Trasferimento di dati personali verso paesi terzi: la Corte annulla il «Privacy Shield», amplia i poteri delle autorità di controllo e responsabilizza ulteriormente i *data exporters*

di Gianluca Bellomo

Title: Transfer of personal data to third countries: the Court cancels the "Privacy Shield", extends the powers of the National Data Protection Authorities and further empowers data exporters

Keywords: Regulation (EU) 2016/679; Privacy Shield; Adequacy Decision.

1. – Il trasferimento di dati personali verso paesi terzi rispetto all'UE rappresenta uno degli snodi cruciali, in un mondo globalizzato, dell'effettività di un diritto alla tutela dei dati personali che oggi non gode dei medesimi livelli di garanzia in tutto il mondo.

L'Unione da tempo sta lavorando all'interno del proprio ambito di competenza per realizzare un modello che cerchi di contrastare la preponderanza del potere delle multinazionali della tecnologia rispetto ai singoli utenti con riguardo al trattamento dei dati personali. In particolare, con l'avvento e l'affermarsi dell'Internet i più importanti soggetti del settore tecnologico, in quanto monopolisti di fatto su scala globale, possono imporre la cessione dei propri dati personali ai singoli utenti in cambio dell'accesso a servizi di vario genere e natura. Il modello europeo ormai da tempo cerca di garantire quel pieno diritto all'*autodeterminazione informativa* delle persone caro a Rodotà già venti anni or sono (cfr. S. Rodotà, *Discorso del prof. Rodotà di presentazione della "Relazione per l'anno 2000"*, reperibile in www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1335256) che consenta ai singoli di avere il controllo sull'uso dei propri dati personali. Tale modello regolatorio, consolidatosi sempre più nel tempo, a livello eurounitario ha raggiunto ad oggi la sua massima espressione con l'entrata in vigore del regolamento (UE) 679/2016 (Regolamento Generale sulla Protezione dei Dati personali o RGPD – in inglese GDPR), che ha abrogato e sostituito la precedente direttiva 95/46/CE, (su cui cfr., tra gli altri, almeno G. Finocchiaro (dir.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017; Id., *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019; L. Bolognino, E. Pelino, C. Bistolfi, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, Giappichelli, Tomo II, 2016; S. Sica, V. D'Antonio, G.M. Riccio, *La nuova disciplina europea della* privacy, Milano, Cedam-Wolters Kluwer, 2016; G.M. Riccio, G. Scorza, E. Belisario, (cur.), *GDPR e normativa Privacy. Commentario*, I ed., Milano, Wolters Kluwer, 2018; E. Gabrielli (dir.),

Delle persone, *Leggi collegate*, vol. II, in Commentario del Codice civile, 2019). Così, se da una parte a livello eurounitario sono stati preposti a garanzia del diritto alla protezione dei dati personali soggetti istituzionali (singoli Garanti nazionali e Comitato europeo dei garanti – EDPB), principi (es. di *minimizzazzione*, di *privacy by design* e *by defoult*, *di responsabilizzazione*, ecc), di istituti (anche introdotti per via giudiziaria, es. diritto all'oblio e alla deindicizzazione) e sanzioni amministrative dedicate (che possono raggiungere importi anche fino a 20 milioni di euro, o al 4% del fatturato globale annuo), nel tentativo di arginare proprio quel potere di acquisizione ormai massiva di dati personali e di trattamenti indesiderati sugli stessi, in particolare con riguardo alle grandi multinazionali del Web; dall'altra permangono forti criticità nell'ipotesi in cui i dati personali fuoriescono dallo spazio eurounitario rischiando di sfuggire di fatto dall'applicazione del modello europeo. Ciò proprio a causa della difficoltà nel garantire ai dati personali trasferiti in paesi terzi un livello di protezione sostanzialmente analogo a quello previsto nello spazio europeo dal quadro regolatorio vigente, con la conseguenza di assistere a forti compressioni di quel diritto alla tutela dei dati personali sancito direttamente nella Carta dei diritti dell'Unione europea all'art. 8.

