Giovanni Maria Riccio

Model Contract Clauses *e* Corporate Binding Rules*: valide alternative al* Safe Harbor Agreement*?*

Sommario: Introduzione. – 1. Scambi di dati tra Europa e Stati Uniti e impatto economico della decisione. – 2. Il complesso rapporto tra Europa e Stati Uniti su tutela dei dati personali ed esigenze di sicurezza. – 3. *Corporate Binding Rules*. – 4. *Model Contract Clauses*. – 5. L'immodificabilità delle clausole e la soluzione inglese. – 6. Rapporti tra importatore ed esportatore. – Conclusioni.

Introduzione

La decisione della Corte di Giustizia del 6 ottobre 2015, che ha invalidato gli accordi cc.dd. *safe harbor* (2000/520/EC), si presta a molteplici letture. È indiscutibile, però, che rapportarsi a tale pronuncia sulla scorta della mera analisi giuridica rischia di offrire uno scenario parziale, senza dare compiutamente atto delle complesse e intricate vicende che hanno accompagnato prima l'emanazione e poi l'invalidazione di tali accordi. Accordi, pare opportuno ricordarlo, che erano in corso di revisione e che, al momento della decisione dei giudici comunitari, stavano evidenziando una lettura della tematica differente tra le istituzioni europee e quelle statunitensi.

Prima di addentrarci nell'analisi di tali aspetti, alcuni dei quali saranno solo abbozzati in tale sede, considerando che verranno affrontati da altri saggi pubblicati nel presente numero monografico, giova ripercorrere brevemente la funzione di tali accordi nel contesto normativo del trasferimento dei dati personali al di fuori dello spazio europeo.

È noto che l'art. 25 della direttiva n. 46/95/CE prevede un generale divieto di trasferire dati personali al di fuori dell'Unione europea.

Questa regola ammette, però, una serie di eccezioni: il trasferimento è consentito nel caso in cui vi sia il consenso della persona cui i dati personali si riferiscono oppure avvenga in esecuzione di misure contrattuali o precontrattuali o, ancora, per rispondere ad un interesse pubblico; in

presenza di strumenti negoziali, validati dalla Commissione europea, che offrano garanzie di sicurezza; infine, in caso di decisioni di adeguatezza, oppure decisioni della Commissione europea che attestino che un determinato Paese, non appartenente all'Unione europea o allo Spazio economico europeo, assicuri un livello di protezione 'adeguato' ossia sia dotato di misure legislative, nonché tecniche e di sicurezza, che offrano un grado di tutela dei dati personali conforme agli standard comunitari[1].

Tra le decisioni di adeguatezza – che hanno interessato, tra gli altri, Israele, Svizzera, Australia e Canada – la più nota è quella del 26 luglio 2000 tra Unione europea e Stati Uniti, annullata dalla sentenza oggetto del presente scritto e sostituita, nel febbraio del 2016, dai nuovi accordi, denominati *EU-US Privacy Shield*.

Le ipotesi, pertanto, in cui sussiste la legittimazione al trasferimento dei dati personali all'estero possono essere riassunte in due macroaree: una prima ipotesi in cui la legittimazione discende da un'intesa tra istituzioni pubbliche (la Commissione europea e singoli Stati terzi, non appartenenti all'Unione europea); l'altra ipotesi che trova fonte, invece, nell'autonomia privata, seppur integrata dalle prescrizioni legislative.

All'interno di questa seconda macroarea occorre poi distinguere l'ipotesi in cui sia lo stesso soggetto interessato a prestare il proprio consenso, *in maniera inequivocabile* al trasferimento del dato (art. 26, par. 1, lett. *a)* della direttiva), da quella in cui sia stata la Commissione europea ad approvare gli accordi interni alle imprese (nel caso delle *corporate binding rules*) o, in alternativa, a dettare le clausole da recepire nei contratti di esportazione dei dati personali (nel caso delle *model contract clauses*).

1. Scambi di dati tra Europa e Stati Uniti e impatto economico della decisione

In via preliminare, ancor prima di occuparci di tali strumenti alternativi agli accordi di adeguatezza, occorre però esaminare alcuni profili che,

[1] G. Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna-Roma, 2012, p. 283, sottolinea correttamente che la legge italiana ha invertito l'approccio della direttiva comunitaria. Difatti, «*la legge italiana vieta all'art. 45 il trasferimento all'estero se l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato e lo consente se ricorrono alcune specifiche circostanze individuate negli artt. 43 e 44 del Codice*», *la direttiva, invece,* «*dispone che i dati personali possono essere trasferiti dall'Europa verso Paesi extraeuropei, se i Paesi di destinazione garantiscono un adeguato livello di sicurezza*».

sebbene alieni dalla stretta analisi giuridica, consentono di comprendere appieno le sfaccettature intricate della fattispecie in esame.

Difatti, sebbene la sentenza della Corte di Giustizia abbia ricevuto apprezzamenti da più parti, non da ultimo dal nostro Garante per la protezione dei dati personali[2], che ha sottolineato l'importanza del rispetto dei diritti dei cittadini anche al di fuori dei confini comunitari, si è al cospetto di opinioni che, seppur astrattamente condivisibili, fotografano solo una faccia di un prisma molto più complesso.

Non può essere sottaciuto, infatti, l'impatto economico e politico della sentenza Schrems.

Non si tratta di una sentenza che colpisce Facebook, Google o altri 'colossi' della *new economy*, come semplicisticamente si è detto: sono oltre quattromila le imprese europee e statunitensi che hanno beneficiato dei principi di *Safe Harbor* e, di queste, circa il 60% sono piccole e medie imprese, incluse numerose start-up. Allo stesso modo, non deve dimenticarsi come l'utilizzo della rete internet – che ha catalizzato l'allarme associato al trasferimento dei dati – abbia incrementato fortemente le esportazioni da parte delle imprese medie e piccole, che hanno sfruttato le opportunità date dalla possibilità di offrire a costi contenuti i propri prodotti al di fuori dei confini nazionali[3].

Le relazioni commerciali tra imprese statunitensi ed europee sono le più importanti del mondo, in termini numerici e di fatturato: basti pensare che 61% delle importazioni statunitensi proviene da scambi commerciali con imprese europee e il 33% delle importazioni comunitarie proviene dagli Stati Uniti[4]. Sono dati destinati a crescere e che dipendono anche dall'accresciuta fiducia e dimestichezza degli utenti con gli acquisti on-line[5] e dalla penetrazione di internet nella popolazione, che negli Stati

[2] Garante per la protezione dei dati personali, *Facebook: dichiarazione di Antonello Soro sulla sentenza della Corte di Giustizia Europea*, 6 ottobre 2015, Doc. web 4308245.

[3] Al riguardo, è interessante la lettura del report pubblicato da eBay, la più grande piattaforma di aste on-line e uno dei maggiori operatori di e-commerce, secondo cui il 95% delle PMI statunitensi che utilizzano i propri servizi ha esportato i prodotti commercializzati, a fronte di una percentuale pari al 5% delle imprese che non operano *on-line*. Allo stesso modo, se si comparano le imprese che continuano ad esportare a tre anni dalla prima transazione, si registra che il 75% di queste operano *on-line*, mentre solo 15% delle PMI che non utilizzano internet riesce a mantenere le esportazioni nel medesimo arco temporale, cfr. eBay, 2015 *US Small Business Global Growth Report*, 2015.

[4] Cfr. D.S. Hamilton – J.P. Quinlan, *The Transatlantic Economy 2014*, Vol. 1, 2014. Nel 2014, il valore delle esportazioni statunitensi verso l'Unione Europea è stato di oltre 219 miliardi di dollari; le importazioni dall'Europa pari a 169 miliardi di dollari.

[5] Dal 2011 al 2013, l'e-commerce negli Stati Uniti è cresciuto da $ 13.630.000.000

Uniti ha raggiunto l'83% e in Europa oscilla dal 90% del Regno Unito al 60% dell'Italia, a fronte di una media mondiale pari ad appena il 32%[6].

