Tutela dei dati personali e deroghe in materia di sicurezza nazionale dopo l'entrata in vigore del *Privacy Shield*

STEFANO SALUZZO (*)

Dopo diversi mesi di negoziato, la Commissione e il governo statunitense hanno infine raggiunto un accordo sul trasferimento verso gli Stati Uniti di dati personali raccolti nel territorio dell'Unione europea. Il negoziato, per la verità avviato già a partire dalle rivelazioni del *Datagate*, aveva subito una consistente accelerazione dopo l'intervento della Corte di giustizia a seguito della nota sentenza *Schrems* del 6 ottobre 2015. Con la sentenza, la Corte ha annullato la decisione di adeguatezza – fondata sui *Safe Harbour Principles* – che legittimava, *ex* art. 25 della Direttiva 95/46, il trasferimento di dati verso gli USA (sulla sentenza v. il post di Nino). Secondo la Corte, infatti, le deroghe alla tutela dei dati personali, contemplate dal sistema *Safe Harbour* e fondate su esigenze connesse alla sicurezza nazionale, avrebbero consentito alle autorità statunitensi un accesso generalizzato e indiscriminato ai dati dei cittadini europei, tale da costituire un pregiudizio del contenuto essenziale del diritto al rispetto della vita privata di cui all'art. 7 della Carta dei diritti fondamentali (*Schrems*, par. 94).

Il 12 luglio 2016 la Commissione ha adottato una decisione fondata sui nuovi principi contenuti nel c.d. *Privacy Shield*, riconoscendo nuovamente l'adeguatezza della tutela offerta dall'ordinamento statunitense.

Va ricordato che, affinché i dati personali raccolti nel territorio dell'Unione possano essere legittimamente trasferiti verso un paese

(*) Università di Palermo.

terzo, la direttiva 95/46 prevede un meccanismo di tutela di tali dati e dei loro titolari nel paese di destinazione. Lo strumento principale previsto a tal fine è proprio la decisione di adeguatezza, con cui la Commissione certifica che il paese terzo offre una tutela "adeguata", termine che la Corte ha interpretato nel senso di "sostanzialmente equivalente" a quella offerta dall'ordinamento UE (*Schrems*, par. 73). In realtà, una buona parte del traffico di dati trovava comunque la propria disciplina, anche dopo la sentenza *Schrems*, in specifiche clausole contrattuali o nelle norme vincolanti d'impresa, sebbene in queste ipotesi, e a differenza di quanto accade con la decisione di adeguatezza, i trasferimenti debbano sempre essere autorizzati di volta in volta dalle autorità indipendenti. L'adozione di una nuova decisione di adeguatezza è tanto più importante se si considera che le clausole contrattuali standard (c.d. *model clauses*) sono in questo momento oggetto di un ulteriore esame da parte del garante per i dati personali irlandese, in un procedimento che vede contrapposti Schrems e Facebook e nel quale gli Stati Uniti hanno chiesto di intervenire. Inoltre, il Garante irlandese ha recentemente comunicato di voler sollevare, con riferimento a detto procedimento, un nuovo rinvio pregiudiziale alla Corte di giustizia.

Il meccanismo su cui si fonda il trasferimento di dati dall'UE verso paesi terzi ha già ricevuto ampia trattazione in dottrina e si rimanda ad altri contributi per un approfondimento in merito (v. Kuner). Ciò che interessa in questa sede è offrire una breve panoramica e una prima valutazione delle nuove regole contenute nel *Privacy Shield* in tema di deroghe alle norme sulla protezione dei dati personali giustificate da esigenze connesse alla sicurezza nazionale. Già più di un dubbio di compatibilità con il diritto UE è stato sollevato in relazione a tali deroghe, soprattutto per quanto attiene ad un eventuale futuro sindacato della Corte di giustizia (Crespi).