Proprio per cercare di contrastare un possibile aggiramento delle garanzie previste dal RGPD a tutela dei dati personali trattati all'interno del territorio dell'Unione, il legislatore europeo ha previsto all'art. 44 un regime generale di trattamento dei dati personali. Secondo il «Principio generale per il trasferimento» recato dalla disposizione vige un divieto di trasferimento di dati personali dal territorio dell'UE verso paesi terzi, salvo che, almeno in prima approssimazione, nei paesi di destinazione: si abbia un livello sostanzialmente analogo di protezione del diritto alla tutela dei dati personali; o che, in ultima istanza, lo stesso interessato dia il consenso informato al trasferimento dei dati personali che lo riguardano con piena consapevolezza dei relativi rischi.

Il Regolamento stesso prevede che per quanto riguarda il livello minimo di garanzia del diritto alla tutela dei dati personali nel singolo paese terzo la valutazione possa essere effettuata o direttamente dalla Commissione Ue, con l'adozione di una apposita decisione di adeguatezza in esito a una approfondita analisi di molteplici fattori presenti nel paese di destinazione che possono incidere sull'effettività della tutela dei dati personali; o sulla base di accordi tra le parti (chi invia dall'UE e chi riceve i dati nel paese terzo) a clausole tipo, approvate anch'esse dalla Commissione, alle quali ricorrere per cercare di garantire detto livello minimo di adeguatezza degli standard di tutela accordati ai dati personali.

Nel 2015, con l'approvazione da parte della Commissione UE della decisione n. 2000/520 del 26 luglio 2000, quest'ultima aveva riconosciuto all'ordinamento USA proprio quel livello minimo necessario di adeguatezza nella protezione sufficiente a consentire il trasferimento di dati personali presso gli Stati Uniti.

Tuttavia, la Corte di giustizia dell'Unione europea con la successiva sentenza del 6 ottobre 2015, C-362/14, *Schrems* (*Schrems I*) ha annullato tale decisione, su ricorso presentato da uno studente austriaco, Maximilian Schrems, che nel 2013 aveva proposto denuncia nei confronti di *Facebook Ireland Limited* dando successivamente origine alla citata sentenza (su cui tra i molteplici commenti si segnala almeno R. Bifulco, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giurisprudenza costituzionale*, n. 1, 2016, 289-307; S. Crespi, *Il trasferimento dei dati personali UE in Stati terzi: dall'approdo sicuro allo Scudo UE/USA per la privacy*, in *Diritto pubblico comparato ed europeo*, fasc. 3, luglio-settembre 2016, 687-714; mentre da una prospettiva d'oltreoceano cfr. D. Bender, *Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective*, in *International Data Privacy Law*, vol. 6, n. 2, 2016, 117-138; Y. Padova, *The Safe Harbour is invalid: what tools remain for data transfers and what comes next?*, in *International Data Privacy Law*, vol. 6, n. 2, 2016, 139-

161; L. Determann, *Adequacy of data protection in the USA: myths and facts*, in *International Data Privacy Law*, vol. 6, n. 3, 2016, 244-250).

2. – Nella sentenza della Grande sezione della Corte di Lussemburgo che qui si osserva, la questione pregiudiziale origina dalla controversia tra la *Data Protection Commissioner* (Commissario per la protezione dei dati irlandese), *Facebook Ireland Ltd* e lo stesso, ormai famoso, sig. Maximillian Schrems della citata sentenza *Schrems I* (molteplici sono già i commenti ad oggi pubblicati sulla sentenza qui in esame tra i quali si segnalano almeno, R. Bifulco, *Il trasferimento dei dati personali nella sentenza Schrems II: dal contenuto essenziale al principio di proporzionalità e ritorno*, in *Diritto pubblico europeo rassegna online*, fasc. 2, 2020, 1-17; O. Pollicino, F. Resta, *Dati personali, perché la Corte di Giustizia ha annullato il «Privacy Shield»*, in *IlSole24Ore*, 20 luglio 2020, 1-3; O. Pollicino, *Diabolical Persistence: Thoughts on the Schrems II Decision*, in *VerfBlog*, 2020/7/25, reperibile in verfassungsblog.de/ diabolicalpersistence/; A. Chander, *Is Data Localization a Solution for Schrems II?*, in *Journal of International Economic Law*, n. 23, 2020, 771–784; J.X. Dhont, *Schrems II. The EU adequacy regime in existential crisis?*, in *M.J.E.C.L.*, vol. 26, n. 5, 2019, 597–601; S. Fantin, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems: AG Discusses the Validity of Standard Contractual Clauses and Raises Concerns over Privacy Shield*, in *E.D.P.L.*, vol. 6, n. 2, 2020, 325-331; Xavier Tracol, *"Schrems II": The return of the Privacy Shield*, in *C.L.S.R.*, n. 39, 2020, 1-11).