Come è facile immaginare, la maggiore diffusione di internet si traduce anche in un aumento dei dati[7], non necessariamente di natura personale, scambiati per mezzo delle infrastrutture (reti terresti o cavi sottomarini): anche in questo caso, l'esame del flusso dei dati evidenzia che la maggiore mole di trasferimenti avviene tra Europa e Stati Uniti[8].

Peraltro, in molti casi, il transito dei dati è solo temporaneo e dipende dalla localizzazione dei sistemi informatici adoperati; in altri casi, invece,

a $ 42.130.000.000 e dovrebbe raggiungere $ 133.000.000.000 di fatturato entro il 2018, cfr. Statista Dossier, *Global Internet Usage* 2014, 47. Cfr. anche J.F. Gonzales – J. Bradford – K. Yunhee – K.N. Hildegunn, *«Globalisation of Services and Jobs»*, in *Policy Priorities for International Trade and Jobs* (OECD 2012), 186.

[6] Sul punto si rinvia a J.P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment, Brookings Working Paper* 79, October 2014, 5.

[7] Cfr., al riguardo, il *Considerando 4* della Proposta di Regolamento Generale sulla tutela dei dati personali: «The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows. The exchange of data between public and private actors, including individuals, associations and undertakings across the Union has increased», nonché il *Considerando 5*: «Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data» e il *Considerando 78*: «Cross-border flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international co- operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer may only take place if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller or processor».

[8] cfr. J.P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment*, cit., cfr. in particolare la mappa pubblicata a pag. 6, dove si rappresenta che lo scambio dei dati tra Europa e Stati Uniti è pari al doppio di quelli che avvengono tra Stati Uniti e Cina.

il trasferimento dei dati è funzionale solo a ragioni di sicurezza (si pensi, ad esempio, alla duplicazione dei dati e all'utilizzo di server in diversi continenti, al fine di prevenire i rischi connessi alla perdita o alla distruzione dei dati personali). A riprova di quanto si sostiene, basti riflettere sui servizi di *cloud*, nei quali il trasferimento dei dati, caricati dagli utenti sulla piattaforma ai fini della conservazione o della condivisione degli stessi, rappresenta il corollario del servizio principale offerto dalle imprese del settore. Servizi che, è opportuno rimarcarlo, si riverberano anche sulla produttività dei lavoratori e sull'efficienza dei servizi forniti dalle imprese[9].

Alla luce di tali dati, pare possibile concludere (ma trattasi di conclusione ovvia) che il flusso transfrontaliero dei dati non può essere impedito. Ciò determinerebbe la paralisi per molte imprese, tacendo il potenziale isolamento commerciale per l'Europa: una ricerca del 2013 di *Syntech Numérique* dimostra, con chiarezza, che l'interruzione del flusso dei dati transfrontalieri porterebbe alla riduzione del PIL dell'Unione europea del 1,3% e un'emorragia nelle esportazioni dei servizi forniti dall'Europa verso gli Stati Uniti, che diminuirebbero del 6,7%. Il punto, quindi, è che le imprese che intendono (o che sono costrette) ad esportare dati personali sono indotte a ripiegare, sino alla nuova decisione di adeguatezza, sulle clausole contrattuali standard – unico strumento 'sopravvissuto' al crollo del *safe harbor* –, il cui costo verrà sopportato da tutti i soggetti interessati, con un impatto differente su piccole e grandi imprese.

In tale ottica, del resto, pare possa essere spiegato anche il motivo che ha indotto le autorità comunitarie e statunitensi ad accelerare il processo di revisione – seppur per *key-point* – degli accordi e, quindi, giustificata la fretta che ha guidato alla prima bozza del *Privacy Shield* e all'adesione, probabilmente non del tutto convinta, che gli Stati Uniti hanno prestato a questo 'scudo' normativo.

[9] M. Falk – E. Hagsten, *E-Commerce Trends and Impacts Across Europe*, UNCTAD Discussion Paper No. 220, March 2015, UNCTAD/OSG/DP/2015/2, 2015; United States International Trade Commission, *Digital Trade in the U.S. and Global Economies*, Part 2 Pub. 4485 Investigation No. 332-540, 2014, 71.

2. Il complesso rapporto tra Europa e Stati Uniti su tutela dei dati personali ed esigenze di sicurezza

Si è detto in apertura che la sentenza Schrems non può essere incasellata in un'unica lettura. Sarebbe, quindi, un errore (metodologico ed ermeneutico) valutare la fondatezza della sentenza stessa alla luce della mera ripercussione negativa che essa produce sul piano economico.

Il tema, difatti, è complesso e non può essere circoscritto a una visione semplicistica, che tenderebbe a legittimare soluzioni che siano pensate nell'interesse esclusivo degli operatori economici. Il conflitto tra diritti fondamentali – quello delle imprese, da un lato, e quello dei cittadini, dall'altro – allo stesso modo, non può essere ingabbiato in una prospettiva statica, finalizzata ad evidenziare la supremazia di un diritto su di un altro: è evidente che quelli connessi alla tutela dei dati personali dei singoli sono costi sociali che le imprese devono prevedere, così come, in passato, hanno considerato, ad esempio, i costi per la sicurezza sociale dei lavoratori[10]. Sarebbe banalizzante, quindi, demarcare i confini della discussione nel rapporto tra costo di impresa e sicurezza dei dati dei cittadini.

Analogamente, la natura *lato sensu* politica della decisione della Corte di Giustizia non è sfuggita ai primi commentatori[11].

Innanzi tutto, come si accennava, la protezione dei dati personali – dopo l'approvazione Carta di Nizza – ha assunto un valore di rango costituzionale e, in tale processo di 'costituzionalizzazione', la Corte di Giustizia, nei casi *Digital Ireland*[12], *Google Spain*[13] o ora in *Schrems*, sta

[10] K. Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, *Stan. Tech. L. Rev.* 1 (2000); J.E. Cohen, *What Privacy is For?*, 126 *Harv. L. Rev.* 1904 (2003). Un recente studio ha analizzato (criticamente) l'aumento dei costi per le imprese che potrebbero scaturire a seguito dell'approvazione del Regolamento generale in materia di dati personali: L. Christensen – A. Colciago – F. Etro – G. Rafert, *The Impact of the Data Protection Legislative Framework in the E.U.*, Intertic Policy Paper, 2013.

[11] Cfr. L. Bolognini, *Una sentenza politica che non stupisce*, in *Formiche*, novembre 2015, 50; M. Mensi, *Il vero sconfitto è la Commissione europea*, *ivi*, 52; V. Zeno-Zencovich, *Serve un approccio meno ideologico*, *ivi*, 56.

[12] Corte di giustizia, 8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications,* cause riunite C-293/12 e C-594/12, in *Nuova giur. civ. comm.,* 2014, I, 1044, con nota di C.M. Cascione, *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione* data retention *della Corte di giustizia e gli echi del datagate*, ma sul tema, in generale, v., tra gli altri, T. Konstadinides, *Destroying Democracy on the Ground of Defending It? The Data Retention Directive, the Surveillance State and Our Constitutional Ecosystem*, in *Eur. L. Rev.*, 2011, 722.

[13] Corte di giustizia, 13 maggio 2014, *Google Spain SL e Google Inc. c. Agencia Española*

giocando un ruolo fondamentale nel progressivo ampliamento dei margini di tutela riconosciuti ai cittadini comunitari e sulla reinterpretazione della normativa comunitaria in materia di privacy (a partire dalla direttiva 96/47/CE) alla luce dei principi fissati dagli artt. 7 e 8 della Carta[14].

L'interventismo della Corte di Giustizia solleva, peraltro, l'intricato tema dei rapporti e delle competenze degli organi comunitari. Le pronunce giudiziarie in materia di *data retention* e diritto all'oblio, seppur in larga parte condivisibili, hanno aperto 'voragini' interpretative, costringendo gli operatori commerciali e le autorità garanti nazionali ad un adeguamento che, però, a ben vedere, si è tradotto in un, sia consentito il termine, 'rattoppo' della disciplina vigente più che ad un suo radicale ripensamento. Le decisioni della Corte, inevitabilmente, hanno evidenziato i punti critici dell'assetto normativo, ma non hanno offerto soluzioni applicative: soluzioni che coinvolgono, in primo luogo, le competenze della Commissione, impegnata nel difficile iter di approvazione del Regolamento in materia di dati personali, spesso pregiudicato, come per il diritto all'oblio, dalle censure della Corte di Giustizia[15].