Va preliminarmente ricordato che il *Privacy Shield* non costituisce accordo internazionale in senso proprio, essendo composto da una serie di atti unilaterali adottati dalla Commissione e dal governo statunitense volti a regolare in traffico transatlantico di dati. Se dall'adozione di tali atti possa comunque farsi derivare la conclusione di un accordo in forma semplificata è questione cui sembra doversi dare risposta negativa per diverse ragioni. In *primis*, non è mai menzionata, in alcuno degli atti, la volontà di concludere un accordo internazionale, così come vorrebbero gli artt. 12 e 13 della Convenzione di Vienna; inoltre, ai sensi del diritto dell'Unione, la conclusione di un accordo internazionale in *subiecta materia*, anche in forma semplificata, dovrebbe seguire la procedura dell'art. 218 TFUE, che prevede peraltro la previa approvazione del Parlamento europeo. Al contrario, il *Privacy Shield* è essenzialmente costituito da alcuni atti ascrivibili al governo statunitense (in particolare alla *Federal Trade Commission* e al Dipartimento di Stato) e dalla decisione di adeguatezza della Com-

missione, che è un atto esecutivo. Se è vero che, rispetto al precedente *Safe Harbour*, nel caso del *Privacy Shield* la volontaria adesione delle società statunitensi ai principi ivi contenuti si accompagna anche alle espresse assicurazioni e garanzie offerte dal governo americano, non sfugge però che, non trattandosi di obblighi internazionali, tali impegni non siano esigibili da parte dell'UE e rimangano dichiarazioni di valore meramente politico.

Quanto al contenuto, il *Privacy Shield* è costituito da un insieme di principi cui – come già accadeva per il *Safe Harbour* – le società statunitensi possono volontariamente aderire per ottenere la certificazione che consenta loro di ricevere e gestire dati personali provenienti dall'UE. Il fatto che si tratti di un regime applicabile solo sulla base di una scelta di volontaria adesione non dovrebbe precludere la possibilità di ritenere che la tutela prevista sia adeguata, secondo quanto ritenuto dalla stessa Corte di giustizia (*Schrems*, par. 81). Inoltre, l'adesione a tali principi comporta anche la sottoposizione ad alcuni meccanismi di controllo, gestiti da diversi dipartimenti dell'esecutivo statunitense. La parte introduttiva del *Privacy Shield* (Allegato II, Parte I, punto 5) prevede la possibilità di derogare ai principi sul trattamento dei dati personali quando *a*) ciò sia necessario per soddisfare esigenze di sicurezza nazionale, di interesse pubblico o di applicazione della legge; *b*) la legge (così come una giurisprudenza costante) imponga un obbligo confliggente con i principi o autorizzi l'organizzazione a discostarsi dal rispetto di tali principi, purché l'organizzazione dimostri che le misure in deroga sono strettamente funzionali al raggiungimento degli obiettivi perseguiti dalla norma confliggente; *c*) quando eccezioni o deroghe previste dalla Direttiva 95/46 o dalle leggi degli Stati membri dell'Unione siano applicabili per analogia al contesto («in a comparable context») in cui opera l'organizzazione statunitense. La formulazione di tali deroghe appare ancora eccessivamente ampia e di incerta definizione, come recentemente osservato anche dal Garante europeo per la protezione dei dati.

È proprio nei confronti di tali clausole di deroga che si sono concentrate le maggiori critiche al nuovo *Privacy Shield* da parte di diversi organi dell'Unione, intervenuti durante le fasi conclusive del negoziato. In particolare, le critiche si concentrano su alcuni profili attinenti alle garanzie che devono accompagnare l'adozione di misure di interferenza con i diritti fondamentali perché queste ultime possano ritenersi legittime. Tali garanzie, recentemente riassunte in un documento dell'*Article 29 Working Party*, si applicano a tutti i casi di ingerenza nel godimento del diritto alla riservatezza e alla protezione dei dati personali e fanno parte di quel *corpus* normativo al quale le tutele offerte dagli ordinamenti di Stati terzi devono – secondo il meccanismo delle decisioni di adeguatezza – sostanzialmente equivalere (v. *European Essential Guarantees*). Si tratta di garanzie ricavate dalla giurisprudenza della Corte di giustizia e della Corte EDU, incentrate

sul rispetto del principio di legalità, sulla rispondenza delle deroghe ai criteri di necessità e proporzionalità e sulla sussistenza di adeguati meccanismi di tutela (non necessariamente giurisdizionali) nelle ipotesi di lesione dei diritti dei singoli.