La sentenza prende le mosse da un processo avviato dallo studente nei confronti del Commissario per la protezione dei dati irlandese riguardo al trasferimento di dati personali da parte, ancora una volta, di *Facebook Ireland Ltd* a *Facebook Inc.* negli Stati Uniti, paese nel quale tali dati sono sottoposti a trattamento.

Dopo la sentenza *Schrems I*, alla luce di quanto statuito all'epoca dalla Corte di giustizia, seguirono nuove e complesse trattative tra Stati Uniti e Unione europea volte alla stipula di un accordo rispettoso dei rilievi mossi dal giudice di Lussemburgo relativamente al rispetto del quadro normativo in materia ed in particolare della direttiva 95/46/CE all'epoca dei fatti vigente. Il risultato del confronto fu rappresentato dal «*Privacy Shield*» o «scudo per la privacy» che veniva adottato dalla Commissione con la decisione (UE) 2016/1250 sancendo, in caso di rispetto delle condizioni previste all'interno dello stesso, l'adeguatezza della protezione dei dati personali nel trasferimento di dati personali verso gli USA.

A seguito della nuova decisione della Commissione, il sig. Schrems rilevava la sussistenza dell'obbligo per *Facebook Inc.*, con sede in USA, di rendere disponibili alle autorità statunitensi (tra le quali la *National Security Agency* e il *Federal Bureau of Investigation*) i dati in proprio possesso per le attività di intelligence a queste affidate dall'ordinamento di appartenenza.

Gli approfondimenti attuati dal Commissario irlandese evidenziavano la sussistenza dei rischi rappresentati dal ricorrente e rilevavano in particolare che le clausole tipo di protezione dei dati personali, approvate dalla decisione di esecuzione (UE) 2016/2297, che aveva modificato la precedente decisione, sempre della Commissione, 2010/87/UE del 5 febbraio 2010 ed emanata anch'essa alla luce dell'allora vigente direttiva 95/46/CE, non fornivano una protezione adeguata ai cittadini dell'UE proprio in quanto atti con natura privatistica e di per sé inidonei a vincolare le autorità pubbliche statunitensi.

Così, partendo da tale ultimo presupposto e dai principi della decisione *Schrems I*, il Commissario irlandese si rivolgeva ancora una volta all'*High Court* (Alta Corte irlandese) affinché proponesse una serie di questioni pregiudiziali al giudice europeo. Cosa effettivamente poi verificatasi il 31 maggio 2018 con le numerose questioni sollevate e dalle quali è poi scaturita la sentenza qui in commento.

Più in particolare l'Alta Corte irlandese ha chiesto al giudice di Lussemburgo di pronunciarsi su ben undici questioni pregiudiziali così individuate e raggruppate dalla stessa Corte di Giustizia in base a condivisibili criteri di omogeneità:

1) con la prima questione, se il RGPD si applichi al trasferimento dei dati personali tra operatori economici qualora vi sia la possibilità che essi siano trattati da un paese terzo per fini di sicurezza pubblica, di difesa e di sicurezza dello Stato (punto 80);
2) con la seconda, terza e sesta questione, quale livello di protezione sia richiesto dall'art. 46, par. 1 e par. 1 lett. c), del Regolamento nel caso di trasferimento dei dati personali verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati; e quali siano in detto ambito gli elementi da prendere in considerazione ai fini della garanzia nella determinazione di un adeguato livello di protezione (punto 90);
3) con l'ottava questione, se l'autorità di controllo competente sia tenuta a sospendere o vietare un trasferimento di dati personali effettuato sulla base di clausole contrattuali tipo adottate dalla Commissione nel caso in cui suddetta autorità ritenga che tali clausole non sono o non possono essere rispettate nel paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione non possa essere garantita, oppure nel senso che l'esercizio di tali poteri sia limitato ad ipotesi eccezionali (punto 106);
4) con la settima e la undicesima questione, se la decisione CPT sia valida alla luce degli artt. 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea (punto 122);
5) con le rimanenti, se sostanzialmente la decisione «scudo per la privacy» garantisca un livello adeguato di protezione dei dati personali trasferiti dall'Unione verso gli Stati Uniti ai sensi dell'art. 45 RGPD (punto 160).

