncia a far valere diritti per loro natura irrinunciabili. Va infatti rilevato come, pur riconoscendo margini di libertà all'individuo in termini di disponibilità dell'esercizio dei propri diritti della personalità,[37] permangano i limiti posti dall'irrinunciabilità del diritto stesso, che non ne consentono una compressione eccessiva basata sul consenso dell'interessato.[38]

Se si pensa dunque alla raccolta massiva e continua di informazioni realizzata dalle agenzie governative statunitensi,[39] alle capacità di impiego di software di *big data analytics* per estrarre ulteriori inferenze da tali dati ed alla mancanza di adeguate tutele per l'interessato, si evince chiaramente come il consenso ad un trattamento che implica tali conseguenze si traduca nella sostanziale parziale rinuncia alle prerogative costitutive del diritto fondamentale alla protezione dei dati riconosciuto al singolo, la cui ammissibilità contrasta con il nucleo indisponibile di tale diritto.[40]

Si deve in tal senso riflettere sul ruolo stesso riconosciuto in generale dalla direttiva comunitaria al consenso dell'interessato, che costituisce un

[35] Cfr. anche Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein, *Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015*, C-362/14, cit.

[36] Cfr. artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

[37] Cfr. anche G. Resta, *I diritti della personalità*, in G. Alpa e G. Resta, *Le persone fisiche e i diritti della personalità, in Trattato di Diritto Civile*, diretto da R. Sacco, Torino, 2006, 560 ss.; G. Resta, *Contratto e persona*, in V. Roppo (a cura di), *Trattato del Contratto*, vol. VI, *Interferenze*, Milano, 2006, 67 ss.; A. Orestano, *La circolazione dei dati personali*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, vol. II, 142 ss.; V. Zeno-Zencovich, *Profili negoziali degli attributi della personalità*, in *Dir. Inf.* 1993, 545 ss. Per maggiori riferimenti dottrinali, in ragione dell'economia del presente scritto, si rinvia a A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, 2007, 69 ss. Cfr. anche P. M. Schwartz, *Property, Privacy, and Personal Data*, in *Harv. L. Rev.*, 2003, 117, 2056 ss.; P. Samuelson, *Privacy as Intellectual Property*, in *Stan. L. Rev.*, 1999, 52, 1125 ss.

[38] Cfr. G. Resta, Il diritto alla protezione dei dati personali, in F. Cardarelli, S. Sica e V. Zeno-Zencovich (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 53 ss.

[39] Cfr. *supra* nota 34

[40] Cfr. art. 52, c. 1, Carta dei diritti fondamentali dell'Unione europea. Cfr. anche V. Zeno-Zencovich, *Profili negoziali degli attributi della personalità*, cit., 549; C. Scognamiglio, *Il diritto all'utilizzazione economica del nome e dell'immagine delle persone celebri*, in *Dir. Inf.* 1988, 139 s.; C. Pedrazzi, voce *Consenso dell'avente diritto*, in *Enc. Dir.*, vol. IX, Milano, 1961, § 9.

presupposto di legittimazione del trattamento, ma non prescinde dalla necessaria sussistenza degli altri requisiti di liceità di quest'ultimo, *in primis* quello di proporzionalità.

Posto che anche la generazione di un flusso transfrontaliero rappresenta una modalità di trattamento, v'è da chiedersi come possa il consenso dell'interessato legittimare un flusso di dati che, per le ulteriori modalità di trattamento successive all'invio dei dati verso Paesi terzi, si configura come contrastante con i princìpi di liceità del trattamento. In proposito, pare doversi escludere che il consenso possa da solo sopperire ai limiti che connotano il trattamento in termini di proporzionalità dello stesso, ovvero alla carenza di determinatezza delle finalità o alla mancanza di trasparenza circa le modalità di gestione dei dati, tutti aspetti che ad oggi affliggono il possibile utilizzo delle informazioni ad opera delle agenzie governative statunitensi.

Va infine osservato come il ricorso al consenso dell'interessato ponga problemi specifici connessi alla diversità di disciplina esistente nei vari Paesi dell'UE con riguardo alla prestazione dello stesso (si pensi ad es. al consenso relativo ai minori per i dati che li riguardano), cui si aggiunge la difficoltà di fare ricorso a tale strumento in situazioni ove la libertà del consenso rispetto al trattamento transfrontaliero dei dati può risultare limitata o dubbia (e.g. rapporti di lavoro).

Stanti gli evidenti limiti posti ad una legittimazione dei flussi transfrontalieri incentrata sul solo consenso dell'interessato, le imprese dovranno necessariamente valutare soluzioni alternative o complementari. A tal proposito, gli strumenti che assumono maggior rilievo sono in primo luogo le già richiamate *standard contractual clauses* approvate dalla Commissione Europea,[41] cui si affiancano le c.d. Binding Corporate Rules[42] e, da ultimo,

[41] Cfr. European Commission, *Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271)*, 2004/915/EC, Annex (in seguito abbreviata come European Commission, 2004/915/EC) e European Commission, *Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593)*, 2010/87/EU (in seguito European Commission, 2010/87/EU). Cfr. anche European Commission, *Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (notified under document number C(2001) 1539)*, 2001/497/EC (in seguito European Commission, 2001/497/EC). Tutti i testi sono consultabili al seguente indirizzo: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

[42] Cfr. Article 29 Data Protection Working Party, Working Document: Transfers

gli accordi individuali fra *data importer* e *data exporter*.

Senza qui anticipare la più dettagliata disamina di tali istituti che verrà svolta altrove,[43] va rilevato come, dal punto di vista dell'impresa, le soluzioni ora elencate comportino nuovi oneri organizzativi, che possono trovare giustificazione solo in un'ottica di medio o lungo periodo. A differenza del consenso dell'interessato, la scelta su quale fra le strategie in questione porre in essere richiede quindi una valutazione preliminare circa la natura, la complessità e la rilevanza dei flussi transfrontalieri che interessano l'impresa, nonché della continuità degli stessi nel tempo.