Similmente, la sentenza *Schrems* apre delle falle cui si sta tentando di rimediare in tempi ristretti, al fine di scongiurare i danni economici di cui si diceva dinanzi, ripensando *ex novo* e con mutati rapporti di forza, i negoziati che hanno coindotto al *Privacy Shield*.

Il conflitto che si è inasprito, ma che è aperto da tempo, sta evidenziando una visione sostanzialmente antitetica tra Stati Uniti ed Europa in materia di protezione dei dati personali, da un lato, e di sorveglianza e sicurezza nazionale, dall'altro. Il caso Microsoft, deciso dalla *Second Circuit Court of Appeals* di New York e criticato apertamente dalla Commissione europea, sulla richiesta, ai sensi dello *Stored Communications Act* del

de Protección de Datos (AEPD) e Mario Costeja González, causa C-131/12, su cui si rinvia ai numerosi commenti pubblicati in *Dir. Inf.* n. 4-5, 2014, ora raccolti in G. Resta - V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015.

[14] Su tale profilo, che in questa sede può essere solo accennato, si rinvia ai contributi di O. Pollicino e M. Bassini e di G. Resta in questo Volume, con i riferimenti *ivi* menzionati.

[15] La tematica dei rapporti tra Corte di Giustizia e Commissione europea è stata ampiamente indagata dalla dottrina: cfr., tra gli altri, G. de Burca – J.H.H. Weiler, *The Worlds of European Constitutionalism*, Cambridge Univ. Press, 2011 (in particolare G. de Burca, *The ECJ and the international legal order: a re-evaluation*); M. Dawson – B. De Witte – E. Muir, *Judicial Activism At The European Court Of Justice*, Elgar Publ., London, 2013.

1986[16], di produzione di e-mail archiviate su server localizzati in Irlanda[17], è solo la punta dell'iceberg di un rapporto privacy/sicurezza che, anche a livello costituzionale, sta segnando una cesura netta tra le due sponde dell'Atlantico[18].

Una punta dell'iceberg che, tuttavia, dimostra che la raccolta indiscriminata di dati personali (c.d. *bulk metadata collection*), agevolata dal contesto normativo statunitense (specialmente con l'emanazione del *Patriot Act*[19], ma già con il *Foreign Intelligence Surveillance Act - FISA*[20]), non è arginata neanche dal potere giudiziario[21], spesso invocato come ultimo baluardo per le libertà dei cittadini[22].

[16] 18 U.S.C. §§ 2701–2712.

[17] *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014), 15 F. Supp. 3d 466 (No. 13-MJ-2814). Sul caso in questione, si rinvia a T.J. McIntyre, *Implementing Information Privacy Rights in Ireland*, in S. Egan (ed.), *International Human Rights: Perspectives from Ireland,* Dublin, Bloomsbury, 2015, 272 (articolo interessante, anche perché indaga il rapporto tra il diritto irlandese, i recenti casi decisi dalla Corte di Giustizia e l'importanza assunta dall'Irlanda nel settore che ci interessa, poiché Stato in cui molte delle società della *new economy* hanno scelto di stabilire le proprie sedi europee. Un'importanza che, come l'A. osserva, potrebbe essere accresciuta dal meccanismo *one stop shop* contenuto nel Regolamento comunitario.

[18] S.J. Shackelford, *Fragile Merchandise: A Comparative Analysis of the Privacy Rights for Public Figures*, 49 *Am. Business L. J.* 125, 132 (2012); J.Q. Whitman, *The Neo-Romantic Turn*, in P. Legrand – R. Munday (eds.), *Comparative Legal Studies: Traditions and Transitions*, Cambridge Univ. Press, 2003, 330.

[19] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Public Law Pub.L. 107–56.

[20] Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C. Ch. 36.

[21] Si pensi, ancor prima, al caso *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013), in cui la Corte Suprema ha rigettato le richieste degli attori perché «they were likely to be targets of surveillance were based too much on speculation and on a predicted chain of events that might never occur, so they could not satisfy the constitutional requirement for being allowed to sue». Il caso riguardava la possibilità riconosciuta, in base al *FISA Amendments Act of 2008*, alla *Foreign Intelligence Surveillance Court* di sorvegliare cittadini stranieri senza dover dimostrare che gli stessi rappresentassero un'effettiva minaccia, con margini operativi ritenuti dai ricorrenti eccessivamente ampi e incostituzionali. I commenti della dottrina alla decisione sono stati tendenzialmente negativi: A. Butler, *Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance*, 48 *New England L. Rev.* 56 (2013); N.M. Richards, *The Dangers of Surveillance*, 126 *Harv. L. Rev.* 1934, 1944 (2013); *contra* però A. Rubow, *Standing in the Way of Privacy Protections: The Argument for a Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action*, 29 *Berkeley Tech. Law J.* (2014).

[22] Sulla questione, per ulteriori approfondimenti, si rinvia al saggio di G. Resta in questo Volume, ma v. già F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 *Law & Cont. Probl.* 101, 108. Un'opinione diametralmente opposta è

Né può ritenersi che l'emanando *Judicial Redress Act*[23], attualmente in fase di discussione e approvazione al Senato, possa essere una risposta appagante alla decisione della Corte di Giustizia. Il JRA, infatti, si limiterebbe ad estendere ai cittadini europei i medesimi diritti riconosciuti dal *Privacy Act* ai cittadini americani in caso di violazioni dei dati personali: una soluzione comunque non idonea a frenare le preoccupazioni che hanno condotto alle censure della Corte di Giustizia, atteso che il *Privacy Act* offre garanzie insufficienti in caso di sorveglianza di massa[24].

Ma, soprattutto, una soluzione che dimostra un approccio contrapposto tra il diritto comunitario, che, anche per mezzo dei ripetuti interventi della Corte di Giustizia, sta segnando la supremazia della tutela dei dati personali, intesa quale diritto fondamentale, rispetto alle esigenze di sicurezza che, al contrario, appaiono ancora predominanti per il legislatore statunitense e nell'interpretazione del formante giurisprudenziale[25].

Non sorprende, quindi, che nel *draft* dei *Privacy Shield* limitino fortemente la raccolta indiscriminata di dati, che può avvenire in casi estremi e non come normale prassi di sicurezza nazionale[26].

---

invece sostenuta da P. Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, *Georgia Tech Scheller College of Business Research Paper*, No. #36, secondo cui la convergenza di *rule of law*, separazione dei poteri e controllo giurisdizionale assicurerebbe un livello di protezione sostanzialmente equivalente a quello europeo. L'A. osserva che la Corte di Giustizia non avrebbe considerato adeguatamente le modifiche intervenute nel corso del 2013 e avrebbe valutato non correttamente i mezzi istruttori prodotti durante la controversia.

[23] H.R.1428.

[24] Cfr. D. Bender, *The Judicial Redress Act: A Path to Nowhere, in Privacy Advisor*, Dec. 17, 2015.

[25] In termini simili anche M. Mensi, *Il vero sconfitto è la Commissione europea*, cit., 52, secondo cui «a sopperire le difficoltà della Commissione, la Corte scende in prima linea per rivendicare la primazia di un ordinamento (quello europeo) che, a fronte della *disruptive innovation* della Rete e dei suoi protagonisti (gli operatori Ott, Google, Facebook, Amazon, ecc.), negli ultimi anni aveva segnato il passo a vantaggio di quello di matrice anglosassone, laddove le transazioni online e l'*e-commerce* si sono sviluppate su un sistema più agile e *business friendly*, fondato sull'autodichiarazione e sul consenso delle parti».

