IL TRASFERIMENTO DEI DATI PERSONALI NELLA SENTENZA SCHREMS II: DAL CONTENUTO ESSENZIALE AL PRINCIPIO DI PROPORZIONALITÀ E RITORNO[*].

di Raffaele Bifulco[**]

1. Introduzione.

Nel 2015 la Corte di giustizia aveva annullato la decisione della Commissione europea nota come "approdo sicuro" (*Safe Harbour*)[1]. Con tale decisione la Commissione aveva espresso una valutazione di adeguatezza del diritto statunitense in materia di protezione dei dati nell'assicurare un livello di protezione dei dati personali equivalente a quello che richiede il diritto dell'Unione europea. A provocare la sentenza fu uno studente austriaco, che, alla luce delle rivelazioni di E.Snowden sui sistemi di sorveglianza elettronica statunitensi, chiedeva al Commissario per la protezione dei dati irlandese di impedire che Facebook trasferisse i propri dati dall'Irlanda verso la casa madre ubicata negli Stati uniti. Quello stesso studente, Maximilian Schrems, è all'origine della sentenza della Corte di giustizia, cui sono dedicate queste pagine. La nuova sentenza è sostanzialmente in linea di continuità con il precedente del 2015 ed è coerente anche con le più recenti sentenze della Corte in materia di protezione dei dati, evocate nel corso della decisione. Tuttavia essa contiene anche elementi di novità riguardanti, in particolare, il rapporto tra la decisione di adeguatezza della Commissione e le clausole tipo di protezione e il ruolo delle autorità di

[*] *Pubblicazione destinata agli scritti in onore di Mario Bertolissi*.
[**] Professore ordinario di Diritto costituzionale – Università LUISS "Guido Carli".
[1] Corte di giustizia dell'Unione europea, 6 ottobre 2015, C-362/14, *Schrems* (da ora sentenza Schrems I). Per un commento sia permesso rinviare a R.Bifulco, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giurisprudenza costituzionale*, 1, 2016, 289-307

controllo che viene ulteriormente rafforzato. Rivela interesse anche per il parametro del giudizio che in essa viene utilizzato. Nel 2015 il parametro era la direttiva 95/46, oggi esso è divenuto il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (da ora anche il Regolamento o RGPD)[2].

Anche in questo caso la Corte annulla la nuova decisione di adeguatezza della Commissione, nota come "scudo per la privacy", riaprendo così la questione di una adeguata regolamentazione del regime di trasferimento dei dati verso un paese terzo. Ma questo è forse l'aspetto più appariscente, per così dire, della sentenza. La pronuncia della Corte interviene infatti su questioni nuove di notevole rilevanza per il trattamento dei dati personali, enfatizzando in particolare il ruolo dei titolari dei dati personali e dei destinatari del trasferimento dei dati nel paese terzo. Si tratta di un serio richiamo alle responsabilità che i grandi *players* di Internet e della gestione dei dati devono assumersi se vogliono essere presenti sul mercato europeo. Chiamati dalla decisione a valutare attentamente le caratteristiche degli ordinamenti giuridici di destinazione dei dati, l'adeguatezza di questi ordinamenti a garantire un livello di tutela dei dati personali omogeneo agli standard europei, l'affidabilità dei destinatari del trasferimento, i titolari di dati personali che vogliano trasferirli al di fuori dell'Unione dovranno essere non solo attrezzati ma consapevoli delle responsabilità cui vanno incontro. E il compito non sarà dei più facili, soprattutto se i destinatari dovessero trovarsi in ordinamenti poco trasparenti e restii a svelare le proprie tecniche di sorveglianza elettronica. Insieme ai titolari dei dati personali, la decisione pone in rilievo il ruolo che le autorità di controllo (da noi il garante per la privacy) devono assumersi nel valutare l'operato dei titolari dei dati personali in caso di trasferimento degli stessi verso paesi terzi. A dirla tutta, la sentenza in commento potrebbe addirittura essere all'origine di rischi di una frammentazione della tutela o, meglio ancora, di una tutela a macchia di leopardo, legata alle specificità ordinamentali e alla maggiore sensibilità di qualche autorità di controllo di uno Stato membro rispetto ad altre.

La sentenza in commento va quindi ben oltre la pur importante questione del trasferimento

[2] In verità, la domanda di pronuncia pregiudiziale fa ancora riferimento alle disposizioni della direttiva 95/46 che, però, nel corso del complesso giudizio principale, è stata abrogata e sostituita dal RGPD. Poiché il Commissario irlandese non aveva ancora adottato una decisione definitiva sulla denuncia di M. Schrems al momento dell'entrata in vigore del RGPD, e cioè il 25 maggio 2018, la Corte ha deciso di rispondere alle questioni tenendo presente le disposizioni del RGPD e non quelle della direttiva 95/46 (punti 77 e 78 della sentenza).

dei dati verso gli Stati Uniti. Come si mostrerà più nel dettaglio, la decisione Schrems II ha un rilievo di politica transnazionale del diritto che oltrepassa il caso deciso, poiché essa innalza decisamente l'asticella del livello di tutela che tutti coloro che sono attivi nel mercato europeo devono poter superare se non vogliono essere eliminati da questa importantissima fetta di mercato.