3. – La Corte di Giustizia, risolta preliminarmente in senso positivo la questione relativa alla ricevibilità della domanda di pronuncia pregiudiziale che era stata inizialmente sollevata da *Facebook Ireland* e dai governi tedesco e inglese, passa all'analisi della prima questione pregiudiziale, relativa all'applicabilità dell'RGPD al trasferimento dei dati personali tra operatori economici qualora vi sia la possibilità che i dati siano trattati da un paese terzo per fini di sicurezza pubblica, di difesa e di sicurezza dello Stato.

La questione viene rapidamente risolta dalla Corte in senso positivo sia alla luce dell'ambito di applicazione del RGPD perimetrato dall'art. 2, par. 1 (*contra* Avv. Generale punto 104 delle Conclusioni), sia della nozione di «trattamento», prevista all'art. 4, par. 1, punto 2) del medesimo Regolamento. Ed ancora in base alla presenza specifica accordata dal Legislatore europeo all'interno di quest'ultimo dal Capo V dedicato proprio al trasferimento di dati personali verso paesi terzi e dal quale se ne può ulteriormente presumere, appunto, l'operatività. La Corte, peraltro, non ritiene configurabile nessuna delle esimenti previste dal medesimo art. 2 par. 2, in quanto il trasferimento dei dati viene effettuato tra due soggetti privati (*Facebook Ireland* e *Facebook Inc.*) e non da uno Stato o da una persona fisica nell'ambito di un'attività strettamente personale o domestica (punto 85 della Sentenza).

4. – La seconda, terza e sesta questione attengono al livello di protezione richiesto dall'art. 46, par. 1 e par. 1 lett. c), del Regolamento nel caso di trasferimento dei dati personali verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati, e agli elementi da considerare ai fini della garanzia del raggiungimento di un adeguato livello di protezione. La Corte decide di affrontare le tre questioni congiuntamente.

La Corte, in piena sintonia con lo spirito funzionalista che pervade il RGPD, rileva preliminarmente che tali questioni andranno indagate partendo dall'assunto generale previsto nel Capo V del Regolamento stesso ed in particolare alla luce dell'art. 44 che dispone che, indipendentemente dalle opzioni di legittimità previste in tale Capo volte a consentire il trasferimento verso paesi terzi di dati personali, queste andranno comunque orientate in sede applicativa ad assicurare un livello di protezione nel trattamento dei dati delle persone fisiche sostanzialmente analogo a quello previsto dal RGPD (punto 92 della Sentenza) alla luce della Carta. Così, in caso di assenza di una decisione di adeguatezza approvata da parte della Commissione Ue ai sensi dell'art. 45, par. 3, il titolare potrà trasferire dati in paesi terzi solo in presenza di «garanzie adeguate», «diritti azionabili» e «mezzi di ricorso effettivi». Tali elementi potranno essere oggettivizzati attraverso l'inserimento di clausole tipo di protezione dei dati adottate dalla Commissione, ma essi andranno comunque valutati dai singoli titolari alla luce dell'effettivo contesto in cui dette clausole dovranno essere applicate nei paesi di destinazione dei dati personali. Detto passaggio rappresenta un ulteriore passo in avanti rispetto alla precedente sentenza *Schrems I.* Oltre alle singole clausole contrattuali stabilite tra il titolare o il responsabile del trattamento e il destinatario dei dati nel paese terzo, la decisione impone una complessa valutazione circa tutti gli altri elementi di contesto legati al rischio paese specifico ed in particolare, ma non solo, agli elementi rilevanti del sistema giuridico così come richiamati all'art. 45 par. 2 del Regolamento (Stato di diritto, rispetto dei diritti umani e delle libertà fondamentali, legislazione generale e settoriale di riferimento, analisi della giurisprudenza nonché diritti effettivi e azionabili degli interessati e vie di ricorso interne amministrativa e giudiziali accessibili agli interessati i cui dati personali sono oggetto di trasferimento, nonché esistenza e reale funzionamento di una o più autorità di controllo indipendenti, impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione). In tale valutazione l'unica bussola dovrà essere rappresentata dalla Carta dei diritti fondamentali dell'Ue, non già dai diritti garantiti negli Stati membri (punto 101 della Sentenza), né da quelli sanciti dalla CEDU (punto 98 della Sentenza).