[26] Cfr. in particolare il *Considerando 59* dei *Privacy Shield*: «In this regard, the representations of the Office of the Director of National Intelligence (ODNI) provide further assurance that these requirements, including the definition of bulk collection in PPD-28 (n. 5), express a general rule of prioritisation of targeted over bulk collection. According to these representations, Intelligence Community elements «should require that, wherever practicable, collection should be focused on specific foreign intelligence targets or topics through the use of discriminants (e.g. specific facilities, selection terms and identifiers). While PPD-28 explains that Intelligence Community elements must sometimes collect bulk signals intelligence in certain circumstances, for instance in order to identify

3. Corporate Binding Rules

L'azzeramento del *Safe Harbor Agreement* ha imposto un ripensamento degli strumenti giuridici alternativi per il trasferimento transfrontaliero di dati personali, spesso trascurati sia dalla prassi commerciale sia dagli studi dottrinali.

Clausole contrattuali standard e *binding corporate rules* garantiscono la medesima efficacia, legittimando i trasferimenti di dati oltre lo spazio europeo, ma impongono costi transattivi più alti. Quanto appena detto vale specialmente per le clausole contrattuali standard (anche note come *model contract clauses*), che sono clausole da inserire all'interno di contratti tra imprese che non appartengono al medesimo gruppo (cui, invece, sono riservate le *binding corporate rules*)[27].

Le *corporate binding rules* sono, invece, strumenti utilizzati dai gruppi di società per trasferire dati personali da un Paese comunitario o rientrante nello Spazio economico europeo ad un Paese terzo, nel caso in cui il trasferimento avvenga tra società appartenenti allo stesso gruppo. Non si può ricorrere a tale strumento, quindi, quando il soggetto che riceve i dati personali non afferisce al gruppo societario; tale limite vale anche nel caso in cui detto soggetto abbia un rapporto continuativo con la società, titolare del trattamento, che esegue il trasferimento dei dati[28].

Le *corporate binding rules* sono il complesso delle norme tecniche, degli strumenti di sicurezza, delle *policy* aziendali, delle attività di *training* e di *audit* che si intendono realizzare e così via discorrendo, che sono adottate dalle società infragruppo nel trattamento dei dati personali. È necessario il parere positivo di un'autorità garante che, in assenza del consenso del soggetto interessato, legittimi il trasferimento. È altresì richiesto che tale trasferimento sia preventivamente comunicato nell'informativa fornita a clienti e utenti: difatti, sebbene l'autorizzazione del Garante nazionale sia

new or emerging threats, it directs these elements to prioritise alternatives that would allow the conduct of targeted signals intelligence. Hence, bulk collection will only be allowed where targeted collection via the use of discriminants is not possible «due to technical or operational considerations". This applies both to the manner in which signals ntelligence is collected and to what is actually collected. According to representations of the ODNI all this ensures that the exception does not swallow the rule».

[27] Tali costi, poi, sono ancora più alti nel caso in cui si voglia raccogliere il consenso dei singoli soggetti cui si riferiscono i dati personali, atteso che, da un lato, tale pratica impone alle imprese di contattare singolarmente gli interessati e che, dall'altro, la prestazione del consenso potrebbe essere negata dagli stessi.

[28] Cfr. WP 155: Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, 2.

finalizzata a scavalcare la necessità della raccolta del consenso, è comunque obbligatorio che il soggetto interessato sia edotto in merito ai soggetti terzi cui potrebbero essere trasferiti i suoi dati personali.

L'*Article 29 Working Party* ha pubblicato numerosi documenti per sensibilizzare le imprese e per fissare le linee guida da seguire nella redazione delle regole imprenditoriali[29]. Si tratta, apparentemente, di regole di *soft-law*, atteso il loro carattere meramente persuasivo e derogabile da parte dei soggetti interessati; tuttavia, l'analisi delle posizioni delle singole Autorità garanti nazionali, che adottano pedissequamente le linee-guida del *Working Party*, induce ad assegnare, seppur di fatto, una natura vincolante a tali regole.

L'Autorità presso la quale presentare la richiesta è quella dove ha sede la società madre ovvero quella della sede societaria presso la quale avviene il trattamento dei dati in via principale[30]. La società scelta deve essere comunque stabilita nell'Unione europea; il *Working Party* elenca i criteri che dovrebbero essere seguiti in tale eventualità, quali, ad esempio, la società che effettuerà il maggior numero di trattamenti di dati, quella che sarà responsabile per le scelte relative alle finalità e alle modalità del trattamento e così via discorrendo[31].

La società che presenterà l'istanza al proprio Garante nazionale sarà altresì responsabile per eventuali violazioni commesse in Paesi terzi; similmente a quanto stabilito per le *standard contract clauses*, è ammessa una

[29] WP 107: Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From «Binding Corporate Rules»; WP 108: Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules; WP 133: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data; WP 153: Working Document setting a table with the elements and principles to be found in Binding Corporate Rules; WP 154: Working Document Setting up a framework for the structure of Binding Corporate Rules; WP 155: Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules.

[30] Per la precisione, il Working Party (cfr. WP 108: Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, 14 aprile 2005, 3) parla di *«ultimate parent or operational headquarters»*.

[31] Le lingue da utilizzare sono l'inglese e la lingua dell'Autorità nazionale che riceve la richiesta; cfr. WP 133: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data; nonché WP 107: Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From «Binding Corporate Rules»: «The language of the application shall be set up according to WP 107, Section (8), where [...] as a general rule and without prejudicing to other translations where necessary or required by law, first and consolidated drafts should be provided both in the language of the leading authority and in English. The final draft must be translated into the languages of those DPAs concerned».

responsabilità solidale tra la società esportante e quella importante. In ogni caso, si tratta di previsioni non tassative, nel senso che il gruppo societario può proporre al Garante nazionale una diversa ripartizione delle responsabilità, tenuto conto della propria struttura organizzativa[32].

La Raccomandazione del 2007 stabilisce che la società debba dimostrare che le regole societarie siano approvate internamente (nel senso che vi sia un accordo formale tra la società madre e le società controllate) e quali siano i vantaggi per i soggetti interessati, i cui dati sono trasferiti fuori dai confini europei.

L'art. 43 della proposta di Regolamento ha recepito le istanze del *Working Party*, prevedendo che tutte le società appartenenti al gruppo si impegnino a rispettare i principi previsti in materia di dati personali e, in particolare, i principi di finalità, di minimizzazione dei dati, di conservazione dei dati per periodi limitati, nonché ad adottare le regole di protezione dei dati *by design* e *by default*. Le *corporate binding rules* dovranno inoltre evidenziare le misure per garantire la sicurezza e i principi applicabili a specifiche categorie di dati personali.

Le regole del gruppo dovranno essere approvate secondo il *consistency mechanism* di cui agli artt. 57 ss.: dopo l'approvazione dell'Autorità garante nazionale, sarà richiesto un parere dell'*European Data Protection Board* e (ma il testo della proposta licenziato non è chiaro al riguardo) un'autorizzazione da parte della Commissione.

Le *corporate binding rules* presentano il vantaggio di non incontrare limiti geografici, nel senso che possono essere estese a tutte le società appartenenti al gruppo, anche se vi abbiano aderito successivamente all'approvazione delle regole.

Al contempo, però, sono considerate uno strumento frutto di un processo elaborato e oneroso (i cui tempi sembrano destinati ad allungarsi dopo l'entrata in vigore del Regolamento)[33], che tende a scoraggiare gli interessi imprenditoriali, come dimostra il fatto che solo una ventina di gruppi vi ha fatto sinora ricorso[34]. Inoltre, trovando applicazione ai soli rapporti tra società che appartengono al medesimo gruppo, non possono essere considerate un'alternativa unica agli accordi di adeguatezza, dal

[32] WP 155: Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, 3.

[33] Al momento, i tempi per ottenere l'autorizzazione sono stimati tra i 18 e i 24 mesi, con una previsione di budget medio di 220.000 dollari, cfr. K. Bloom – K. Royal, *Transferring Personal Data Out of the European Union: Which Export Solution Best Fits Your Needs?*, *Associate of Corporate Counsel*, June 2015, 32 e 34.

[34] K. Bloom – K. Royal, *Transferring Personal Data Out of the European Union*, cit., 30.

momento che, in caso di trasferimento di dati a società terze, si dovrà necessariamente ricorrere ai *model contract clauses*.