Ora la palla torna alla Commissione, che dovrà mettersi al lavoro per trovare un nuovo compromesso con gli Stati Uniti. Le due sentenze Schrems offrono direttive abbastanza chiare alla Commissione, che non dovrebbe più incorrere in concessioni pericolose agli Stati Uniti (come, ad esempio, la prevalenza dei motivi di sicurezza e di difesa nazionale, bocciata per ben due volte dalla Corte di giustizia). E forse dovrebbero essere cercate nuove soluzioni da parte della Commissione e degli Stati Uniti rispetto a quelle percorse fino ad ora senza grande successo. La strada passa, come si vedrà, attraverso la cruna del diritto fondamentale a un ricorso effettivo.

2. I fatti di causa.

La sentenza origina da un processo avviato da Maximilian Schrems contro il Commissario per la protezione dei dati irlandese relativamente al trasferimento dei dati effettuato da Facebook Ireland verso la casa madre (Facebook Inc.) ubicata negli Stati Uniti, dove tali dati vengono sottoposti a trattamento. Schrems aveva già chiesto nel 2013 al Commissario di vietare a Facebook di trasferire i dati in suo possesso verso gli Stati Uniti e il rigetto della sua denuncia fu all'origine, come si è detto, della sentenza Schrems I, con la quale la Corte aveva dichiarato invalida la decisione 2000/520 della Commissione secondo la quale gli Stati Uniti garantivano un livello adeguato di protezione dei dati. A seguito di tale sentenza l'Unione europea e gli Stati Uniti hanno condotto nuove e non facili trattative per trovare un assetto della disciplina del trasferimento dei dati capace di superare le obiezioni della Corte di giustizia. Raggiunto un nuovo compromesso (noto come 'scudo per la privacy'), la Commissione ha adottato la decisione di esecuzione (UE) 2016/1250 sull'adeguatezza della protezione offerta dal nuovo regime. Si noterà che anche questa decisione viene assunta vigente ancora la direttiva 95/46.

Schrems ha così riformulato la propria denuncia, evidenziando in particolare l'obbligo in

capo a Facebook Inc. di mettere a disposizione delle autorità statunitensi (tra cui la *National Security Agency* e il *Federal Bureau of Investigation*) i dati in possesso di Facebook. L'indagine avviata dal Commissario irlandese confermava i rischi evidenziati da Schrems, osservando in particolare che le clausole tipo di protezione dei dati contenuti nella decisione CPT [3] non erano idonee a garantire i dati personali dei cittadini europei, in quanto esse non vincolavano le autorità statunitensi. È su questa base, e ovviamente sulla base del precedente costituito da Schrems I, che il Commissario si è rivolto nuovamente all'*High Court* irlandese, la quale, il 31 maggio 2018, ha rivolto alla Corte di giustizia l'articolato rinvio pregiudiziale, all'origine della sentenza in commento.

Le questioni pregiudiziali sono sintetizzate dalla Corte nella maniera seguente: 1) 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) quale sia il livello di protezione richiesto dall'art.46 del Regolamento nel caso di trasferimento dei dati personali verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati (punto 90); 3) se l'autorità di controllo competente sia tenuta a sospendere o proibire il trasferimento dei 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 (punto 106); 4) 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) se la decisione "scudo per la privacy" garantisca un livello adeguato di protezione dei dati personali ai sensi dell'art. 45 RGPD (punto 160).

3. Sicurezza pubblica e trasferimento dei dati.

La prima questione di rilievo risolta dalla Corte riguarda l'applicabilità del Regolamento ai casi di trasferimento dei dati personali verso un paese terzo nel quale tali dati possano

[3] La decisione CPT (decisione di esecuzione (UE) 2016/2297) ha modificato la precedente decisione 2010/87/UE della Commissione del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46.

essere trattati dalle autorità del paese medesimo a fini di sicurezza, di difesa e di sicurezza dello Stato.

Le obiezioni in senso contrario delle parti costituite non erano poche. Soprattutto il giudice del rinvio chiedeva se l'art.4, par.2, TUE, secondo cui all'interno dell'UE la sicurezza nazionale resta di esclusiva competenza degli Stati membri, potesse rappresentare una base per la non applicazione del RGPD alla fattispecie concreta, in cui il trasferimento dei dati personali può portare al trattamento degli stessi da parte delle autorità del paese terzo a fini di sicurezza pubblica, di difesa e di sicurezza dello Stato. La Corte ritiene che la disposizione del TUE non sia pertinente.