In tale ottica, prima ancora di optare per un rimedio o per l'altro, andrebbe accuratamente monitorato il trattamento dati in questione, valutando soluzioni di minimizzazione dell'impiego dei dati personali e, ove possibile, optando per il ricorso all'anonimizzazione. È infatti noto come le prassi operative aziendali[44] non di rado diano vita a trattamenti ridondanti, eccessivi o superflui, che già di per sé sarebbero dunque in contrasto con i princìpi del D.Lgs. 196/2003.

All'esito di tale revisione possono dunque isolarsi processi che non necessitano di essere condotti facendo uso di dati in forma nominativa. Poiché tuttavia, ai sensi dell'art. 4, c. 1, lett. b), D.Lgs. 196/2003, costituiscono dato personale anche le informazioni riferite a soggetti meramente identificabili e poiché l'identificazione può avvenire anche indirettamente «mediante riferimento a qualsiasi altra informazione», va tenuto conto che un anonimato pressoché assoluto è difficile da conseguirsi nel contesto delle moderne tecnologie di *big data analytics*.[45]

---

of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 3 giugno 2003, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf; Article 29 Data Protection Working Party, Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From «Binding Corporate Rules», 14 aprile 2005, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp107_en.pdf; Article 29 Data Protection Working Party, Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, 14 aprile 2005, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp108_en.pdf. Per un elenco completo dei documenti adottati dall' Article 29 Data Protection Working Party si rinvia al seguente indirizzo: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/tools/index_en.htm.

[43] Cfr. G.M. Riccio, *Gli strumenti alternativi per il trasferimento dei dati personali extra UE (clausole contrattuali standard e binding corporate rules)*, in questo Volume.

[44] Cfr. A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa*, cit., 87 ss.

[45] Cfr. A. Narayanan, J. Huey, E. W. Felten, *A Precautionary Approach to Big Data*

Fermo tale limite, in applicazione del principio di proporzionalità, si può comunque ritenere che ove il processo di re-identificazione richieda risorse sproporzionate e l'aggiramento di divieti di re-identificazione[46] o barriere tecnologiche, il livello di anonimato possa considerarsi sufficiente al fine di escludere i dati in questione dall'ambito di applicazione del D.Lgs. 196/2003. In relazione ai flussi transfrontalieri, dovrebbe tuttavia in questi casi prevedersi uno specifico impegno contrattuale del *data importer* a non procedere all'eventuale re-identificazione dei dati, con conseguente assunzione di responsabilità per sé per gli eventuali *sub-processors*.

Ove invece si sia necessariamente in presenza di dati personali, occorrerà ragionare in termini di adozione delle *standard contractual clauses*. Tali clausole[47] consentono di fornire un livello di tutela - ritenuto ad oggi[48]

Privacy, 2015, http://randomwalker.info/publications/precautionary.pdf; A. Narayanan, E. W. Felten, *No silver bullet: De-identification still doesn't work*, 2014, http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf; P. Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, in *UCLA L. Rev.*, 2010, 57, 1701 ss.; P. Golle, *Revisiting the uniqueness of simple demographics in the US population*, in A. Juels (a cura di), *Proceedings of the 5th ACM workshop on Privacy in electronic society (ACM 2006)*, New York, NY, 2006, 77 ss.; United States General Accounting Office, *Record Linkage and Privacy. Issues in creating New Federal Research and Statistical Information*, 2011, 68 ss., http://www.gao.gov/assets/210/201699.pdf; L. Sweeney, *Simple Demographics Often Identify People Uniquely*, Carnegie Mellon University, 2000, http://dataprivacylab.org/projects/identifiability/paper1.pdf; L. Sweeney, *Foundations of Privacy Protection from a Computer Science Perspective*, in *Proc. Joint Statistical Meeting, AAAS, Indianapolis (2000)*, http://dataprivacylab.org/projects/disclosurecontrol/paper1.pdf.

[46] Cfr. A. Cavoukian, D. Reed, *Big Privacy: Bridging Big Data and the Personal Data Ecosystem through Privacy by Design*, in A. Cavoukian, *Privacy by design. From rhetoric to reality*, 2014, 82 http://www.ipc.on.ca/images/Resources/PbDBook-From-Rhetoric-to-Reality.pdf; Y. Lagos, J. Polonetsky, *Public vs. Nonpublic Data: The Benefits of Administrative Controls*, in *Stan. L. Rev. Online*, 2013 (66), 103 ss.; F. H. Cate, V. Mayer-Schönberger, *Data Use and Impact. Global Workshop*, 2013, 13, http://cacr.iu.edu/sites/cacr.iu.edu/files/Use_Workshop_Report.pdf; Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Business and Policymakers*, 2012, 21, http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[47] Su cui si rinvia a G.M. Riccio, *Gli strumenti alternativi per il trasferimento dei dati personali extra UE (clausole contrattuali standard e binding corporate rules)*, cit.

[48] A seguito dei rilievi mossi dalla Corte di Giustizia non pare improbabile un'eventuale contestazione della validità delle clausole approvate dalle Commissione, ad opera delle autorità garanti nazionali. Contestazione che aprirebbe ad una sospensione dell'operatività delle stesse e, in ultima istanza, ad un'eventuale pronuncia della Corte di Giustizia sulle decisioni adottate dalla Commissione.

adeguato dalla Commissione - mediante accordi pattizi fra *data importer* e *data exporter*. Va però ricordato che, sebbene non richiesto dalla normativa italiana,[49] in diversi stati dell'Unione l'adozione di tali clausole è subordinata alla specifica approvazione dell'autorità garante locale. Questo comporta che una multinazionale potrebbe trovarsi a dover richiedere specifiche autorizzazioni per i flussi transfrontalieri generati da controllate con sede in altri Paesi dell'Unione, salva l'ipotesi di non far confluire tutti i dati in uno stato come l'Italia, ove non è richiesta un'autorizzazione specifica all'uso delle *standard contractual clauses*, e da lì generare un unico flusso verso i Paesi terzi.