4. Model Contract Clauses

Un'ulteriore deroga al generale divieto di trasferimento di dati personali verso Paesi che non assicurino un livello adeguato di protezione è rappresentato, come si diceva, dalle clausole contrattuali standard (o *model contract clauses*, conformemente alla terminologia internazionale). Si tratta di clausole dettate da decisioni della Commissione europea che sono incorporate nel testo dei contratti che regolano l'esportazione di dati personali, contratti a cui aderisce, assumendo specifiche obbligazioni, il soggetto importatore stabilito al di fuori dell'Unione europea.

La fonte normativa, ancora una volta, è il secondo paragrafo dell'art. 26 della Direttiva 95/46/CE: tuttavia, la decisione della Commissione, sebbene non precluda la possibilità che le singole Autorità nazionali rilascino autorizzazioni per il trasferimento dei dati, obbliga le Autorità stesse a riconoscere che le clausole standard, se incluse nei contratti che disciplinano il trasferimento dei dati personali tra un soggetto stabilito nel territorio dell'Unione ed un soggetto extracomunitario, assicurino di per sé un adeguato livello di protezione.

In assenza di accordi di adeguatezza, le *model contract clauses* sono lo strumento maggiormente utilizzato dalle società commerciali per il trasferimento dei dati personali.

Nel momento in cui si scrive, la Commissione europea ha adottato quattro decisioni[35], che, nel corso del tempo, hanno modificato e integrato le clausole inizialmente previste e hanno specificato gli obblighi di esportatori e importatori.

Le *model contract clauses* presentano l'indiscutibile vantaggio di essere

[35] Si tratta della Decisione Commissione, Clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento in paesi terzi, dir. 95-46-CE del 5 febbraio 2010; della Decisione della Commissione per l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi del 27 dicembre 2004; della Decisione della Commissione, Clausole contrattuali tipo per trasferimento dati a carattere personale verso paesi terzi a norma dir. 95-46-CE del 5 giugno 2001; della Decisione della Commissione, Clausole contrattuali tipo per trasferimento dati personali a incaricati del trattamento residenti in paesi terzi, dir. 95-46-CE del 27 dicembre 2001.

uno strumento giuridico 'sicuro', nel senso che il loro recepimento legittima l'esportazione dei dati personali verso Paesi terzi che non possono giovare di accordi di adeguatezza. È evidente, tuttavia, che, in quanto clausole da inserire all'interno di un regolamento contrattuale, determinano un aumento dei costi transattivi[36], dal momento che, seppur non modificabili (ma sul punto si ritornerà a breve), si inseriscono all'interno di una negoziazione, gravando l'importatore di una vasta gamma di obblighi e di responsabilità.

Peraltro, è appena il caso di osservare che l'importatore assume tali obblighi – prescritti dalla legge e non frutto di una autonoma manifestazione di volontà – nei confronti sì dell'esportatore, ma nell'interesse del soggetto interessato, che è naturalmente terzo rispetto al contratto stipulato tra le parti[37].

5. L'immodificabilità delle clausole e la soluzione inglese

Le clausole contrattuali standard rappresentano, a parere di chi scrive, un esempio di fonte di integrazione del contratto. Come da tempo ha osservato la migliore dottrina, le fonti di integrazione non operano, infatti, nel solo caso in cui vi siano lacune ovvero dove il regolamento contrattuale sia inidoneo ad operare o sia, in ogni caso, improduttivo di effetti giuridici[38], ma agiscono quali forme di eterointegrazione della volontà contrattuale[39].

Nel caso che ci interessa, tuttavia, la volontà legislativa pare sostitu-

[36] In termini simili anche S.J. Shackelford, *Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's Schrems Decision and What it Means for Transatlantic Relations*, in corso di pubblicazione in *Eton Hall J. of Diplomacy & Int'l Rel.* (2016), 4 del dattiloscritto.

[37] Il tema degli obblighi di protezione nel trattamento dei dati personali è affrontato, tra gli altri, da F. Piraino, *Il codice della privacy e la tecnica del bilanciamento di interessi*, in *Libera circolazione e protezione dei dati personali*, a cura di R. Panetta, Milano, 2006, 709 s.

[38] Osserva S. Rodotà, *Le fonti di integrazione del contratto*, Milano, 1969, 8: «il problema dell'integrazione non è strettamente condizionato dall'esistenza di lacune. In altri termini, non è soltanto nei casi di oggettiva inidoneità ad operare del regolamento predisposto dalle parti che può aver luogo il ricorso agli strumenti integrativi (come, invece, continua ad accadere al livello dell'ordinamento legislativo per il ricorso all'analogia)».

[39] S. Rodotà, *op. cit.*, 4.

irsi completamente quella privata[40]. Difatti, se è vero che «gli esportatori e gli importatori dei dati sono pertanto liberi di inserire qualsiasi altra clausola commerciale ritenuta pertinente ai fini del contratto, purché non incompatibile con le clausole tipo», tuttavia la formulazione letterale delle clausole dovrebbe essere lasciata intatta.

Si è in presenza, quindi, di una forma (estrema) rimediale di natura anticipatoria, nel senso che l'ordinamento comunitario si sostituisce all'autonomia dei privati, ritenuti inidonei o incapaci di compiere una valutazione degli interessi in gioco[41]. Non siamo in presenza, quindi, di una clausola da sostituire, perché contraria ad una prescrizione normativa, né, in senso stretto, dinanzi ad una *default rule*[42]. Al più, la fattispecie in esame potrebbe essere accostata alle *immutable rules*, pensate, secondo l'insegnamento della dottrina americana, per tutelare non solo (e non tanto) le parti del contratto, quanto i terzi, la cui sfera giuridica potrebbe essere lesa dagli effetti o dall'esecuzione del contratto stesso[43].

Peraltro, l'ipotesi in esame non rappresenta neanche un caso isolato nella legislazione di derivazione comunitaria: basti pensare, ad esempio, all'art. 129, comma 2 del Codice del consumo, in materia di indici di conformità del bene nella vendita di beni di consumo[44].

La metodologia percorsa dalla Commissione, da un punto di vista comparatistico, appare in antitesi con la visione tradizionale del diritto dei contratti dei sistemi giuridici appartenenti all'area di *civil law*, in cui l'elemento volontaristico è predominante e le forme di sostituzione della volontà privata da parte dell'ordinamento sono considerate come eccezionali[45]. Pertanto, sebbene da tempo si discorra di un avvicinamento della

[40] Intesa, secondo l'insegnamento della migliore dottrina, come libertà di determinare il contenuto del contratto, F. Messineo, *Il contratto in genere*, in *Tratt. dir. civ. e comm.* Dir. da A. Cicu - F. Messineo, Milano, 1966, 802.

[41] Sul punto, per ulteriori rilievi, v. U. Mattei, *I rimedi, in Il diritto soggettivo*, in *Tratt. dir. civile* diretto da R. Sacco, Torino, 2001, 131 ss.

[42] Cfr. V. Roppo, *Il contratto*, Milano, 2011, 435.

[43] In questo senso v. I. Ayres – R. Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules, 99 Yale Law Journal* 87 (1989).

[44] L'esempio è menzionato in S. Mazzamuto – A. Plaia, *I rimedi nel diritto privato europeo*, Torino, 2012, 6, cui si rinvia per ulteriori approfondimenti sull'approccio del legislatore comunitario.

[45] Cfr., tra i tanti, G. Mirabelli, *Dei contratti in generale*, in *Comm. Cod. civ.*, IV, t. II, Torino, 1958, 87, e, per l'ordinamento francese, P. Durand, *La tendence à la stabilité du rapport contractuel*, Paris, 1960, 10 ss., ma v. anche, per una comparazione tra Inghilterra e Francia, D. Harris – D. Tallon (eds.), *Contract Law Today: Anglo-French Comparisons,* Oxford, Clarendon Press, 1989.

disciplina contrattuale tra ordinamenti del *common law* e del *civil law*[46], pare plausibile ritenere che l'idea che possa essere il legislatore a fissare i termini del regolamento contrattuale sia mutuato da esperienze appartenenti all'area del diritto angloamericano.