5. – Con l'ottava questione, la Corte irlandese chiede se l'autorità di controllo competente sia tenuta a sospendere o vietare un trasferimento di dati personali effettuato sulla base di clausole contrattuali tipo adottate dalla Commissione, nel caso in cui l'autorità ritenga che tali clausole non siano o non possano essere di fatto rispettate nel paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione non possa essere garantita (ma anche nel senso che l'esercizio di tali poteri sia limitato ad ipotesi eccezionali).

Con riguardo a questo specifico punto va rilevato, come già ricordato, che il trasferimento di dati personali verso paesi terzi, tra le varie basi giuridiche sulle quali può fondarsi, può essere collegato sia a una decisione di adeguatezza, approvata dalla Commissione, del quadro giuridico di un paese terzo alla disciplina prevista dal RGPD, ma anche, in assenza della prima, su clausole tipo, anch'esse approvate dalla Commissione, che le parti in causa possono decidere di utilizzare nei rispettivi accordi di trasferimento dei dati. Le due basi giuridiche non sono uguali. Infatti la prima si fonda su di una valutazione preventiva circa il livello di protezione dei dati personali, conseguente ad una analisi complessiva del quadro giuridico esistente nel paese che, una volta ritenuto idoneo dalla Commissione, di fatto dovrebbe garantire sufficientemente gli interessati coinvolti e conseguentemente autorizzare il relativo trasferimento. La seconda, che invece prevede il ricorso alle clausole tipo, cerca di fornire uno strumento con portata limitata alle parti e non a carattere generale, ma che comunque miri a garantire il medesimo risultato. Va rilevato, però, che la seconda base giuridica opera attraverso meccanismi di tipo sostanzialmente privatistico e soprattutto

alla luce delle differenti situazioni di contesto estremamente variabili, da paese a paese e da situazione a situazione, nelle quali avvengono i relativi trattamenti.

Alla luce di quanto appena richiamato, quindi, dovrebbe risultare evidente quanto argomentato dalla Corte già in *Scherms I* e cioè che in presenza di decisioni di adeguatezza i singoli Stati membri ed i rispettivi organi interni, tra cui le singole autorità di controllo, non potranno adottare misure contrarie a tale decisione (punto 118 della Sentenza). Diversamente, infatti, si produrrebbe una netta differenziazione dei regimi di circolazione dei dati esistenti tra i vari paesi membri, in riflesso ai singoli orientamenti assunti dalle differenti autorità interne. In caso di presunta lesione dei diritti degli interessati, questi ultimi comunque potranno ricorrere alle singole autorità di controllo nazionali che però, ove dovessero ravvisare delle criticità circa la decisione di adeguatezza approvata dalla Commissione, dovranno seguire la via del ricorso di fronte ai singoli giudici dei rispettivi Paesi membri che, ove siano convinti delle ragioni poste alla base del ricorso da parte delle singole autorità, potrebbero proporre rinvio pregiudiziale volto alla verifica della validità della decisione di adeguatezza emanata dalla Commissione.

Al contrario, nell'ipotesi proposta con l'ottava questione, la base giuridica oggetto di valutazione dell'effettiva idoneità a garantire un sufficiente livello di tutela dei dati personali trasferiti in un paese terzo è rappresentata dalle clausole tipo di adeguatezza, anch'esse approvate dalla Commissione. In questo caso il risultato che raggiunge la Corte però è opposto. Infatti viene riconosciuto alle singole autorità di controllo il potere di «sospendere o vietare un trasferimento di dati personali verso un paese terzo qualora ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le clausole tipo di protezione dei dati personali non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione non possa essere garantita con altri mezzi» (punto 113 della Sentenza). Tale potere, riconosciuto alle singole autorità di controllo, se, da una parte, consente di aumentare i margini di flessibilità del sistema consentendo di volta in volta alle stesse di tenere conto del contesto di operatività di dette clausole, aumentando parallelamente i margini di discrezionalità delle autorità stesse; dall'altra rischia di far dipendere dalle rispettive singole sensibilità il livello di ammissibilità o meno nel trasferimento dei dati verso paesi terzi, rischiando in definitiva di creare un pericoloso *vulnus* alla omogeneità applicativa del Regolamento.