In particolare, i principi espressi nel *Privacy Shield* e le deroghe ivi previste rivelano almeno due profili di maggiore criticità: il primo riguarda alcune lacune normative in tema di trasferimenti successivi di dati verso un altro paese, diverso dal paese di destinazione (*onward transfers*); il secondo, invece, attiene alla persistente possibilità, per le agenzie di *intelligence* statunitensi, di ricorrere a strumenti di sorveglianza di massa, anche se in ipotesi specificamente previste.

Per "trasferimento successivo" si intende un trasferimento di dati di origine UE da un operatore statunitense verso un paese terzo; in questo caso, cioè, i dati personali raccolti nel territorio dell'Unione transitano verso gli Stati Uniti, per essere poi ritrasferiti verso operatori che hanno sede in un paese diverso. L'ipotesi è regolata dall'*Accountability for onward tranfer principle* (di cui al punto 3 del *Privacy Shield*), in base al quale l'operatore statunitense – che abbia aderito al *Privacy Shield* – è tenuto a concludere un contratto con il controllore ricevente che ha sede nel paese terzo, con il quale quest'ultimo si impegna a utilizzare i dati ricevuti per una finalità specifica e definita e a garantire una tutela equivalente a quella garantita dai principi del *Privacy Shield*. Regole analoghe, che non necessitano però di un regime contrattuale *ad hoc*, sono previste quando il soggetto ricevente nel paese terzo operi come agente di un'organizzazione statunitense. Ci si chiede, tuttavia, se questo insieme di regole, previste per il trattamento di dati personali a fini commerciali, sia altresì applicabile al trasferimento di dati verso paesi terzi nei quali tali dati saranno poi raccolti nell'ambito di attività di *intelligence*. La questione si sostanzia nell'individuare quale portata possano avere le deroghe in materia di tutela della sicurezza nazionale nel caso di trasferimenti successivi. Si profilano, in realtà, diversi scenari: può accadere, innanzitutto, che un'organizzazione statunitense trasferisca dati ad operatori privati di paesi terzi in cui vigono regole meno rigide per la raccolta di dati personali da parte delle pubbliche autorità; può, però, anche verificarsi il caso in cui una autorità pubblica statunitense acceda a dati di origine UE e successivamente – nel quadro di una cooperazione investigativa o di *intelligence* – trasferisca tali dati ad agenzie di Stati terzi.

Quanto alla prima ipotesi, secondo il parere dell'*Article 29 Working Party*, le regole in materia di trasferimenti successivi dovrebbero comunque trovare applicazione, quantomeno nel senso di richiedere, all'organizzazione che trasferisce dati UE in un paese terzo, di valutare il livello di tutela offerto dall'ordinamento di quel paese e, se del caso, di sospendere il trasferimento, dopo aver informato il titolare del trattamento. Quando sia lo stesso responsabile del trattamento di ori-

gine UE a conoscere i rischi di un eventuale successivo trasferimento verso un paese terzo e lo autorizzi ugualmente, o partecipi direttamente al trasferimento di dati, tale trasferimento non avverrà sulla base del *Privacy Shield*, ma si configurerà come trasferimento di dati direttamente dall'UE verso lo Stato terzo, con conseguente ricaduta nella disciplina generale di cui agli artt. 25 e 26 della Direttiva 95/46.