La fattispecie in parola, tuttavia, presenta alcuni elementi peculiari. La Decisione del 2011, all'art. 10, rubricato 'Modifica del contratto', prevede che le parti si impegnino «a non alterare o non modificare le presenti clausole»; è ammesso invece l'inserimento di altre clausole, purché non siano in contrasto con quelle previste dalla Decisione stessa.

Pertanto, dovrebbe concludersi per il divieto assoluto di modificare la formulazione prevista dalla Commissione europea, anche nel caso in cui la stessa sia più favorevole al soggetto interessato.

Una conclusione che risponde, evidentemente, alla necessità, da un lato, per le imprese, di utilizzare un modello contrattuale, appunto, standardizzato e sicuro, in modo da rispondere a criteri di efficienza temporale ed economica. Pare evidente, infatti, che l'eventuale negoziazione singola delle clausole con tutti gli importatori potrebbe determinare aumento dei tempi e dei costi transattivi (*in primis* le spese legali per la revisione dei singoli contratti): in questo modo, inoltre, si risponde anche alla critica, spesso mossa alle clausole contrattuali standard, di non essere estensibili a tutti i rapporti contrattuali dell'impresa con i singoli importatori. Questi ultimi, infatti, sebbene spesso nella pratica degli affari siano soggetti economicamente più deboli e quindi inclini ad aderire acriticamente alle condizioni dell'esportatore, potrebbero non voler assumere specifici obblighi, imponendo alla controparte una negoziazione: eliminare *ab origine* tale rischio si traduce, evidentemente, in un vantaggio per l'impresa esportatrice, che è vincolata, ai sensi del precitato art. 10, al divieto di modifica delle clausole.

Del resto, la modifica delle *model contract clauses* potrebbe determinare altresì l'obbligo di revisione da parte delle Autorità garanti nazionali, che dovrebbero approvare, e conseguentemente autorizzare, le variazioni apportate al testo della Commissione. Anche in questo caso, il divieto di modifica risponde all'esigenza di evitare che le singole Autorità siano gravate da un carico di lavoro eccessivo. Se, poi, si analizza tale ipotesi dalla prospettiva dell'impresa, l'eventuale autorizzazione determinerebbe, inevitabilmente, ulteriori rallentamenti nell'adozione delle stesse, pregiudicando i rapporti commerciali tra esportatore e importatore.

[46] Per tutti, J. Gordley, *The Philosophical Origins of Modern Contract*, Oxford, Clarendon Press, 1991, 1 ss.

Sotto il profilo della patologia del contratto, tuttavia, è bene precisare che la modifica delle condizioni contrattuali non determina, di per sé, alcuna forma di invalidità o di inefficacia del contratto. Al più, come si osservava, pare possibile ipotizzare che l'alterazione della formulazione proposta (*rectius*: imposta) dalla Commissione possa determinare l'insorgere dell'obbligo di ottenere una preventiva autorizzazione da parte dell'Autorità garante competente – che, argomentando *ex* art. 9 della Decisione, è quella del Paese dove è stabilito il soggetto importatore – autorizzazione che legittima il trasferimento dei dati personali al di fuori del territorio dell'Unione europea.

L'assenza dell'autorizzazione, tuttavia, non dovrebbe comportare alcuna forma di responsabilità, né nei confronti dei soggetti interessati né dell'Autorità di garanzia competente. A tale conclusione può pervenirsi argomentando che le clausole, anche se modificate, assicurano comunque uno spettro di tutela adeguato per gli interessati: pertanto, l'eventuale trattamento illecito potrebbe essere al più il frutto di un'indagine specifica del Garante territorialmente competente, nella sola ipotesi in cui gli obblighi assunti dalle parti e dagli eventuali subcontraenti non siano ritenute conformi alle prescrizioni della Commissione europea.

Nel diritto inglese, peraltro, una soluzione parzialmente differente alla questione della modificabilità delle clausole pare essere stata suggerita dall'ICO (*Information Commissioner's Officer*), secondo cui eventuali emendamenti non determinerebbero automaticamente il venir meno del requisito dell'adeguatezza[47]. A giudizio dell'Autorità inglese, infatti, le

[47] ICO, *Model Contract clauses – International transfers of personal data*, 2012, 6: «Use of any version of the model clauses, whether as a stand-alone contract or incorporated into another contract, where the wording is changed (even if the meaning or effect of the changed clause remain unaltered), will not amount to use of clauses that are authorised by the Information Commissioner as providing adequate safeguards under one of the Information Commissioner authorisations set out above. If you choose to amend the model contract clauses, you may take the view that your amended clauses are sufficient to provide adequate safeguards for the protection of the rights of the data subjects whose personal data you propose to transfer. Your amended clauses will not be 'model contract clauses' (attracting the Commission 'guarantee' that they provide adequate safeguards for data subjects rights) but may operate as contractual arrangements which in the reasonable view of the data controller provide adequate safeguards for data subjects' rights. Providing adequate safeguards by using your own clauses is an equally valid basis on which to proceed with a transfer as is the use of model contract clauses. The only difference is that you need to be prepared to offer evidence in support of your view (that your clauses provide adequate safeguards) if it is challenged. If you use model contract clauses, given that the Commission has determined that such clauses offer adequate safeguards, there can be no challenge as to the effectiveness of the safeguards the model contract

variazioni al testo approvato dalla Commissione europea comporterebbero solo l'insorgere, in capo all'esportatore dei dati personali, dell'onere di dover dimostrare che le nuove clausole siano idonee ad assicurare un livello di protezione pari a quello previsto dalle decisioni comunitarie.

Si deve ritenere, quindi, che, a giudizio del Garante inglese, tale controllo sia successivo ed eventuale e che, quindi, non sia richiesta neanche un'autorizzazione preventiva da parte dell'autorità nazionale alla modifica delle clausole. Tale conclusione, del resto, risponde sia ad un'ottica solidaristica e antiformalistica della tutela dei soggetti interessati, sia ad un'ottica giuseconomica, considerando i costi transattivi associati alla riscrittura delle clausole contrattuali.

Difatti, da un lato la modifica delle clausole, nel caso in cui siano apprestate comunque garanzie adeguate o addirittura superiori (ad esempio, l'adozione di specifiche misure di sicurezze per la protezione dei dati) rispetto a quelle dettate dalla Commissione, risponde alle esigenze di tutela non solo delle controparti contrattuali, ma anche (e soprattutto) dei soggetti terzi (ossia dei soggetti cui appartengono i dati personali). Dall'altro, se la variazione del testo delle clausole richiedesse l'autorizzazione preventiva dell'Autorità garante nazionale, allora sarebbe una soluzione in gran parte impraticabile, dal momento che causerebbe un significativo aumento dei tempi per l'approvazione del contratto e un aumento, altrettanto significativo, dei costi transattivi relativi al contratto stesso.

La scarsa flessibilità delle *standard contractual clauses*, del resto, aveva indotto la Commissione ad adottare una Decisione nella quale, alle originarie clausole del 2001, erano affiancate clausole alternative e differenti, proposte e negoziate da un consorzio di associazioni imprenditoriali[48].

Tale decisione, però, a proposito dell'annosa questione di cui si discute, aveva fornito una risposta negativa, emendando l'art. 1 della Decisione 2001/497/CE e stabilendo (in anticipo rispetto alla Decisione del 2011) il divieto di modifica o di combinare le clausole della Decisione del 2001 con quelle del 2004.

clauses offer».

[48] Cfr. Decisione della Commissione per l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi del 27 dicembre 2004, *Considerando n. 2*. Il consorzio era formato da: Camera di commercio internazionale (ICC), Japan Business Council in Europe (JBCE), European Information and Communications Tech- nology Association (EICTA), EU Committee of the American Cham- ber of Commerce in Belgium (Amcham), Confederation of British Industry (CBI), International Communication Round Table (ICRT) e Federation of European Direct Marketing Associations (FEDMA).

Aderendo all'interpretazione più restrittiva, considerando quindi immodificabili le clausole, dovrebbe peraltro ritenersi che il contratto possa essere stipulato esclusivamente in una delle lingue dell'Unione europea (lingue nelle quali le *standard contract clauses* sono disponibili) e che l'eventuale traduzione nella lingua madre dell'importatore, costituendo in ogni caso una variazione rispetto al testo licenziato dalla Commissione, non possa essere la lingua del contratto avente ad oggetto il trasferimento dei dati personali[49].