È il concetto di trattamento per come sviluppato all'interno degli artt. 2 e 4 del Regolamento che porta a tale conclusione. Infatti, poiché l'art. 4, par. 2, del Regolamento non distingue le operazioni di trattamento a seconda che siano realizzate all'interno dell'Unione o presentino un nesso con un paese terzo, la Corte può sostenere che il trasferimento di dati personali da uno Stato membro verso un paese terzo costituisce trattamento ai sensi dell'art. 4 Reg., trattamento al quale il Regolamento si applica in forza dell'art. 2, par.1 (punto 83) (ma in senso diverso era andato l'Avvocato generale: cfr. punto 104 delle sue conclusioni). La Corte ritiene peraltro che la disciplina specifica del trasferimento dei dati non possa farsi rientrare nei casi di espressa esclusione del Regolamento previsti dall'art.2, par.2, del Regolamento (punto 85).

4. Quale livello di protezione per il trasferimento dei dati?

Seguendo le domande del giudice irlandese, la Corte di Lussemburgo affronta poi la questione del livello di protezione richiesto dall'art. 46 per il caso di un trasferimento di dati personali verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati.

A tale proposito è bene chiarire che il capo V del Regolamento contiene due diverse ipotesi normative, quella prevista dall'art. 45 del trasferimento realizzato sulla base di una decisione di adeguatezza adottata dalla Commissione che attesti che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo garantiscono un livello di protezione adeguato e quella prevista dall'art. 46 per il caso in cui la decisione della

Commissione non sia stata adottata, con la conseguenza che il titolare del trattamento può trasferire i dati personali verso un paese terzo solo se ha fornito adeguate garanzie e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Su entrambe le ipotesi normative sovrasta il principio espresso dall'art. 44 in base al quale le disposizioni del capo V mirano ad assicurare che il livello di protezione delle persone fisiche garantito dal Regolamento non sia pregiudicato. Questa precisazione della Corte è di notevole interesse poiché l'equivalenza sostanziale da essa stabilita si dovrà applicare a tutti gli strumenti di trasferimento previsti dall'art. 46 Reg.

Ciò chiarito in via preliminare, conviene osservare che la Corte riprende un punto che aveva già affrontato in Schrems I, vale a dire che il livello di protezione adeguato di cui si ragiona nell'art.45 Reg. va interpretato «nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali *sostanzialmente equivalente* a quello garantito all'interno dell'Unione in forza di tale regolamento, letto alla luce della Carta».

La novità ulteriore sta nel fatto che tale equivalenza va garantita anche nel caso in cui il trasferimento dei dati non avvenga sulla base di una decisione della Commissione, bensì sulla base di clausole tipo di protezione dei dati, previste dall'art.46, par.2, lett. *c)* (punto 96). Nel dire ciò, la Corte segue esplicitamente l'opinione dell'Avvocato generale (par. 115 delle conclusioni).

Tale livello di protezione sostanzialmente equivalente deve essere inoltre determinato in base alle disposizioni del Regolamento, lette alla luce dei diritti fondamentali garantiti dalla Carta dei diritti fondamentali dell'Unione europea, con esclusione del diritto degli Stati membri come eventuale parametro (punto 101).

Al giudice del rinvio che chiede di sapere quali elementi prendere in considerazione per determinare l'adeguatezza del livello di protezione assicurato dalle clausole tipo, la Corte risponde appoggiandosi sul dato letterale del Regolamento che, all'art. 46, par.1, precisa che gli interessati devono godere di garanzie adeguate e disporre di diritti azionabili e mezzi di ricorso effettivi. E la valutazione, osserva la Corte, andrà fatta prendendo in considerazione sia le clausole tipo sia gli elementi rilevanti del sistema giuridico del paese terzo, con particolare riguardo agli elementi che prevede l'art. 45, par.2, Reg., come indici di adeguatezza (in sintesi lo Stato di diritto, la presenza di autorità di controllo indipendenti,

gli impegni internazionali del paese terzo) (punto 104).

L'approdo della Corte è estremamente rilevante perché, nel richiedere un livello equivalente di protezione per entrambe le ipotesi normative, la Corte innalza l'asticella delle garanzie di tutela, impedendo altresì che possano esservi diversi livelli di tutela a seconda dello strumento regolativo prescelto. Allo stesso tempo la Corte impone ai titolari del trattamento che effettuano trasferimenti dei dati verso paesi terzi un obbligo di conoscenza dei sistemi giuridici dei paesi terzi non sempre facile da realizzare.