Come si vede da questi pochi cenni, anche l'adozione di clausole standard implica comunque una riorganizzazione dei flussi di dati interni alle aziende o, quantomeno, nuovi specifici adempimenti. Adempimenti che non riguardano solo l'eventuale autorizzazione dell'autorità garante, ma anche quanto richiesto dalle *standard contractual clauses* in termini di *audit* e di responsabilità solidale fra *data importer* e *data exporter*.

Due sono però i principali limiti strutturali che si frappongono ad un ampio ricorso alla soluzione in esame. In primo luogo va rilevato come non vi siano clausole *ad hoc* per il trasferimento dati fra un *data processor* stabilito nell'UE ed un *sub-processor* di un Paese terzo, con la conseguenza che occorrerà ricorrere ad una delle seguenti opzioni:[50] l'impiego delle clausole-tipo comunitarie direttamente ad opera del titolare del trattamento (*controller*) mediante un accordo con il *sub-processor*; un mandato da parte del *controller* al *processor* affinché quest'ultimo stipuli in suo nome le clausole-tipo con il *sub-processor*; il ricorso a specifici accordi contrattuali fra le parti, previa autorizzazione dei competenti organi del Paese dell'esportatore.[51] Sebbene questo limite paia dunque superabile, risulta

[49] Cfr. Garante per la protezione dei dati personali, Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso Paesi non appartenenti all'Unione europea, effettuati in conformità alle clausole contrattuali tipo, di cui all'allegato alla decisione della Commissione europea del 5 febbraio 2010, n. 2010/87/UE, 27 maggio 2010, doc. web n. 1728496, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1728496.

[50] Per un maggior dettaglio, cfr. Article 29 Data Protection Working Party, FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, Bruxelles, 12 luglio 2010, 4 ss., in http://ec.europa.eu/justice_-home/fsj/privacy/docs/wpdocs/2010/wp176_en.pdf.

[51] Si rinvia a riguardo alle considerazioni espresse in merito al trattamento dati nel contesto dei servizi di *cloud computing*, ove è più frequente la presenza di un'ampia filiera di

comunque evidente come esso renda l'adozione delle *standard contractual clauses* onerosa.

Il secondo limite, più strettamente correlato al *decisum* della Corte di Giustizia, riguarda le previsioni contenute nella clausola II(c) delle Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers),[52] ai sensi della quale «[The data importer warrants and undertakes that:] It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws».[53] Ne consegue che, sulla base dei rilievi della Corte e delle considerazioni espresse dalla Commissione circa il livello di tutela offerto dalle normative statunitensi,[54] si dovrebbe concludere che la semplice adozione delle *standard contractual clauses* non esima dalla valutazione circa i limiti dell'ordinamento USA, ma anzi implichi la comunicazione di cui alla menzionata clausola. A seguito di tale comunicazione il *data exporter* europeo dovrebbe bloccare il flusso transfrontaliero di dati o quantomeno integrare le clausole con ulteriori e specifiche tutele, in assenza delle quali le clausole in questione potrebbero in concreto non offrire un livello adeguato di protezione.[55]

Va tuttavia rilevato come non paia emergere, a livello generale, l'intenzione delle autorità garanti europee di mettere in dubbio la validità dei

processors e *sub-processors*, in A. Mantelero, Processi di *outsourcing* informatico e *cloud computing*: la gestione dei dati personali ed aziendali, in *Dir. Inf.* 2010, 687 ss.

[52] Cfr. European Commission, 2004/915/EC, Annex, cit. Cfr. anche la clausola 5(a) delle standard contractual clauses di cui all'allegato della decisione European Commission, 2001/497/EC, cit.

[53] Cfr. anche disposizione di analogo tenore contenuta nella clausola 5(b) delle standard contractual clauses di cui all'allegato della decisione European Commission, 2010/87/EU («[The data importer agrees and warrants:] that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract»).

[54] Cfr. *supra* nota 7. [prese di posizione critiche da parte delle istituzioni comunitarie]

[55] Cfr. anche Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein, *Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14*, cit.

trasferimenti effettuati avvalendosi delle *standard contractual clauses,*[56] né tantomeno la Commissione pare orientata in tal senso.[57] Come però riconosciuto dalla Commissione medesima, questo non impedisce a singole autorità garanti di valutare se tali clausole, come anche le *binding corporate rules*, possano considerarsi idonee a fornire un'adeguata protezione con riferimento a casi specifici ed a specifici Paesi terzi.[58]

Se dunque nel breve periodo l'adozione delle *standard contractual clauses* potrebbe costituire una soluzione, in un più ampio arco di tempo l'eventuale contestazione della validità delle stesseo la loro modifica ad opera della Commissione, in conseguenza della decisione che si commenta, potrebbero comportare un esito negativo per le imprese che hanno assunto i maggiori oneri derivanti dall'adozione di tali clausole.

Le medesime considerazioni paiono valide per le *binding corporate rules*, rispetto alle quali occorre poi ricordare come si tratti di una soluzione non adatta a tutte le imprese, in ragione dei costi organizzativi e del tempo necessario per la loro adozione. Se si aggiunge poi che l'approvazione delle *binding corporate rules* ad opera dell'autorità garante preposta richiede

[56] Cfr. Article 29 Data Protection Working Party, *Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)*, cit.

[57] Cfr. European Commission, *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*, COM(2015) 566 final, Brussels, 6 novembre 2015, 5 s., http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf.

[58] Cfr. European Commission, *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*, cit. («in the absence of a Commission finding of adequacy, the responsibility is on controllers to ensure that their data transfers take place with sufficient safeguards in accordance with Article 26(2) of the Directive. This assessment needs to be carried out in the light of all the circumstances surrounding the transfer at issue. In particular, both the SCCs and BCRs provide that if the data importer has reasons to believe that the legislation applicable in the recipient country may prevent it from fulfilling its obligations, it shall promptly inform the data exporter in the EU. In such a situation, it is up to the exporter to consider taking the appropriate measures necessary to ensure the protection of personal data. These may range from technical, organisational, business-model related or legal or measures to the possibility to suspend the data transfer or to terminate the contract. Taking into account all the circumstances of the transfer, data exporters may thus have to put in place additional safeguards to complement those afforded under the applicable legal basis for transfer to meet the requirements of Article 26(2) of the Directive»).

mediamente fra i 12 ed i 18 mesi e si guarda alla prossima applicazione del nuovo regolamento comunitario, anche qui occorre concludere che l'opzione in questione è più consona ad una strategia di lungo periodo.