Non è chiaro, invece, quali regole siano applicabili alla seconda ipotesi, vale a dire quella del trasferimento di dati da una pubblica autorità statunitense ad un altro soggetto pubblico di un paese terzo. Si tratta, all'evidenza, di una più tradizionale forma di scambio di informazioni tra organi di paesi diversi, la cui peculiarità risiede nel fatto che i dati oggetto di scambio sono soggetti ad un particolare regime di protezione, ad esempio per quanto riguarda la finalità o la durata della loro conservazione. Stante la mancanza di una regola certa e l'impossibilità di replicare l'applicazione analogica di cui si è detto – posto che il trasferimento non avviene tra soggetti privati – resta da definire se, nella fattispecie, esistano obblighi vincolanti per le autorità pubbliche statunitensi. Qualche indicazione in questo senso proviene dall'accordo tra UE e USA in materia di protezione dei dati personali relativi alla prevenzione e alla repressione di reati (accordo per ora soltanto firmato dalle due parti e non ancora in vigore, in attesa dell'approvazione del Parlamento europeo). L'art. 7 dell'accordo disciplina proprio il caso dei trasferimenti successivi, prevedendo che quando un'autorità di una delle parti del trattato abbia trasferito dati personali alle autorità dell'altra parte, tali dati potranno a loro volta essere trasferiti alle autorità di un paese terzo soltanto previo consenso dell'autorità competente che per prima li aveva trasferiti. Nel prestare il proprio consenso, l'autorità competente dovrà tener conto di una serie di elementi, tra cui la serietà del reato in relazione al quale le informazioni sono state richieste, la finalità in vista della quale i dati erano stati inizialmente trasferiti, nonché il livello di tutela offerto dal paese terzo. Una siffatta disposizione risolverebbe dunque il problema dei trasferimenti successivi, benché non sia facile comprendere, dalla lettera dell'accordo, se esso si applichi anche alle attività di *intelligence* o se sia destinato a regolare lo scambio di informazioni nel solo caso di procedimenti penali. Cionondimeno, rimane priva di una regolamentazione l'ipotesi in cui i dati siano stati trasferiti da un soggetto privato UE ad un soggetto privato statunitense, per poi essere raccolti in territorio americano dall'autorità pubblica e solo successivamente trasferiti in un paese terzo. La mancanza di una regola chiara in quest'ultima ipotesi desta, dunque, più di una preoccupazione, potendo costituire un facile strumento di elusione della disciplina europea.

Il secondo profilo critico, che emerge dalla lettura dei documenti allegati alla nuova decisione di adeguatezza, riguarda la possibilità, per le agenzie di *intelligence* americane, di fare ricorso alla c.d. *bulk collection of data*, vale a dire la raccolta e la conservazione su larga

scala di dati e informazioni personali, senza l'utilizzo di criteri discriminanti. Sebbene la materia sia stata recentemente interessata da alcune modifiche, tra cui quelle apportate dalla Direttiva Presidenziale 28 del 17 gennaio 2014, permangono alcune perplessità circa la compatibilità di intercettazioni massive con i principi di necessità e proporzionalità.

La Direttiva 28, approvata durante la Presidenza Obama, prevede infatti che l'intercettazione di comunicazioni e dati per finalità di *intelligence* sia sempre «as tailored as feasible», dunque riferibile a singoli individui identificati e per motivi specifici. Questa forma di intercettazione non sembra porre problemi particolari, posto che anche la giurisprudenza più recente della Corte di Strasburgo ne ha riconosciuto la legittimità, purché l'esistenza di un ragionevole sospetto nei confronti di un individuo sia verificabile. Inoltre, il soggetto sottoposto a intercettazione deve essere sempre identificato o comunque identificabile (v. Corte EDU, *Zakharov v. Russia*, par. 264). Rimane in ogni caso qualche dubbio sulla formulazione impiegata dalla Direttiva 28, posto che questa non specifica le circostanze in cui l'intercettazione di singoli individui debba ritenersi non più praticabile.

Ai sensi della Direttiva 28, poi, la *bulk collection* sarà possibile soltanto per finalità espressamente previste: individuazione e contrasto di determinate attività di governi stranieri; lotta al terrorismo; lotta alla proliferazione di armi; *cybersecurity*; individuazione e contrasto di minacce per gli Stati Uniti e per i loro alleati; lotta al crimine transnazionale. Le operazioni di raccolta di dati su larga scala sono sottoposte a una revisione annuale, condotta però da organi afferenti all'esecutivo. È ben evidente che l'ampiezza di tali finalità solleva già di per sé qualche dubbio circa il rispetto del requisito di necessità, almeno come recentemente interpretato nella sentenza *Schrems* (par. 93). Ma ciò che desta maggior preoccupazione è che il perseguimento delle menzionate finalità presuppone un'attività di raccolta dei dati di natura sostanzialmente esplorativa, tanto che la stessa Direttiva 28 ammette che alla raccolta su larga scala si farà ricorso «in certain circumstances in order to identify new or emerging threats and other vital national security information that is often hidden within the large and complex system of modern global communications». Ciò pare altresì confermato dal fatto che la Direttiva 28 consente il ricorso alla raccolta massiva di dati allo scopo di facilitare l'intercettazione di singoli individui. Come appare chiaro, si tratta di una sorta di corto circuito, in base al quale l'intercettazione mirata diviene possibile quando preceduta da una raccolta di dati su larga scala che abbia consentito di individuare una minaccia, con il rischio che l'eccezione della *bulk collection* diventi la regola.