5. Autorità di controllo e Commissione nella valutazione delle clausole di protezione tipo.

Con la domanda successiva viene affrontata la questione del ruolo delle autorità di controllo rispetto alla decisione della Commissione. In pratica il giudice del rinvio chiede di sapere se l'autorità di controllo abbia il potere di sospendere o vietare un trasferimento di dati personali verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati adottate dalla Commissione nel caso in cui l'autorità di controllo si convinca che esse non sono o non possono essere rispettate in detto paese terzo e che la protezione dei dati richiesta dal diritto dell'Unione non possa essere garantita (punto 106).

La Corte, seguendo anche in questo caso l'opinione dell'Avvocato generale, risponde positivamente (punto 113). Ed è questa una risposta che, come anticipato, conferisce alle autorità di controllo un potere notevole anche nei confronti della Commissione. Non si deve mancare di osservare, infatti, che la posizione della Corte è sviluppata in relazione alle clausole tipo di protezione, che, come recita l'art. 46, par.2, lett. c), Reg., sono adottate dalla Commissione. In questo caso il giudizio della Commissione non è ritenuto vincolante nei confronti delle autorità di controllo dalla Corte di giustizia. Il punto 115 della sentenza è dirimente in proposito. La soluzione della Corte responsabilizza dunque ulteriormente le autorità di controllo che, in caso di clausole di protezione tipo, possono essere chiamate a decidere se sospendere o vietare il trasferimento. È qui che si annida tuttavia il rischio di quella tutela a macchia di leopardo, cui si accennava nell'introduzione. Il Comitato europeo per la protezione dei dati è quindi chiamato a svolgere un attento ruolo di coordinamento.

Quanto al rapporto tra autorità di controllo e Commissione nel diverso caso in cui esista

una decisione di adeguatezza della Commissione in applicazione dell'art. 45, par.1, Reg., la Corte ripete invece la posizione che aveva già espresso in Schrems I, vale a dire che, finché la decisione di adeguatezza non sia stata dichiarata invalida dalla Corte, gli Stati membri e le loro autorità di controllo non possono adottare misure contrarie a tale decisione (punto 118).

6. Clausole di protezione tipo e decisione di adeguatezza.

La successiva questione riguarda più da vicino la natura e gli effetti delle clausole di protezione tipo previste dall'art. 46, par.2, lett.c, del Regolamento. In particolare il giudice del rinvio chiede se la decisione CPT sia idonea a garantire un livello di protezione adeguato dei dati personali trasferiti verso paesi terzi visto che le clausole tipo in essa contenute non vincolano le autorità dei paesi terzi (punto 123).

Sulla scorta del Regolamento la Corte opera una distinzione tra la decisione di adeguatezza, prevista dall'art. 45 e le clausole di protezione tipo, previste dall'articolo successivo. Con la prima la Commissione constata, con effetto vincolante, il livello di protezione adeguato garantito da un paese terzo, tenendo conto in particolare della legislazione pertinente in materia di sicurezza nazionale e di accesso delle autorità pubbliche ai dati personali. Le seconde muovono da un presupposto differente, giacché esse sono un mero strumento contrattuale che vincola solo le parti contraenti, in particolare il titolare del trattamento e il destinatario del trasferimento dei dati, non anche le autorità del paese terzo. Da ciò segue che, quando la Commissione adotta clausole di protezione dei dati (come ha fatto con la decisione CPT), essa non è tenuta a procedere a una valutazione dell'adeguatezza del livello di protezione garantito dai paesi terzi (punto 130).

La natura meramente contrattuale, privatistica, delle clausole di protezione tipo esenta dunque la Commissione da assunzioni di responsabilità sul livello di protezione adeguato garantito dal paese terzo, scaricando così sui soggetti privati l'onere di assicurare tale livello adeguato. È chiaro che qui, nell'uso delle clausole tipo, rischia di incrinarsi il muro di garanzie elevato dalla Corte a tutela dei dati personali dei cittadini europei. Come fare, dunque, a garantire un livello adeguato?

La Corte non fornisce risposte precise in proposito, appoggiandosi su alcuni *considerando*

del Regolamento, che incoraggiano i titolari del trattamento ad «aggiungere altre clausole o garanzie supplementari» (cons. 109, ma anche 108 e 114). Tali misure supplementari devono essere adottate dal titolare del trattamento, che, in collaborazione con il destinatario del trasferimento, dovrà valutare se il diritto del paese terzo garantisca una protezione adeguata. Nel caso in cui il titolare non sia in grado di adottare idonee misure supplementari, esso o l'autorità di controllo dovrà sospendere o porre fine al trasferimento dei dati (punto 135).