6. Rapporti tra importatore ed esportatore

Un altro dei punti critici della clausole contrattuali standard è rappresentato dalla rigidità dei rapporti tra importatore ed esportatore e dalle complessità associate ad eventuali subcontratti.

Ai sensi dell'art. 3 della Decisione del 2011, l'esportatore è qualificato quale titolare del trattamento (ovvero come responsabile, conformemente alla terminologia comunitaria), mentre l'importatore riveste il ruolo di incaricato del trattamento. La Decisione, quindi, esclude la possibile sussistenza di una contitolarità nel trattamento dei dati tra i due soggetti, conformemente a quanto previsto da alcune decisioni dei Garanti nazio-

[49] Così K. Bloom – K. Royal, *Transferring Personal Data Out of the European Union*, cit., 32. Gli studi di diritto comparato hanno evidenziato le insidie nella traduzione dei termini giuridici e la frequenza con cui termini apparentemente simili celino concetti giuridici differenti: tra i tanti studi sulla materia si rinvia a R. Sacco, *Riflessioni di un giurista sulla lingua (la lingua del diritto uniforme, e il diritto al servizio di una lingua uniforme)*, in *Riv. dir. civ.*, 1996, I, 57, Id., *Traduzione giuridica*, in *Dig. disc. priv., sez. civ.*, Agg., 2000, 722; L.-J. Constantinesco, *Il metodo comparativo,* ed. it. a cura di A. Procida Mirabelli di Lauro, Torino, 2000, 123; M. Morris (ed.), *Translation and the Law*, in *American Translators Association Scholarly Monograph Series*, VIII, Amsterdam-Philadelphia, 1995; B. Pozzo (a cura di), *Lingua e diritto: oltre l'Europa*, Milano, 2014; C.J.W. Baaij *The Role of Legal Translation in Legal Harmonization*, Kluwer Law Int., 2014; S. *Šarčević*, *Language and Culture in EU Law. Multidisciplinary Perspectives*, Ashgate, 2015. Nella prassi dei contratti aventi ad oggetto il trasferimento di dati personali, il linguaggio e la terminologia, anche a livello internazionale, sono generalmente mutuati da quelli delle normative comunitarie, dalle quali sono riprese le definizioni e la ripartizione dei soggetti coinvolti (es. soggetto interessato, titolare/responsabile del trattamento, incaricato, ecc.); ciò tuttavia non esclude a priori l'eventualità di errori, *false friends* e ulteriori imprecisioni, determinati dalle diversità tra gli istituti giuridici nazionali (basti pensare alla panoplia dei rimedi apprestati dai singoli ordinamenti giuridici in caso di violazione degli obblighi contrattuali).

nali[50], nonché l'eventualità che l'importatore sia tenuto a trattare i dati personali ricevuti «per conto e secondo le istruzioni dell'esportatore stesso», permanendo in capo a quest'ultimo la titolarità (e, pertanto, il potere di determinare gli strumenti, le modalità e le finalità del trattamento).

È ammesso il subcontratto ossia l'eventualità che l'importatore assegni a terzi l'esecuzione, totale o parziale, degli eventuali obblighi assunti nei confronti dell'esportatore; in questa ipotesi, è però richiesto il previo consenso scritto dell'esportatore (clausola 11). A fronte di un subcontratto, tuttavia, l'importatore resterà responsabile, in via solidale, nei confronti dell'esportatore e del soggetto interessato, per gli eventuali obblighi di protezione previsti dall'accordo stipulato con l'esportatore.

Il regime di responsabilità delineato dalla Decisione del 2010 presenta alcune singolarità, se comparato a quello della direttiva 95/46/CE[51], sebbene esso sia, essenzialmente e nei termini in cui si dirà a breve, di natura mista (vicaria e sussidiaria).

La clausola 6 della Decisione del 2011, infatti, stabilisce che l'interessato che abbia subito un danno che sia riconducibile alla condotta di una delle parti del contratto di trasferimento dati ovvero a quella del subincaricato, abbia «diritto di ottenere dall'esportatore il risarcimento del danno sofferto».

In prima istanza, quindi, la Commissione europea ha scelto di imputare all'importatore il costo degli eventuali illeciti trattamenti dei dati per-

[50] Cfr. ICO, *Guide to Data Protection. Sending personal data outside the European Economic Area (Principle 8)*, nonché Garante per la protezione dei dati personali, provv. 15 giugno 2011, *Titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali*, in *Gazz. Uff.*, n. 153 del 4 luglio 2011, in cui l'Autorità ha chiarito che i call center non possano essere nominati contitolari del trattamento, ma che la titolarità debba rimanere in capo al soggetto che stabilisce le modalità e le finalità del trattamento dei dati personali.

[51] Sul modello di responsabilità civile previsto dalla direttiva si rinvia, *ex multis*, a S. Sica, *Commento sub art. 18*, in E. Giannantonio - M. G. Losano - V. Zeno- Zencovich, *La tutela dei dati personali. Commentario alla l. 675/96*, Padova, 1997, 176 ss.; M. Franzoni, *Dati personali e responsabilità civile*, in *Resp. civ. prev.*, 1998, 902 ss.; G. Comandè, *Danni cagionati per effetto del trattamento dei dati personali*, in F.D. Busnelli - C.M. Bianca, *Tutela della privacy*, in *Nuove leggi civ. comm.*, 1999, 482 ss.; F.D. Busnelli, *Il «trattamento dei dati personali» nella vicenda dei diritti della persona: la tutela risarcitoria*, in V. Cuffaro - V. Ricciuto - V. Zeno-Zencovich, *Trattamento dei dati e tutela della persona*, Milano, 1998, 177 ss.; G. Alpa, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in *Dir. Inf.* 1997, 703 ss.; D. Carusi, *La responsabilità*, in V. Cuffaro - V. Ricciuto, *Il trattamento dei dati personali*, 2a ed., Torino, 1999, 356 ss.; G. Buttarelli, *Banche dati e tutela della riservatezza*, Milano, 1997, 350 ss.; V. Roppo, *La responsabilità civile per trattamento di dati personali*, in *Danno e resp.*, 1997, 660 ss.

sonali, così come avviene all'interno della direttiva, che prevede la responsabilità del titolare del trattamento anche per il fatto degli incaricati. Una opzione normativa che risponde ad almeno due esigenze: da un lato, quella di favorire la posizione processuale dell'interessato, che non sarà costretto ad indirizzare la propria richiesta risarcitoria ad un soggetto stabilito fuori dai confini dell'Unione europea e, dall'atro, quella di allocare i *costs of accidents* in capo all'importatore che, nella maggior parte dei casi, è la *deep pocket party*, ossia il soggetto economicamente nella posizione più efficiente per compensare i costi del risarcimento dovuto all'interessato[52].

La Decisione del 2010 prende in esame anche la fattispecie in cui l'esportatore sia «scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente»: in questa eventualità, la responsabilità si trasferirà in prima istanza sull'importatore, che sarà chiamato a rispondere anche delle violazioni commesse dall'importatore nonché, a titolo solidale, di quelle commesse dal subincaricato, non potendo eccepire la violazione degli obblighi assunti da quest'ultimo «al fine di escludere la propria responsabilità», come espressamente disposto dalla clausola 6, secondo capoverso.

La responsabilità del subincaricato è, al pari di quella dell'importatore, di natura sussidiaria, atteso che l'interessato potrà rivalersi in giudizio nei suoi confronti nel solo caso in cui sia l'importatore sia l'esportatore «siano scomparsi di fatto, abbiano giuridicamente cessato di esistere o siano divenuti insolventi» (clausola 6, terzo capoverso). Il subincaricato, tuttavia, risponderà esclusivamente per i trattamenti effettuati da quest'ultimo e non anche per quelli posti in essere esclusivamente dall'importatore o dall'esportatore.