Soprattutto nel caso di grandi imprese si potrà dunque vagliare quest'ultimo rimedio, che ha il beneficio di legittimare i trattamenti posti all'interno dell'organizzazione, ma si dovrà anche qui tener in conto che trattasi di una soluzione che implica la mappatura e, in molti casi, la riorganizzazione dei flussi di dati intra-gruppo, nonché la definizione di sistemi di monitoraggio successivi all'adozione delle *binding corporate rules*, la definizione di nuovi e specifici ruoli in materia di *data protection* e l'applicazione di un approccio di *privacy by design* ai processi. Un percorso dunque piuttosto oneroso, che può essere intrapreso solo se gode dell'adeguato sostegno dei vertici aziendali.

1.2 (segue). Strategia di lungo periodo e valore competitivo della tutela dei dati personali

Se nel breve periodo permane incertezza e nel medio termine si può ipotizzare l'adozione di soluzioni orientate alla tutela dei dati, ma non senza oneri ed eventuali maggior costi per le imprese, guardando al lungo periodo l'orizzonte pare potersi rasserenare.

In primo luogo, va rilevato come sul lungo periodo l'investimento in tutela dei dati sia destinato a premiare le imprese, quindi anche maggiori oneri ed adempimenti si tradurranno plausibilmente in un vantaggio competitivo.[59]

In secondo luogo, le dinamiche che si sono viste essere alla base dei rapporto fra UE ed USA in materia di trattamento dei dati e che hanno portato all'accordo «Safe Harbour» sono ragionevolmente destinate a trovare compimento. In particolare, sul versante statunitense già da tempo si assiste ad una crescente domanda da parte dei consumatori circa l'innalzamento dei livelli di protezione riconosciuti ai dati personali[60] e, sul fronte delle imprese, v'è una richiesta di standard normativi maggiormente com-

[59] In ragione dell'economia del presente scritto si rinvia a riguardo alle considerazioni espresse in A. Mantelero, *Competitive value of data protection: the impact of data protection regulation on online behaviour, in International Data Privacy Law*, 2013, 3(4), 229 ss.

[60] Cfr. M. Madden, L. Rainie, Americans' Attitudes About Privacy, Security and Surveillance, Pew Research Cente, 20 maggio 2015, http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf.

patibili con quello europeo, tali da evitare uno svantaggio competitivo per le imprese USA.[61]

In quest'ultimo senso vanno le azioni intraprese ad esempio da una grande multinazionale statunitense quale Microsoft concretizzatesi nella causa contro il governo americano a difesa dell'extraterritorialità dei dati contenuti sui propri *server* situati in Europa,[62] iniziativa che ha goduto dell'appoggio di molte imprese del settore ICT.[63] In analoga direzione pare andare il supporto delle grandi imprese statunitensi ai progetti di legislazione federale volti a riformare sia l'attuale sistema di raccolta dati ad opera delle agenzie governative, sia le procedure di *mutual legal assistance*.[64]

Non è dunque un caso che un primo effetto della decisione della corte di Giustizia sia consistito nella ripresa della discussione sul Judicial Redress Act,[65] una proposta bipartisan già approvata a fine ottobre dalla House of Representatives, che riconosce anche ai cittadini europei il diritto di agire

[61] Cfr. D. Kehl, K. Bankston, R. Greene, R. Morgus, *Surveillance Costs. The NSA's Impact on the Economy, Internet Freedom & Cybersecurity*, New America's Open Technology Institute, luglio 2014, https://www.newamerica.org/downloads/Surveilance_Costs_Final.pdf.

[62] Cfr. *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 14-02985, U.S. Court of Appeals for the Second Circuit (Manhattan). Si vedano a riguardo i documenti pubblicati dall'Electronic Frontier Foundation nella pagina dedicate al caso, consultabili al seguente indirizzo: https://www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland. Cfr. anche Center for Democracy & Technology, *Microsoft Ireland Case: Can a US Warrant Compel A US Provider to Disclose Data Stored Abroad?*, 30 giugno 2014, https://cdt.org/insight/microsoft-ireland-case-can-a-us-warrant-compel-a-us-provider-to-disclose-data-stored-abroad/.

[63] Cfr. gli Amicus Brief a support di Microsoft richiamati in Center for Democracy & Technology, *Microsoft Ireland Case: Can a US Warrant Compel A US Provider to Disclose Data Stored Abroad?*, cit.

[64] Cfr. a riguardo A. K. Woods, *Data Beyond Borders: Mutual Legal Assistance in the Internet Era*, Global Network Initiative, gennaio 2015, http://globalnetworkinitiative.org/content/data-beyond-borders-mutual-legal-assistance-internet-era. Cfr. in merito il negoziato EU-USA sul c.d. «umbrella agreement», volto a definire un quadro comune in materia di tutela dei dati personali trattati per finalità giudiziaria, v. a riguardo European Commission, Joint EU-US Statement, Brussels, 13 novembre 2015, http://europa.eu/rapid/press-release_STATEMENT-15-6087_en.htm?locale=en; European Commission, *Questions and Answers on the EU-US data protection «Umbrella agreement»*, Brussels, 8 settembre 2015, http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm.