Tale conclusione discende, come rilevato dalla stessa Corte, dall'impossibilità di limitare materialmente da parte della Commissione i poteri di controllo delle autorità le quali sono le uniche autorità indipendenti esplicitamente preposte dalla Carta dei diritti fondamentali dell'Unione europea (art. 8, par. 3) alla tutela di un diritto fondamentale.

6. – Con la settima e l'undicesima questione, così come individuate dalla Corte, a questa viene chiesto di pronunciarsi sulla validità della decisione CPT, con la quale sono state adottate dalla Commissione le clausole contrattuali tipo sulla base delle quali vengono di fatto autorizzati alcuni trattamenti di dati personali consistenti nell'invio degli stessi in paesi terzi, alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Ue. La Corte è sollecitata, in particolare, a verificare l'idoneità di tali clausole a garantire adeguati livelli di protezione nel trattamento dei dati personali nonostante esse vincolino solo le parti e non le autorità dei paesi terzi coinvolti.

I giudici di Lussemburgo, ripercorrendo la distinzione che il Regolamento RGPD fa tra *decisione di adeguatezza*, *ex* art. 45, e *clausole di protezione tipo*, *ex* art. 46, rileva che nel primo caso è onere della Commissione verificare con un esame complesso l'effettivo livello di sostanziale adeguatezza del livello di tutela dei dati personali all'interno del singolo paese; nel secondo, invece, la Commissione si limita a verificare

che in astratto le clausole di protezione tipo possano condurre al medesimo risultato in termini di garanzie prodotte rispetto al modello europeo, ma solo tra le parti e non con riferimento al contesto di operatività delle stesse e alle specifiche caratteristiche dei singoli paesi terzi nei quali dette clausole saranno successivamente impiegate. Tale onere spetterà alle parti quindi e non alla Commissione (punto 130 della Sentenza).

Resta così in capo al titolare, in collaborazione con il destinatario nel paese terzo, valutare di volta in volta se in base al contesto di operatività delle clausole queste siano sufficienti o meno a garantire il livello di adeguatezza minimo previsto dal RGPD. Laddove tale standard non sia raggiunto, è onere delle parti prevedere ulteriori clausole o garanzie supplementari (cosi come previsto ai *Considerando* 109, 108 e 114 del Regolamento richiamati dalla Sentenza) funzionali a elevare il livello di tutela, o, diversamente, sospendere tale trattamento. In caso di inerzia delle parti, le singole autorità di controllo dei paesi membri di invio dei dati godono in ogni caso di poteri di inibizione del trasferimento per carenza di garanzie adeguate.

La *decisone di adeguatezza*, pertanto, resta comunque valida alla luce della presenza di meccanismi efficaci di protezione dei dati personali trasferiti in forza di tali clausole e della possibilità concretamente attuabile di sospendere o vietare detti trasferimenti in caso di violazioni di tali clausole o di impossibilità a rispettarle (punto 137 della Sentenza). Ancora una volta quindi la direzione intrapresa dalla Corte ricalca quella del RGPD nella direzione di una responsabilizzazione del titolare e del responsabile del trattamento, concedendo ampi margini di discrezionalità nella valutazione di elementi che consentano di decidere se materialmente o meno venga garantito o sia possibile garantire quel livello minimo di adeguatezza richiesto dalla normativa. Peraltro tale orientamento sembra ad oggi l'unico che consenta la ricerca di un bilanciamento materiale efficiente tra tutela dei dati personali e libertà di circolazione di detti dati in ogni singolo caso, e una eventuale verifica da parte delle singole autorità di controllo.