La rilevanza pratica di questa statuizione non può passare inosservata giacché da questo momento tutti i titolari di dati che si avvalgono di responsabili per il trattamento dei propri dati sono chiamati a controllare il contratto stipulato con il responsabile per valutare se quest'ultimo è autorizzato al trasferimento dei dati verso gli Stati Uniti. Nel caso ciò fosse previsto e non fosse possibile introdurre misure supplementari, appare indispensabile una riformulazione del contratto per vietare il trasferimento dei dati. La conclusione non dovrebbe essere differente nel caso in cui il contratto dovesse prevedere l'autorizzazione a trasferire i dati personali verso paese terzi diversi dagli Stati Uniti, nel caso in cui si dovesse giungere alla conclusione che tale paese terzo non assicura un livello adeguato di protezione.

Può sorgere, a questo punto, una legittima domanda sul senso di una decisione della Commissione che adotta clausole tipo di protezione dei dati, per come prevista dall'art. 46, par. 2, lett. *c)*, Reg. Se le clausole tipo non vincolano le autorità del paese terzo, qual è il senso dell'intervento della Commissione? In altri termini, se le clausole non vincolano il paese terzo, mettendo così in pericolo il livello di tutela richiesto dal diritto dell'Unione, il rischio è che le decisioni della Commissione ai sensi dell'art. 46, par.2, lett. *c)*, Reg., vengano esposte al rischio di un'intrinseca, strutturale invalidità. Per evitare ciò, la Corte afferma, intervenendo a soccorso della Commissione, che la validità della decisione della Commissione dipende solo dalla presenza di meccanismi efficaci che consentano, in pratica, di garantire che sia rispettato il livello di protezione e che i trasferimenti di dati personali, fondati su siffatte clausole, siano sospesi o vietati in caso di violazioni di tali clausole o impossibilità di rispettarle (punto 137).

Sulla base di tali premesse la Corte svolge un esame delle clausole della decisione CPT dalle quali emerge che su titolare e destinatario del trasferimento incombono obblighi diretti a verificare costantemente il livello di garanzia di trattamento dei dati, in particolare

diretti ad assicurare che la legislazione del paese terzo consenta al destinatario di conformarsi alle clausole tipo di protezione dei dati. La Corte estrapola dalle clausole in questione un obbligo, in capo al titolare del trattamento e al destinatario del trasferimento dei dati personali, di «verificare, preliminarmente, il rispetto, nel paese terzo interessato, del livello di protezione richiesto dal diritto dell'Unione», con l'ulteriore precisazione che il destinatario ha pure l'obbligo di informare il titolare della sua eventuale impossibilità di conformarsi a tali clausole, consentendo così al titolare di sospendere il trasferimento di dati e/o di risolvere il contratto (punto 142). L'analisi così condotta permette alla Corte di confermare la validità della decisione CPT.

È indubbia la rilevanza di questa parte della sentenza rispetto al suo noto precedente. La Corte distingue nettamente, sulla scorta del Regolamento, tra decisione di adeguatezza e clausole tipo di protezione. Queste ultime possono essere uno strumento utile per il trasferimento dei dati, nonostante la loro natura contrattuale. La Corte insiste sulle misure ulteriori che le parti possono prevedere per garantire il livello di protezione adeguata, ma si guarda bene dal precisare quali essi siano.

Il ricorso alle clausole tipo di protezione, esentando la Commissione da responsabilità sostanziali, è quindi rimesso alla discrezionalità delle parti private, sulle quali incombono obblighi di indubbia portata, in particolare quello di verificare la sussistenza di un livello di protezione richiesto dal diritto dell'Unione all'interno del paese terzo. Se ciò spingerà ad una "europeizzazione" dei grandi players americani, è questione aperta. Certo è che da ora saranno maggiormente esposti ad un controllo *ab externo* del livello di garanzia assicurato ai dati personali dei cittadini europei. Non si trascuri infatti il rilevante passaggio contenuto nel punto 146 nel quale è detto che la decisione della Commissione adottata ai sensi dell'art. 46, par.2, lett.c), Reg., non impedisce, «in alcun modo», all'autorità di controllo competente di sospendere o vietare il trasferimento dei dati verso un paese terzo. Grandi multinazionali e autorità di controllo sono dunque avvertite!

7. La decisione "scudo per la privacy" alla luce dell'art. 52, par.1, della Carta dei diritti fondamentali dell'Unione europea.

L'ultima domanda posta dal giudice irlandese è quella che porta alla dichiarazione d'invalidità della decisione "scudo per la privacy", che aveva sostituito quella del cd. "Approdo sicuro" (Safe Harbour) annullata con la sentenza Schrems I. Anche in questo caso il giudice del rinvio chiede se e in che limiti l'autorità di controllo di uno Stato membro sia vincolata dalle constatazioni contenute nella decisione "scudo per la privacy" secondo le quali gli Stati Uniti assicurano un livello di protezione adeguato. Più precisamente egli chiede se il trasferimento dei dati verso gli Stati Uniti avvenuto sul fondamento di clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT violi i diritti garantiti dagli artt. 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea e se l'aver istituito il Mediatore (di cui si fa menzione nell'allegato III della decisione "scudo per la privacy") sia compatibile con l'art. 47 della Carta (punto 150).