[65] Cfr. a riguardo E. Kelly, *Congress Moves to Give Europeans Stronger Data Privacy Rights in the U.S.*, in USA TODAY, 10 novembre 2015. http://www.usatoday.com/story/news/2015/11/10/congress-moves-give-europeans-stronger-data-privacy-rights-us/75315662/.

in giudizio di fronte alle corti statunitensi qualora il governo USA abbia avuto illegittimo accesso ai dati degli interessati.[66]

Va poi ricordato che è ancora giacente il Consumer Privacy Bill of Rights,[67] che, benché non riguardi i flussi transfrontalieri, ove si traducesse in una legge federale costituirebbe un indubbio innalzamento del livello di tutela offerto dall'ordinamento statunitense, in grado di facilitare l'affermarsi di una più forte protezione delle informazioni personali in tutti gli ambiti, compreso quello inerente l'attività delle agenzie governative.[68]

Sempre guardando alle possibili iniziative governative, va poi menzionato il negoziato in corso sul Transatlantic Trade and Investment Partnership (TTIP), fin dall'inizio visto anche come un possibile tavolo di discussione per quanto concerne gli scambi di dati. In proposito, è forte nell'Unione europea l'avversione per soluzioni liberistiche in materia di dati personali e per la stessa introduzione del tema fra i capitoli dell'accordo,[69] pare quindi improbabile che si giunga all'adozione di un testo che ricalchi il modello della Trans-Pacific Partnership. Proprio in tale ottica, i rilievi mossi dalla Corte in merito ai poteri della Commissione ed a quelli dei garanti paiono costituire forti limiti ad eventuali scorciatoie negoziali in materia di dati personali perseguibili dalla Commissione.[70]

[66] Cfr. E. Kelly, *Congress Moves to Give Europeans Stronger Data Privacy Rights in the U.S.*, cit. («The legislation would give Europeans the same protections as Americans under the Privacy Act of 1974, which governs the collection, use and dissemination of personally identifiable data contained in records held by the federal government. In addition to being able to sue the U.S. government for wilfully disclosing personal data, Europeans could sue if a federal agency refuses their request to review or amend their records. The legislation also would apply to citizens of other nations designated by the Justice Department»).

[67] Cfr. The White House, *A Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 2012, 47 s., http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[68] Va poi ricordato come la moderna sorveglianza si basi su un modello di partnership pubblico-privato, per cui il rafforzamento della tutela dei dati in mano alle imprese, l'adozione di soluzioni volte alla minimizzazione, cancellazione progressiva ed anonimizzazione dei dati, costituiscono tutti rimedi che indirettamente vengono a circoscrivere l'effetto della sorveglianza attuata dai soggetti pubblici. A. Mantelero, G. Vaciago, Digital investigation, 2015,15, 104 ss.

[69] Cfr. European Parliament, *TTIP: Trade agreements must not undermine EU data protection laws, say Civil Liberties MEPs*, 31 marzo 2015, http://www.europarl.europa.eu/pdfs/news/expert/infopress/20150330IPR39308/20150330IPR39308_en.pdf.

[70] Cfr. a riguardo la posizione espressa nel 2013 dalla Commissione Europea in European Commission, *Communication from the Commission to the European Parliament and the Council. Rebuilding Trust in EU-US Data Flows*, COM(2013) 846 final, Brussels, cit. («data protection standards will not be negotiated within the Transatlantic Trade and

Al contrario, la percezione non solo del valore economico dei dati personali, ma anche del valore competitivo della tutela delle informazioni personali, nonché le esigenze di interoperabilità dei sistemi, potrebbero indurre la controparte statunitense a perseguire con maggior decisione la strada delle riforme di cui si è detto. Questo al fine di conseguire non solo un nuovo accordo bilaterale che si sostituisca al «Safe Harbour», ma anche di orientarsi verso una più matura strategia in materia commerciale con riguardo ai dati, nel contesto dei rapporti atlantici.

Guardando, infine, alle azioni che possono essere intraprese dalle singole imprese, va segnalata la scelta della società Microsoft di adottare un modello non incentrato sulla mera delocalizzazione dei *server* nell'Unione europea, già operata da molte imprese USA (ma finora inefficace nel contrastare le norme statunitensi in materia di accesso ai dati da parte delle agenzie governative),[71] bensì imperniato su una 'delocalizzazione' del controllo. L'ipotesi allo studio pare infatti riguardare l'adozione di un modello definito di «data trustee» in cui l'impresa statunitense affida il controllo dei dati ad un *trustee* europeo,[72] che quindi opererà nell'interesse della prima, ma sarà un soggetto giuridico distinto e di diritto comunitario. Sebbene manchino sufficienti dettagli per una piena valutazione del modello, quest'ultimo, pur non facendo venir meno i flussi transfrontalieri verso gli USA, crea uno schermo giuridico all'operatività delle norme statunitensi in materia di accesso ai dati da parte delle agenzie governative,[73] operatività che costituisce la maggiore delle criticità rilevate dalla Corte di Giustizia nel caso Schrems.

Investment Partnership, which will fully respect the data protection rules»).

[71] Cfr. *supra* nota 62.

[72] Cfr. Microsoft Europe, Microsoft Announces Plans to Offer Cloud Services from German Datacenters, 11 novembre 2015, http://www.prnewswire.co.uk/news-releases/microsoft-announces-plans-to-offer-cloud-services-from-german-datacenters-545594412.html («These new cloud services will be a first of their kind innovation from a global hyperscale cloud provider, in that access to customer data stored in these new datacenters will be under the control of T-Systems, a subsidiary of Deutsche Telekom, an independent German company acting as a data trustee. Microsoft will not be able to access this data without the permission of customers or the data trustee, and if permission is granted by the data trustee, will only do so under its supervision»).

[73] Quest'ultime dovranno infatti indirizzare le proprie richieste verso una società europea e dunque avvalersi delle procedure di Mutual Legal Assistance.

2. Prime conclusioni

Al termine della disamina dei diversi scenari che la decisione della Corte di Giustizia apre con riguardo al trattamento dei dati personali posto in essere dalle imprese, non pare necessario ricapitolare quanto accennato in merito all'opportunità di una diversificazione degli approcci, dovuta sia alla tipologia dei soggetti imprenditoriali coinvolti sia alla natura dei trattamenti dati realizzati,nonché all'orizzonte temporale. Merita invece guardare oltre alle mere relazioni atlantiche e chiedersi quale sia il futuro del modello europeo di *data protection*. Un modello apparentemente vincente, capace di imporsi in molti Paesi e di condizionare l'economia globale dei dati.