Secondo la Commissione europea, i limiti previsti per il ricorso a tali misure sarebbero conformi ai requisiti di necessità e proporzio-

nalità, poiché la Direttiva 28 impone il ricorso a intercettazioni mirate e, solo in casi eccezionali e per motivi specifici, consente la raccolta di dati su larga scala (*considerando* 76 e 90). Tuttavia, e al di là di quanto già osservato, la motivazione della Commissione sembra non tenere in considerazione la possibilità che la raccolta di dati, qualificabile come *mass surveillance*, sia di per sé stessa incompatibile con il principio di proporzionalità, come da più parti sostenuto (v. UN High Commissioner for Human Rights, Report on The right to privacy in the digital age, par. 25, nonché il parere dell'*Article 29 Working Party*, par. 3.3), rimanendo dunque privo di rilievo il fatto che ad essa si faccia ricorso in circostanze eccezionali. Si tratta di una questione che avrebbe potuto essere auspicabilmente affrontata già in sede di definizione delle norme che presiedono al ricorso a tale tipologia di sorveglianza. Il problema, però, potrebbe essere risolto dalla giurisprudenza in un futuro prossimo, poiché, sia davanti alla Corte EDU (ric. n. 58179/13, ric. n. 62322/14, ric. n. 24960/15) che davanti alla Corte di giustizia (cause riunite C-203/15 e C-698/15; v. anche la richiesta di parere A-1/15 in merito all'accordo con il Canada sui codici di prenotazione dei passeggeri), pendono ricorsi aventi ad oggetto la legittimità dei programmi di sorveglianza di massa. In senso contrario, tuttavia, si è recentemente espresso l'Avvocato generale Saugmandsgaard Øe, nella causa *Tele2 Sverige*, ritenendo che la possibilità di una raccolta e di una conservazione generalizzata di dati personali non possa ritenersi *a priori* incompatibile con il requisito di proporzionalità, dovendosi di volta in volta ponderare i vantaggi connessi ad operazioni di sorveglianza massiva con i rischi da questa derivanti per i diritti fondamentali degli individui. Nel frattempo, alcuni membri del Parlamento europeo hanno proposto l'adozione di una risoluzione nella quale si ritiene che la *bulk collection of data*, pur configurandosi come eccezione alla regola delle intercettazioni mirate, da applicarsi secondo il principio di ragionevolezza, non risponda ai requisiti di necessità e proporzionalità di cui alla Carta dei diritti fondamentali.

In conclusione, è certo che i principi codificati nel *Privacy Shield* costituiscano un avanzamento rispetto al sistema precedente. Inoltre, accanto ad un più dettagliato impianto normativo, sono stati inseriti meccanismi di controllo delle operazioni di *intelligence*, la cui configurazione solleva comunque alcuni dubbi quanto alla conformità con le garanzie di terzietà ed indipendenza. Se non altro, è oggi consentito agli individui agire di fronte ad un *Ombudsperson* del Dipartimento di Stato per ottenere un rimedio a fronte della violazione del proprio diritto alla riservatezza e, contestualmente, il *Judicial Redress Act* del 2015 ha esteso anche ai cittadini europei la possibilità di agire in sede civile – di fronte al giudice statunitense – per ottenere il risarcimento del danno derivante da intercettazioni illecite. Soltanto una concreta messa in opera dell'intero impianto del *Privacy Shield* consentirà di capire se tali meccanismi saranno in grado di ovviare alle

lacune evidenziate sul piano sostanziale, evitando così che queste ultime si traducano in interferenze indiscriminate e non giustificabili nei diritti dei singoli.

13 settembre 2016