Occorre precisare meglio questo passaggio, e cioè il motivo per il quale la Corte estende il suo controllo anche alla decisione "scudo per la privacy". Nel procedimento principale, infatti, il ricorso del Commissario ha riguardato solo la validità della decisione CPT ed è comunque stato presentato prima che venisse adottata la decisione "scudo per la privacy". E tuttavia è il giudice del rinvio, osserva la Corte, a sottolineare di dover esaminare la vicenda alla luce delle modifiche della normativa intercorse tra la proposizione del ricorso e l'udienza tenutasi dinanzi ad esso. Da ciò l'obbligo di prendere in considerazione la decisione "scudo per la privacy", anche in ragione degli effetti vincolanti che essa è in grado di produrre sull'autorità di controllo (punti 151-154).

Le questioni sollevate dal giudice mettono dunque in dubbio il giudizio espresso dalla Commissione sull'adeguatezza dell'ordinamento statunitense nel garantire il livello di tutela chiesto dal diritto dell'Unione (v.l'art.1, par.1, della decisione "scudo per la privacy"). E i dubbi del giudice del rinvio incontrano quelli della Corte di giustizia, la quale ripercorre lo stesso percorso seguito in Schrems I. Come in quel caso, anche ora essa è costretta ad osservare che, per quanto nella decisione venga constatato il livello adeguato di protezione, è anche precisato (al punto I.5. dell'allegato II alla decisione in esame) che

l'adesione ai principi diretti a garantire tale livello di adeguatezza può essere limitata «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia». Si riproduce così la stessa situazione che aveva portato all'annullamento della decisione "approdo sicuro" in quanto le organizzazioni statunitensi che ricevono dati personali dall'Unione (nella specie Facebook) sono obbligate a disapplicare, senza limiti, i principi che dovrebbero garantire il livello di adeguatezza.

Le ingerenze nei diritti fondamentali delle persone i cui dati personali sono trasferiti negli Stati uniti avvengono grazie all'accesso ai dati personali da parte delle autorità pubbliche statunitensi e tramite l'utilizzo di tali dati nell'ambito dei programmi di sorveglianza PRISM e UPSTREAM fondati sull'art.702 FISA (*Foreign Intelligence Surveillance Act*) nonché sulla base del decreto presidenziale (*Executive Order*) 12333. Rispetto a ciò, la Commissione, nella propria decisione, constata che, «in base alle informazioni sull'ordinamento giuridico statunitense disponibili, […] l'ingerenza nei diritti fondamentali si limit(a)no a quanto strettamente necessario per conseguire l'obiettivo legittimo ricercato e che contro le ingerenze di tale natura esiste una tutela giuridica efficace» (punti 166 e 167).

La Corte di giustizia osserva che anche la mera comunicazione di dati personali a un terzo, quale un'autorità pubblica, costituisce di per sé un'ingerenza vietata dagli artt. 7 e 8 della CDFUE, indipendentemente dall'uso ulteriore delle informazioni comunicate. E tuttavia il giudice dell'Unione ricorda che tali ingerenze possono giustificarsi in ragione della funzione sociale dei diritti previsti dagli artt. 7 e 8.

La chiave di volta del ragionamento della Corte diventa dunque l'art. 52 della Carta, che nella sua prima fase del primo paragrafo stabilisce che eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta devono essere previsti dalla legge e devono rispettare il contenuto essenziale dei diritti e delle libertà. Nella seconda frase, invece, prevede che, nel rispetto del principio di proporzionalità, possano apportarsi limitazioni a tali diritti e libertà solo laddove siano necessarie e rispondano a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Tutto ciò implica che sia la legge a definire la portata della limitazione dell'esercizio; inoltre, per rispettare il principio di proporzionalità, la legge deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura di limitazione e impongano requisiti minimi, stabilendo in quali circostanze e a quali condizioni possa

essere adottata una misura che prevede il trattamento dei dati, così garantendo che l'ingerenza sia limitata allo stretto necessario.

Le ingerenze risultanti dai programmi di sorveglianza fondati sull'art. 702 del FISA e sull'E.O 12333 non risponderebbero ai requisiti richiesti dall'art. 52, par. 1, seconda frase. Questo è il parametro alla luce del quale la Corte decide di esaminare i suddetti programmi di sorveglianza.