Si ha tuttavia la sensazione che, portando a compimento le conseguenze desumibili dai princìpi enunciati dalla Corte, il modello si riveli più debole di quanto ora appare, incapace in concreto di difendere nella sostanza i 'confini' del proprio standard di tutela in un mondo globale ed interconnesso. Ancora forte in termini di spinta propulsiva ed in grado di innalzare il livello di protezione esistente nei Paesi terzi, ma, nel contempo, assai più fragile nella sostanza.

Accordi quali il «Safe Harbour» e rimedi quali le *standard contractual clauses*, della cui concreta operatività ben poco ci si cura, finiscono per offrire spesso più una tutela formale che sostanziale. Così come, anche all'interno dei confini dell'Unione, non mancano i tanti contrasti fra la declamazione di un elevato livello di protezione e la prassi che molte volte riduce la tutela dei dati ad una mera serie di adempimenti formali, senza poi che le informazioni beneficino di una effettiva maggior protezione.

In tale scenario la nuova proposta di regolamento comunitario apporta alcune luci (in particolare va valutato positivamente il rafforzamento dell'approccio preventivo incentrato sull'analisi del rischio), ma anch'essa, da sola, non pare riuscire a scongiurare lo iato fra *law in books* e *law in action*. Per questo, forse occorre investire maggiormente nella promozione della cultura della *privacy*. In tale ottica, l'accademia, pur nel suo raggio di azione, è chiamata ad assumere un ruolo decisivo, mettendo chiaramente in luce come il diritto del XXI secolo ed i diritti di domani si muovano soprattutto su questi terreni.[74]

[74] Cfr. a riguardo S. Rodotà, *Verso una Costituzione di Internet*, estratto dall'intervento tenuto al Convegno «Verso una Costituzione per Internet?», Roma, 16 giugno 2015, dalle ore 10, presso la Sala del Mappamondo di Palazzo Montecitorio, http://camera.civi.ci/discussion/proposals/billofrights; Camera dei deputati XVII Legislatura, Commissione per i Diritti e i Doveri in Internet, *Dichiarazione dei Diritti in*

3. «Privacy Shield». Quasi un epilogo[75]

Quanto ipotizzato nelle pagine che precedono[76] ha trovato conferma negli eventi successivi, in particolare nella nuova proposta di accordo bilaterale fra Unione Europea e Stati Uniti, denominata «Privacy Shield», e nelle reazioni che ne sono scaturite.

Nello specifico, il nuovo accordo non pare risolutivo rispetto alle criticità emerse con riguardo al previgente «Safe Harbour» ed ai rilievi formulati dalla Corte di Giustizia dell'Unione Europea nel caso Schrems. Come ipotizzato, le ragioni economico-politiche, cui si è accennato nei paragrafi che precedono, hanno indotto la Commissione Europea e le controparti statunitensi ad una rapida rinegoziazione. Quest'ultima è però avvenuta senza il coinvolgimento diretto delle autorità garanti. In questo la Commissione ha esercitato le prerogative ad essa riconosciute, ma così facendo ha marginalizzato la voce critica di tali autorità; le stesse cui compete, attraverso l'Article 29 Data Protection Working Party, il parere ad uso della Commissione sul livello di tutela offerto dai Paesi terzi,[77] nonché l'eventuale accoglimento dei ricorsi degli interessati che lamentino un inadeguato livello di protezione dei propri dati trasferiti al di fuori dei confini dell'Unione.[78]

Il diverso orientamento che è parso delinearsi con riferimento alle posizioni (più favorevoli ad un accordo di compromesso) della Commissione

Internet, 28 luglio 2015, http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/TESTO_ITALIANO_DEFINITVO_2015.pdf; L. Gill, D. Redeker, U. Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, 9 novembre 2015, Berkman Center Research Publication No. 2015-15, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2687120.

[75] Il presente paragrafo è stato aggiunto in sede di revisione delle bozze onde dar conto dei più recenti sviluppi della materia, consistenti sia nella presentazione della bozza del nuovo accordo fra Unione Europea e Stati Uniti sui flussi transfrontalieri, denominato Privacy Shield, sia nell'approvazione della General Data Protection Regulation. Con riguardo al nuovo accordo denominato «Privacy Shield» cfr. Commissione europea, comunicato stampa del 29 febbraio 2016, disponibile al seguente indirizzo: http://europa.eu/rapid/press-release_IP-16-433_it.htm (consultato in data 1 marzo 2016); in merito al nuovo regolamento sui dati personali, cfr. invece European Commission, *Joint Statement on the final adoption of the new EU rules for personal data protection*, Brussels, 14 aprile 2016, disponibile al seguente indirizzo: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm (consultato in data 16 aprile 2016).

[76] Cfr. *supra* §2.1.

[77] Cfr. art. 30 (1) (b), dir. 96/46/CE.

[78] Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit.

e quelle (più rigorose) delle autorità garanti, in seguito alla decisione della Corte di Giustizia,[79] ha dunque trovato conferma nelle settimane successive all'accordo sul «Privacy Shield», quando ai toni trionfalistici della Commissione ha risposto un diverso atteggiamento dell'Article 29 Data Protection Working Party. Quest'ultimo, pur lodando i miglioramenti conseguiti con il nuovo accordo, non ha mancato di metterne in luce le significative criticità.

Per queste ragioni, il testo attualmente concordato fra E.U. ed USA non può considerarsi come l'epilogo della vicenda in esame. Diverse e fondatamente argomentate sono infatti le osservazioni critiche espresse dai garanti europei. Nel contempo, l'approvazione del nuovo regolamento sui dati personali (General Data Protection Regulation) implica necessariamente che 'il livello adeguato di protezione' vada rivalutato alla luce dell'innalzamento dello standard di protezione offerto dal nuovo testo normativo.[80]

Critiche sono state anche espresse dalle associazioni a tutela della *privacy*,[81] posto che gli aspetti maggiormente controversi riguardanti la proporzionalità del trattamento dati realizzato dalle agenzie governative statunitensi paiono essere ancora irrisolti.[82] In questo senso, l'accordo è

[79] Cfr. anche Article 29 Data Protection Working Party, *Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)*, Brussels, 16 ottobre 2015, disponibile al seguente indirizzo: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf (consultato in data 10 novembre 2015); European Commission, *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*, Brussels, 6 novembre 2015, disponibile al seguente indirizzo: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf (consultato in data 10 novembre 2015).