In entrambe le fattispecie descritte, il meccanismo della sussidiarietà agirà esclusivamente laddove non vi sia una successione nei rapporti giuridici dell'esportatore o dell'importatore e gli obblighi contrattuali non siano stati trasferiti ad altro soggetto, per contratto o per legge.

La tutela apprestata a favore dell'interessato è poi rafforzata dalla clausola 7, relativa a mediazione e giurisdizione. In base a tale clausola, l'importatore si impegna, in caso di azione per il risarcimento del danno,

[52] Per tutti, G. Calabresi, *Costo degli incidenti e responsabilità civile*, trad. a cura di A. De Vita - V. Varano - V. Vigoriti, pref. di S. Rodotà, Milano, 1975, 65 ss.; l'A. definisce l'allocazione dei costi sui soggetti con maggiori capacità patrimoniali come il metodo più adatto a «ridurre i costi secondari dei sinistri» trasferendoli «su quelle categorie di persone, la cui posizione sociale ed economica meno ne risentirebbe, su quelli, cioè, che generalmente si sogliono definire 'ricchi'»; ma similmente anche R. Posner, *Strict Liability: A Comment*, 2 *J. Legal Studies* 205, 210 (1973).

a «sottoporre la controversia alla mediazione di un terzo indipendente o eventualmente dell'autorità di controllo» ovvero a «deferire la controversia agli organi giurisdizionali dello Stato membro in cui è stabilito l'esportatore».

La Commissione, però, nella consapevolezza che, nell'economia globalizzata, spesso i soggetti interessati possono essere residenti in un Paese diverso rispetto a quello dell'esportatore, fa salvi i «rimedi giuridici previsti dalla normativa nazionale o internazionale»: in altri termini, l'interessato potrà beneficiare delle norme di diritto internazionale privato in materia di illecito aquiliano che stabiliscono l'applicabilità del foro competente dell'attore e della legge applicabile del luogo in cui si sono manifestati gli effetti dannosi della condotta illecita.

Conclusioni

Sino alla sentenza Schrems, *standard contractual clauses* e *corporate binding rules* hanno rivestito un ruolo ancillare rispetto ai *safe harbor agreement* e, in generale, agli accordi di adeguatezza per una molteplicità di ragioni, alcune delle quali sono già state esposte in precedenza.

Innanzi tutto, perché il *safe harbor agreement* è stato considerato uno strumento più sicuro, anche per i controlli blandi esercitati da parte della *Federal Trade Commission* sull'adempimento degli accordi da parte delle società aderenti[53], controlli che, già prima dell'intervento della Corte di Giustizia, avevano sollevato non poche critiche da parte della Commissione[54].

L'inefficiente esercizio della funzione deterrente pare accomunare,

[53] La FTC è intervenuta meno di 20 volte per sanzionare la violazione degli accordi di *Safe Harbor* (e, in dodici casi, si è giunti ad una mediazione con i soggetti coinvolti sul pagamento delle relative sanzioni). Peraltro, la maggior parte degli interventi dell'Autorità statunitense sono avvenuti nel corso del 2014, dopo gli interventi della Commissione europea, cfr. K. Bloom – K. Royal, *Transferring Personal Data Out of the European Union*, cit., 36.

[54] Cfr. 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, COM(2013) 847 final, 27.11.2013; Communication from the Commission to the European Parliament and the Council, *Restoring Trust in EU-US data flows*, COM(2013) 846 final, 27.11.2013, nonché il relativo Memorandum *Restoring Trust in EU-US data flows – Frequently Asked Questions*, MEMO/13/1059, 27.11.2013.

invero, gli accordi di adeguatezza (e, in special modo, quelli di *safe harbor*) e i modelli contrattuali standard, sottolineando la natura formalistica della legislazione in materia di protezione dei dati personali[55]. In altri termini, occorre domandarsi se la predisposizione di modelli contrattuali standard ovvero, per le imprese legittimate, delle *corporate binding rules* siano effettivamente in grado di tutelare i diritti dei soggetti interessati o se si riducano, nei fatti, all'adesione formalistica alle prescrizioni derivanti dalla normativa o ordinate dalle Autorità Garanti.

Di là da tali rilievi, preme osservare che le alternative agli accordi di adeguatezza presentano non pochi svantaggi, alcuni dei quali sono già stati menzionati nelle precedenti pagine.

Le *standard contractual clauses* sono tendenzialmente anelastiche, non potendo essere modificate dalle parti del contratto, e impongono dei limiti così stringenti in caso di subcontratto da non poter trovare applicazione ad alcune tipologie di contratti (es. contratti aventi ad oggetto i servizi di *cloud computing*) in cui il trasferimento dei dati personali è connaturato alla natura stessa del contratto.

Le *corporate binding rules*, d'altro canto, incontrano il limite della loro applicabilità esclusivamente ai trasferimenti di dati personali tra società del medesimo gruppo, non potendo essere estese ai rapporti con società terze. Peraltro, la necessità di una preventiva autorizzazione da parte dell'Autorità Garante determina una significativa espansione dei tempi, spesso difficilmente conciliabile con la rapidità dei traffici commerciali, e la necessità di redigere tali regole per il gruppo societario, in maniera analitica, destinando risorse umane a tale compito e ai rapporti con l'Autorità Garante.

Alla luce di tali riscontri, non può concludersi che, sebbene siano, sul piano dell'efficacia, alternativi ai *safe harbor*, legittimando gli scambi di dati personali tra Europa e Stati Uniti, *corporate binding rules* e *model contract clauses* non rappresentano dispositivi normativi in grado di fronteggiare l'alluvione scaturita dalla sentenza della Corte di Giustizia. Un'alluvione che è stata determinata dall'azzeramento immediato dell'originario *safe harbor agreement*, a partire dal momento della pubblicazione della sentenza, come precisato dal *Working Party* e dai Garanti nazionali[56].

[55] Sul punto, per più ampi rilievi, si rinvia a S. Sica, *Art. 1350. Degli atti che devono farsi per iscritto*, in *Comm. cod. civ.* diretto da F.D. Busnelli, Milano, 2003, 276 ss., che discorre, a proposito degli adempimenti richiesti dalla normativa privacy, di neoformalismo procedimentale.

[56] Cfr. lo *Statement* dell'Article 29 Working Party, 16 October 2015, 2; Garante per la protezione dei dati personali, provv. 22 ottobre 2015, *Trasferimento dati personali verso gli*

Le imprese si trovano – almeno fino al varo definitivo del *Privacy Shield* – a doversi raffrontare con un vuoto normativo che pregiudica il loro operato e che, teoricamente, rischia di paralizzare (o, quanto meno, di ritardare) i traffici commerciali tra Europa e Stati Uniti. Sebbene le istanze di tutela recepite dalla Corte di Giustizia appaiano assolutamente condivisibili e sebbene non si possa non rimarcare il lassismo, probabilmente voluto, degli Stati Uniti, che non hanno saputo fronteggiare adeguatamente l'emergenza PRISM e non hanno voluto ripensare il loro modello di sorveglianza massiva, non può non concludersi per la complessiva inadeguatezza degli strumenti alternativi sopravvissuti alla decisone dei giudici comunitari. Tali strumenti, difatti, non appaiono in grado di tamponare la mole degli scambi intercontinentali di dati personali e di supplire, neanche temporaneamente, al vuoto lasciato dall'annullamento dei *safe harbor*.

Abstract

The ECJ's ruling Schrems v. Data Protection Commissioner *has invalidated the EU-US Safe Harbor Agreement. The decision is the third step of the European Court of Justice – after the* Digital Ireland *and* Costeja Gonzales *cases – towards the acknowledgment of personal data protection as a fundamental right, pursuant to article 9 of the Treaty of Nice, and marks the rift between EU and US on the fair balance among surveillance systems and privacy laws. After the collapse of the Safe Harbor Agreement and before the implementation of the so-called Privacy Shield, binding corporate rules, for multinational organizations or groups of companies, and contract model clauses, in any other case, have been the sole compliant solutions for overseas transfers of personal data.*

USA: caducazione provvedimento del Garante del 10.10.2001 di riconoscimento dell'accordo sul c.d. «Safe Harbor», in *Gazz. Uff.*, n. 271 del 20 novembre 2015.