7. – Con la quarta, quinta, nona e decima questione viene chiesto al giudice di Lussemburgo se la decisione "scudo per la privacy" garantisce un livello adeguato di protezione dei dati personali trasferiti dall'Unione verso gli Stati Uniti ai sensi dell'art. 45 RGPD, e più in dettaglio se il trasferimento di dati personali verso detto paese avvenuto sulla base di clausole di protezione tipo previste nell'allegato alla decisione CPT violi i diritti previsti agli artt. 7, 8 e 47 della Carta dei diritti fondamentali dell'Ue.

Le questioni poste richiedono anzitutto di chiarire se e in che misura eventuali ingerenze nei diritti fondamentali delle persone fisiche interessate dai trattamenti oggetto di trasferimento verso detto paese possano essere limitati. La Corte, dopo ampia analisi dei programmi di sorveglianza statunitensi PRISM e UPSTREAM basati sull'art. 702 FISA (*Foraign Intelligence Survillance Act*) del decreto presidenziale americano (*Executive Order*) n. 12333 e della direttiva (*Presidential Policy Directive*) PPD-28, sempre a firma del Presidente degli Stati Uniti, che di fatto non consentono di garantire i requisiti minimi di proporzionalità nella limitazione dei diritti e delle libertà degli interessati, osserva la conseguente violazione dell'art. 52, par. 1, seconda frase della Carta e cioè il superamento delle condizioni e dei limiti previsti dai Trattati.

Ai fini della valutazione della sussistenza dei requisiti di adeguatezza richiamati, la Corte inoltre rileva, in modo cruciale, la violazione per i soggetti statunitensi interessati al diritto a un ricorso giudiziario effettivo (punto 187 della Sentenza).

Così la Corte alla luce di tutte le considerazioni esposte conclude che negli USA non sussiste sostanzialmente un livello di protezione equivalente a quello garantito dall'art. 47 della Carta dei diritti fondamentali dell'Unione europea (punto 191 della Sentenza).

Del resto, non riesce a convincere la Corte neppure la lodevole iniziativa del Presidente Obama con la PPD-28, che all'art. 4 lett. d) ha previsto l'istituzione della figura di un apposito Mediatore nominato dal Segretario di Stato individuato nella persona del *Primo coordinatore della diplomazia internazionale per le tecnologie dell'informazione*. Sul punto i giudici di Lussemburgo e lo stesso Avvocato generale esprimono forti dubbi, con riguardo all'effettiva indipendenza dell'organo e alla reale idoneità delle funzioni attribuitegli a incidere materialmente sui servizi di intelligence americani, e più in generale a colmare quelle gravi lacune presenti nell'ordinamento americano in termini di equivalenza sostanziale nella tutela dei dati personali rispetto al modello europeo.

Alla luce di quanto sopra, quindi, la Corte dichiara invalida la decisione della Commissione «scudo per la privacy» avendo questi violato l'art. 45, par. 1 del RGPD, alla luce degli artt. 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea.

8. – Per concludere sia consentito accennare brevemente ad alcune questioni strettamente collegate tra di loro che pure vengono in rilievo con riguardo alla sentenza qui in commento.

La prima attiene al ricordato maggiore livello di responsabilizzazione che di fatto la sentenza riversa su chi esporta i dati personali e sulle autorità di controllo, in particolare quando la base giuridica di trasferimento dei dati è rappresentata dall'impiego di clausole contrattuali tipo. Come è stato notato questo rappresenta «un indirizzo … teso a far corrispondere a sempre più rilevanti "poteri privati" altrettanti oneri di carattere, talora, quasi pubblicistico», e ancora «la protezione dei dati appare sempre meno una mera questione "privatistica" e, sempre più, un tema di straordinaria rilevanza costituzionalistica, su cui si misura la tenuta della democrazia. Insomma, un passo indietro dell'idea di monetizzazione del dato, ed un passo avanti di quella, antitetica, del dato personale come base (indisponibile) del patrimonio costituzionale europeo» (su cui cfr. O. Pollicino, F. Resta, op. cit., 2).