[80] Cfr. in tal senso Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU – U.S. «Privacy Shield» draft adequacy decision, Brussels*, 13 aprile 2016, disponibile al seguente indirizzo: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (consultato in data 14 aprile 2016).

[81] Cfr. la lettera inviata ai presidenti dell'Article 29 Working Party e del Committee on Civil Liberties, Justice, and Home Affairs del Parlamento Europeo, firmata da 27 delle associazioni di difesa della privacy maggiormente rappresentative in Europa e negli Stati Uniti, disponibile al seguente indirizzo: https://edri.org/transatlantic-coalition-of-civil-society-groups-privacy-shield-is-not-enough-renogitation-is-needed/ (consultato in data 18 marzo 2016).

[82] Cfr. in tal senso anche Article 29 Data Protection Working Party, *Opinion*

per lo più un compromesso volto a far fronte al vuoto creatosi in seguito all'annullamento della decisione della Commissione sull'adeguatezza del programma «Safe Harbour».

Guardando ai contenuti, l'accordo può essere diviso in due parti: una prima costituita dai Privacy Principles (allegato II) ed una seconda composta dalle dichiarazioni ed impegni adottati rispettivamente dal Governo statunitense e dai dipartimenti del commercio e della giustizia USA (allegati I e da III a VII).

Nella parte relativa ai Privacy Principles, l'accordo si mostra in grado di fornire un livello di protezione di maggior dettaglio e più elevato rispetto a quanto garantito in precedenza dal «Safe Harbour». In tal senso, aspetti positivi sono ravvisabili nell'adozione di un approccio incentrato sul rischio, in un innalzamento del livello di responsabilità dei soggetti che trattano i dati, nella definizione di procedure specifiche per i reclami inerenti ai trattamenti illegittimi, che possono essere presentati sia dai cittadini europei che dalle autorità garanti dell'Unione, ed infine nell'adozione di un sistema di monitoraggio attivo e d'ufficio da parte delle autorità statunitensi. Quest'ultime saranno dunque chiamate a verificare l'effettiva osservanza di quanto previsto dal «Privacy Shield» da parte delle imprese che vi aderiscono.

Sebbene permangano ancora zone grigie, per quanto concerne ad esempio il modello opt-out per i dati non sensibili o la lunghezza delle procedure di reclamo, i principi dettati dal nuovo accordo paiono ridurre il divario esistente fra gli standard di tutela esistenti negli Stati Uniti e nell'Unione Europea. Si tratta tuttavia di un risultato provvisorio, poiché il nuovo regolamento europeo (General Data Protection Regulation) introduce diversi mutamenti ed adotta un approccio più orientato all'analisi del rischio, aspetti che probabilmente finiranno per creare nuovamente un divario sostanziale tra le garanzie previste dalla normativa comunitaria e la protezione fornita dal «Privacy Shield».[83]

Per quanto riguarda invece la seconda parte dell'accordo (allegati I e da III a VII), essa concerne principalmente l'accesso alle informazioni e l'utilizzo delle stesse da parte delle autorità statunitensi nel caso di dati

01/2016 on the EU – U.S. «Privacy Shield» draft adequacy decision, cit.

[83] Cfr. in tal senso, Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU – U.S. «Privacy Shield» draft adequacy decision*, cit., 3 («The WP29 considers a review [of the «Privacy Shield» adequacy decision] must be undertaken shortly after the entry into application of the General Data Protection Regulation, in order to ensure the higher level of data protection offered by the Regulation is followed in the adequacy decision and its annexes»).

trasferiti in ottemperanza al «Privacy Shield». Qui il testo si fa necessariamente più vago, fondandosi su assicurazioni di natura politica («il governo degli Stati Uniti ha assicurato alla Commissione che qualsiasi attività di raccolta di massa per quanto riguarda le comunicazioni via Internet che la Comunità intelligence statunitense compie attraverso i segnali di intelligence operano su una piccola parte di Internet») o rinviando a future implementazioni, quali ad esempio l'istituzione dell'Ombudsperson, che dovrà farsi carico di ricevere e rispondere ai ricorsi dei singoli che lamentino una violazione dei diritti sui dati connessa alle attività dei servizi di intelligence statunitensi.

In assenza tuttavia di cambiamenti significativi con riguardo alle pratiche di sorveglianza d'Oltreoceano ed alle norme che le regolano, pare prevalere un certo scetticismo circa il reale impatto di questa parte del nuovo accordo. In tal senso sembrano essere orientati anche i garanti europei, che hanno mosso diverse e decisive critiche al nuovo testo.

In primo luogo, i garanti sottolineano la mancanza di chiarezza espositiva, dovuta sia alla divisone in più parti dell'accordo, di cui si è detto e tale da rendere difficile una lettura organica del testo, sia alla scarsa chiarezza lessicale del testo. In secondo luogo, alcuni dei principi cardini della normativa europea non risultano essere recepiti dall'accordo (e.g. data retention principle) o sono recepiti in maniera poco lineare (e.g. purpose limitation principle). Mancano poi sufficienti garanzie circa l'eventuale successivo trasferimento dei dati inviati negli USA verso ulteriori Paesi. Lo stesso esercizio dei diritti da parte dei cittadini europei nei confronti dei soggetti che trattano i dati che li riguardano negli USA appare poi troppo complesso e di difficile praticabilità per gli interessati, tanto da far dubitare della reale efficacia del rimedio stesso.

Infine, se da un lato i garanti danno atto che il nuovo accordo affronta la questione del trattamento dati posto in essere dalle agenzie governative statunitensi, rilevano però come una raccolta massiva ed indiscriminata di dati ad opera di tali soggetti non sia esclusa e come la figura di garanzia prevista dal «Privacy Shield» (l'Ombudsperson) mostri limiti intriseci dovuti alla carenza di indipendenza e mancanza di poteri e rimedi adeguati.