La prima carenza viene individuata dalla Corte nei programmi di sorveglianza basati sull'art. 702 del FISA poiché la Corte FISA (il tribunale per la sorveglianza dell'intelligence esterna degli Stati Uniti) non autorizza singole misure di sorveglianza ma programmi di sorveglianza (quali PRISM e UPSTREAM), limitandosi a verificare se tali programmi servano all'obiettivo di ottenere informazioni in materia di intelligence esterna, senza alcuna preoccupazione riguardo al se la persona costituisca un obiettivo adatto per acquisire informazioni di intelligence esterna. Alla luce di ciò la Corte, in accordo con l'Avvocato generale, ritiene che l'art. 702 del Fisa non preveda limitazioni all'autorizzazione e soprattutto che l'ordinamento statunitense non conferisca agli interessati diritti nei confronti delle autorità statunitensi azionabili di fronte ai giudici. Viene così violata l'esigenza posta dall'art. 45, par.2, lett. *a)*, RGPD, secondo cui la constatazione del livello di adeguatezza dipende dall'esistenza di diritti effettivi ed azionabili in capo agli individui i cui dati sono stati trasferiti.

Anche per i programmi di sorveglianza fondati sull'E.O. 12333 emergono le stesse risultanze. In questo caso esiste una direttiva del Presidente degli Stati Uniti (PPD-28), che spiega cosa fanno gli Stati Uniti nelle attività di sorveglianza all'estero e che contiene principi ai quali i programmi di sorveglianza devono attenersi. La Corte osserva tuttavia che la PPD-28 permette la raccolta in blocco di un volume consistente di informazioni o dati senza che tale accesso sia oggetto di controllo giudiziario, così non delimitando, in maniera sufficiente e chiara, la portata di tale raccolta in blocco.

La conclusione è che né l'art.702 del FISA né l'E.O. 12333, in combinato disposto con la PPD-28, rispondono ai requisiti minimi connessi al principio di proporzionalità, sicché tali programmi non sono limitati allo stretto necessario (così punto 184). Da ciò consegue, secondo la Corte, la violazione dell'art. 52, par.1, seconda frase, della Carta.

Ma l'attenzione della Corte si concentra anche sulla violazione dell'art.47 della Carta medesima, che, nel richiedere che ogni persona i cui diritti e le cui libertà garantiti dal

diritto dell'Unione siano state violate abbia diritto a un ricorso effettivo dinanzi a un giudice, è estrinsecazione immediata di uno Stato di diritto. Questa istanza generale è confermata anche dall'art. 45, par.2, lett. *a)*, RGPD, che, come si è detto, chiede alla Commissione, allorquando essa proceda alla valutazione di adeguatezza, di prendere in considerazione gli strumenti di tutela degli interessati.

Ciò premesso, le carenze dell'ordinamento statunitense in relazione all'effettività della tutela sono state evidenziate dalla stessa Commissione che, al punto 115 della decisione "scudo per la privacy", non ha mancato di sottolineare come le possibilità di ricorso della persona sottoposta a sorveglianza elettronica non contemplino alcune delle basi giuridiche di cui possono avvalersi le autorità di intelligence statunitensi (ad esempio l'E.O.12333). E ciò osta, osserva la Corte, a che si concluda che il diritto degli Stati Uniti garantisce un livello di protezione sostanzialmente equivalente a quello garantito dall'art. 47 della Carta (punto 191).

Neppure la nuova figura del Mediatore, sul quale la Commissione aveva pure espresso un'opinione positiva, riesce a riequilibrare la situazione. La figura del Mediatore è stata prevista dall'art. 4, lett.d), della PPD-28, che incarica il segretario di Stato di nominare un Primo coordinatore della diplomazia internazionale per le tecnologie dell'informazione, avente la funzione di referente per i governi stranieri che si pongono interrogativi sull'attività di intelligence dei segnali condotte dagli Stati Uniti d'America. Tale Primo coordinatore svolge la funzione di Mediatore, è indipendente dall'intelligence statunitense, riferisce direttamente al segretario di Stato, il quale assicura che svolga la sua funzione con obiettività e senza indebite ingerenze. In sintonia con l'avvocato generale, la Corte esprime dubbi sull'indipendenza del Mediatore e sulla sua capacità di adottare decisioni vincolanti nei confronti dei servizi di intelligence statunitense.

La conclusione della Corte è che la decisione della Commissione abbia disatteso i requisiti di cui all'art. 45, par. 1, RGPD, letto alla luce degli artt. 7, 8 e 47 della Carta, risultando quindi invalida nel suo complesso.