La seconda riguarda il confronto in atto a livello globale tra i differenti modelli di tutela esistenti. Infatti, se il trasferimento di dati personali all'interno dell'Ue è sostanzialmente libero (dandosi per assunto che i soggetti coinvolti applichino correttamente le prescrizioni del RGPD), quello verso i Paesi terzi, in assenza di idonee garanzie, e cioè di un livello di tutela dei dati personali che rispetti almeno gli standard minimi di protezione previsti dal modello europeo, è, come visto, generalmente vietato. Così la normativa prevede differenti livelli di deroga al generale divieto di trasferimento, modulati sul presupposto che più il paese terzo si adegua sostanzialmente e non solo formalmente al nucleo della disciplina prevista a livello europeo e minori saranno i vincoli nel trasferimento dei dati coinvolti, ma con ogni probabilità anche dei relativi costi. Sul punto va però rilevato che ove il modello europeo non dovesse trovare, almeno nei principi fondamentali, la diffusione sperata (su cui cfr. C. D'Cunha, *L'UE può farcela*, in Aa.Vv., *"Privacy 2030": Una nuova visione per l'Europa, Un manifesto per il nostro futuro. Il manifesto del pensiero di Giovanni Buttarelli*, IAPP e Garante per la protezione dei dati personali italiano, 27, reperibile in www.garanteprivacy.it/ web/ guest/ home/ docweb/ -/ docweb-display/ docweb/ 9456977), il rischio opposto potrebbe essere quello che la normativa adottata in Ue per la tutela dei dati personali si possa trasformare in un *unicum* nello spazio globale che porti all'isolamento dell'Unione e quindi a una contestuale diminuzione dei suoi livelli di competitività nei regionalismi macroeconomici mondiali in continua trasformazione. Ma si correrebbe il rischio anche di andare verso una frammentazione di fatto delle reti di comunicazione globale, rese possibili dalle comunicazioni elettroniche, differenziate sulla base di presunti maggiori o minori livelli di adeguatezza dei differenti regimi

statali di tutela dei dati personali presenti nei vari paesi terzi (su cui cfr. A. Chander, op cit., 14).

In questa problematica interconnessione globale, il ruolo della Corte di giustizia, come si evince anche dalla sentenza qui in commento, diventa centrale, per la sua idoneità a incidere in modo rilevante sulla conformazione materiale del modello europeo di tutela dei dati e sui suoi limiti di applicabilità, così come già accaduto ad esempio in materia di «diritto all'oblio» e nello specifico con riguardo al «diritto alla deindicizzazione» (su cui sia consentito il rinvio in questa Rivista a G. Bellomo, *"Diritto all'oblio" e portata territoriale del "diritto alla deindicizzazione": la Corte ridisegna i confini applicativi*, n. 4, 2019). La centralità della Corte è avvalorata anche dal e nel rapporto con i Garanti nazionali per la protezione dei dati personali, sui quali la prima fa "migrare" pezzi sempre maggiori di sovranità materiale nella garanzia del diritto fondamentale alla tutela dei dati personali. Di questa continua dialettica istituzionale tra la Corte, i Garanti nazionali e il Comitato europeo per la protezione dei dati (EDPB) tesa a implementare il difficile bilanciamento tra effettività della tutela dei dati personali e libera circolazione dei dati evitando eccessive distorsioni del mercato, è prova l'intervento tenuto da ultimo dall'EDPB l'11 novembre 2020, durante la sua 41esima sessione plenaria. In risposta alla sentenza qui in commento, infatti, il Comitato ha messo in consultazione pubblica alcune raccomandazioni («*Recommendations 1/2020 on measures that supplement transfers tools to ensure compliance with the EU level of protection of personal data*») relative alle misure che integrano gli strumenti di trasferimento dei dati per garantire il rispetto del livello Ue di protezione dei dati personali, nonché sulle cosiddette «garanzie essenziali europee» in rapporto alle misure di sorveglianza. Ciò allo scopo di fornire alcune prime risposte operative ai *data exporters* nell'attuazione di adeguate misure supplementari volte a raggiungere quel livello minimo di protezione *sostanzialmente equivalente* che consenta, sia di trasferire i dati personali verso paesi terzi, sia di avere un'applicazione coerente del RGPD e della sentenza qui in parola all'interno dello Spazio Economico Europeo (SEE).

Gianluca Bellomo
Dipartimento di Scienze Giuridiche e Sociali,
Università degli Studi "G. d'Annunzio" – Chieti/Pescara
gianluca.bellomo@unich.it