La critica più incisiva pare poi quella secondo cui il testo del nuovo accordo «does not include a comprehensive assessment of the domestic law and the international commitments of the U.S. in the form of an adequacy report, as has been the regular practice in the past in similar procedures and in line with Article 25 of the Directive». Sembra quindi

essere stata disattesa proprio la richiesta implicita nella decisione sul caso Schrems, in cui la Corte di Giustizia aveva lamentato la mancanza di «sufficient findings regarding the measures by which the United States ensures an adequate level of protection, within the meaning of Article 25(6) of that directive, by reason of its domestic law or its international commitments».[84]

A sei mesi dalla decisione della Corte di Giustizia il quadro giuridico inerente i flussi transfrontalieri di dati fra Unione Europea e Stati Uniti è dunque ancora tutt'altro che definito, lasciando la prassi concreta del trasferimento dati in una sorta di limbo destinato a durare sino a quando qualche autorità garante non deciderà di intervenire rispetto all'irregolarità che connota larga parte della situazione attuale, in cui enormi quantità di dati attraversano l'Atlantico prive di adeguata legittimazione giuridica.[85]

Se a questo si aggiunge l'effetto dell'approvazione del nuovo regolamento dell'Unione sulla tutela dei dati personali e la necessaria revisione del «Privacy Shield» che ne dovrebbe conseguire,[86] si deve concludere che le strategie delineate nei precedenti paragrafi paiono rimanere valide. In tale ottica le imprese con maggior colpevolezza dovrebbero valutare l'opportunità di orientarsi verso soluzioni differenti da quelle basate unicamente sugli accordi bilaterali fra Unione Europea e Stati Uniti. Certamente si tratta di alternative più gravose,[87] ma meno suscettibili di subire i contraccolpi del delicato e variabile equilibrio di interessi che caratterizza l'economia ed il controllo dei dati, sempre più al centro dei dialoghi atlantici.

In un'ottica più ampia, l'effetto della decisione sul caso *Schrems* e la ri-definizione in corso dell'accordo bilaterale sui flussi di dati fra U.E. ed USA, così come le disposizioni contenute nel nuovo regolamento comunitario, inducono a guardare oltre al caso concreto dei rapporti atlantici per domandarsi se il modello europeo in materia di tutela dei dati dei cittadini sia davvero vincente al di fuori dei confini dell'Unione, come sembra apparire a prima vista.

[84] Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit., punto 83.
[85] Si ha avuto recente notizia di un procedimento aperto dall'autorità per la protezione dei dati personali di Amburgo; cfr. D. Windelband, *«Safe Harbour» – Hamburger Aufsichtsbehörde leitet Ordnungswidrigkeitenverfahren ein, in Datenschutz Notizen*, disponibile al seguente indirizzo: https://www.datenschutz-notizen.de/safe-harbor-hamburger-aufsichtsbehoerde-leitet-ordnungswidrigkeitsverfahren-ein-5614585/ (consultato in data 29 aprile 2016).
[86] Cfr. *supra* nota 82.
[87] Cfr. *supra* § 1.1.

Rinviando ad altra sede per più ampie considerazioni a riguardo,[88] va qui osservato come i diversi strumenti disponibili, siano essi accordi *ad hoc* come il «Privacy Shield» o decisioni sull'adeguatezza della normativa dei Paesi terzi o clausole standard, mostrano un'intrinseca debolezza dovuta alla mancanza o carenza di un'effettiva attività di monitoraggio costante dei livelli di protezione concretamente assicurati da tali strumenti. Che si tratti del rispetto delle clausole standard da parte dei contraenti o della prassi applicativa delle leggi straniere ovvero del rispetto dei 'programmi' quali il «Safe Harbour» o il «Privacy Shield» da parte dei soggetti che vi aderiscono, il rischio principale pare essere il divario tra il modello come definito dalla normativa e la prassi concreta, in termini di effettiva tutela dei diritti e delle libertà fondamentali.

In quest'ottica, si ha il sentore che le disposizioni dell'Unione in materia di flussi di dati finiscano per assumere una natura che è sovente declamatoria, la cui effettiva ragion d'essere risiede in una più ampia e complessa operazione politica. Un'operazione che può essere compresa solo guardando alla dimensione multi-stakeholder inerente la *data protection* globale, che coinvolge diverse aree economiche (USA, UE, Cina, ecc) e diverse organizzazioni (COE, APEC, OCSE, Nazioni Unite). Da questo punto di vista, le barriere legali costruite intorno ai dati europei, con i loro effetti sui flussi internazionali di informazioni, sembrano essere uno strumento per rafforzare la *leadership* dell'Unione nell'intento di definire le future linee globali in materia di protezione dei dati, piuttosto che una reale garanzia di un più elevato ed efficace livello di protezione dei dati trasferiti verso Paesi terzi. È infatti sullo scacchiere globale che si gioca la vera partita inerente i dati personali, una partita che non riguarda solo il rispetto dei diritti fondamentali, ma anche e sempre più gli assetti economici e politici.

[88] Cfr. A. Mantelero, *From Safe Harbour to Privacy Shield. The 'medieval' sovereignty on personal data, in Contratto e Impr./Europa*, 2016, in corso di pubblicazione.

Abstract

The Safe Harbour agreement was the result of an economic and political compromise between the European Union and the United States in the field of data protection, where the European regulatory model has demonstrated its influence in an interdependent world. The ECJ judgement has put an end to this compromise.

Against this background, the author points out the different solutions that private companies may adopt in the short-, medium- and long-term. In this light, the article considers the chance of reaching a new international bilateral agreement in short time and the limits posed by the ECJ decision to this potential agreement.

Focusing on the medium-term scenario, the author takes into account the impact of the Schrems case on the different legal alternatives for data transfer (data subject's consent, standard contractual clauses, and binding corporate rules) and discusses the consequences of this judgement on business strategies.

In the long-term scenario, a more optimistic outlook is possible, given the increasing demand for data protection coming from U.S. companies and society at large, as demonstrated by the support provided the U.S. business community to new regulatory initiatives and by the In re Microsoft Corp. *case.*