8. Conclusioni: dal contenuto essenziale al principio di proporzionalità e ritorno.

Il rapporto tra principio di proporzionalità e contenuto essenziale dei diritti fondamentali merita qualche riflessione conclusiva giacché è sulla base di questi due principi o criteri di giudizio che si arriva alla dichiarazione d'invalidità della decisione "scudo per la privacy". Nella presente decisione, tuttavia, la Corte pare percorrere un percorso argomentativo inverso o comunque diverso rispetto a quello intrapreso nella sentenza Schrems I. In quest'ultima, infatti, essa aveva puntato con forza sul contenuto essenziale, affermando in sostanza che, poiché aveva ravvisato una violazione di tale contenuto essenziale (nella specie il contenuto dei diritti fondamentali al rispetto della vita privata e ad un ricorso effettivo), la decisione risultava invalida senza bisogno di verificare se ci fosse anche una lesione del principio di proporzionalità.

Nel caso in esame, invece, la Corte ricorre sia al principio di proporzionalità che al contenuto essenziale in una maniera che non appare, però, del tutto lineare (dal punto 168 a fine). Provo a spiegare perché. La Corte afferma di voler esaminare i programmi di sorveglianza alla luce di quanto previsto dalla seconda frase del paragrafo primo dell'art. 52, quello appunto in cui la proporzionalità è richiamato come principio utile per apporre limitazioni (punto 178). Nell'analisi condotta dalla Corte nei punti successivi (da 179 a 184) la Corte mostra come la legislazione USA non contenga limitazioni alle ingerenze delle autorità pubbliche dirette a garantire ai cittadini europei strumenti di reazione dinanzi ad un'autorità giurisdizionale. In pratica, le ingerenze delle autorità pubbliche statunitensi nei dati personali trasferiti non sono bilanciate dal riconoscimento di un controllo giurisdizionale azionabile dagli interessati. Ciò porta alla già ricordata conclusione per cui né l'art. 702 del FISA né l'E.O. 12333 rispettano i requisiti minimi del principio di proporzionalità (punto 184).

Il riferimento al contenuto essenziale emerge espressamente nei punti successivi. In particolare, al punto 187 la Corte, richiamando Schrems I, ricorda la strettissima connessione tra controllo giurisdizionale effettivo e Stato di diritto sicché una normativa priva della possibilità per il singolo di avvalersi di rimedi giuridici non rispetta il contenuto

essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, sancito dall'art. 47 della Carta. Ed è proprio la carenza delle disposizioni relative al Mediatore dello scudo per la privacy riguardo a tale diritto fondamentale che porta la Corte a concludere per la violazione dell'art. 47 (punto 197). In questa parte dell'analisi non appare il riferimento al principio di proporzionalità.

Due osservazioni conclusive appaiono allora opportune. La prima è che, nel caso di specie, la Corte, appoggiandosi al precedente della sentenza Schrems I, ribadisce che il contenuto essenziale dell'art. 47 della Carta è dato dall'esistenza di un controllo giurisdizionale effettivo. È il rispetto del contenuto essenziale di questo diritto che ha portato alla sentenza Schrems I e che viene ribadito in Schrems II.

La seconda osservazione vuole invece enfatizzare un punto di diversità rispetto alla sentenza Schrems I. Se in questa ultima il ragionamento fu molto audace e innovativo (la violazione del contenuto essenziale rende superflua ogni altra analisi condotta alla luce del principio di proporzionalità), in Schrems II la Corte assume un atteggiamento più inclusivo, per così dire, sviluppando prima un'analisi poggiante sul principio di proporzionalità e poi giungendo al contenuto essenziale. Ma se a esser stato violato, alla fine, è il contenuto essenziale, non si intende il motivo per cui la Corte afferma di voler condurre l'analisi alla luce dell'art. 47, par.1, frase seconda, che non contiene il riferimento al contenuto essenziale.

Poiché la Corte avrebbe potuto seguire la stessa trama intessuta con Schrems I, la novità argomentativa è rilevante. È difficile dire cosa abbia spinto la Corte a questo percorso argomentativo più "*souple*". La ritenuta opportunità di una trama argomentativa più ampia o la consapevolezza che il ricorso al contenuto essenziale contiene dei rischi di decisionismo giudiziario troppo elevati? O forse la volontà di ribadire l'autonomia concettuale tra i due strumenti argomentativi per cui un atto può anche essere rispettoso del contenuto essenziale ma essere in contrasto col principio di proporzionalità?

Abstract: dopo la sentenza Schrems I la Corte di giustizia torna a occuparsi di trasferimento dei dati personali. E lo fa con novità sostanziali. Interessanti risultano anche le strumentazioni dogmatiche utilizzate nella parte conclusiva della sentenza.

Abstract: Schrems I had the features of a leading case. The Court of justice's new

judgement seems to endear itself to the privacy's fan. What about the other cornerstone of the GDPR, the free movement of personal data?

Parole-chiave: Corte di giustizia dell'Unione europea – trasferimento dati – diritti dei privati – titolari e responsabili.

Key words: Court of Justice of the European Union – data transfer – rights of data subjects – controllers and processors – principle of proportionality.