GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

16/IT
WP 238

Parere 01/2016 sul progetto di decisione sull'adeguatezza del regime dello scudo UE-USA per la privacy

adottato il 13 aprile 2016

SINTESI

Il 29 febbraio 2016 la Commissione europea ha pubblicato una comunicazione, un progetto di decisione sull'adeguatezza e i testi allegati che costituiscono un nuovo quadro per gli scambi transatlantici di dati personali a fini commerciali: lo scudo UE-USA per la privacy (di seguito "scudo"), inteso a sostituire il precedente quadro dell'approdo sicuro, dichiarato invalido dalla Corte di giustizia dell'Unione europea (di seguito "Corte di giustizia") il 6 ottobre 2015 con la sentenza nella causa Schrems.

Ai sensi dell'articolo 30, paragrafo 1, lettera c), della direttiva 95/46/CE, il Gruppo di lavoro articolo 29 (di seguito "Gruppo di lavoro" o "Gruppo") ha valutato tali documenti al fine di fornire un parere sul progetto di decisione sull'adeguatezza. Il Gruppo di lavoro ha valutato sia gli aspetti commerciali sia le eventuali deroghe ai principi dello scudo per finalità di sicurezza nazionale, di contrasto e di interesse pubblico.

Il Gruppo di lavoro ha tenuto conto del quadro giuridico dell'UE applicabile in materia di protezione dei dati stabilito nella direttiva 95/46/CE, nonché dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati sanciti all'articolo 8 della Convenzione europea dei diritti dell'uomo e agli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Ha inoltre tenuto presente il diritto a un ricorso effettivo e a un giudice imparziale sancito all'articolo 47 della Carta, nonché la giurisprudenza relativa ai vari diritti fondamentali.

L'analisi riflette inoltre le motivazioni addotte dalla Corte di giustizia nella causa Schrems in merito alla discrezionalità della Commissione in una valutazione di adeguatezza. La verifica e i controlli dei requisiti di adeguatezza devono essere espletati in maniera rigorosa, tenendo conto dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati e del numero di persone potenzialmente interessate dai trasferimenti.

Il regime dello scudo deve essere esaminato nell'attuale contesto internazionale, caratterizzato fra l'altro dalla presenza di grossi volumi di dati e da crescenti esigenze in materia di sicurezza. La portata e la vastità della raccolta e dell'uso di dati personali sono drasticamente aumentate da quando, nel 2000, è stata emanata la decisione originaria "Approdo sicuro". Le autorità europee di protezione dei dati ribadiscono con forza l'importanza dei principi che esse difendono.

Il Gruppo di lavoro plaude innanzitutto ai notevoli miglioramenti apportati dal regime dello scudo rispetto alla decisione sull'approdo sicuro. Rileva che i negoziatori hanno affrontato molte delle lacune che il Gruppo aveva riscontrato nel regime dell'approdo sicuro ed evidenziato nella lettera del 10 aprile 2014 indirizzata alla vicepresidente Reding.

Poiché i principi e le garanzie previsti dallo scudo sono esposti sia nella decisione sull'adeguatezza sia nei relativi allegati, le informazioni risultano difficili da reperire e sono talvolta incoerenti. Ciò contribuisce a determinare, in generale, una mancanza di chiarezza sul nuovo regime e a complicare l'accesso da parte degli interessati, delle organizzazioni e delle

autorità di protezione dei dati. Si ravvisa parimenti una mancanza di chiarezza nel linguaggio utilizzato. Il Gruppo di lavoro esorta pertanto la Commissione a renderlo chiaro e comprensibile su entrambe le sponde dell'Atlantico.

Per quanto riguarda la legislazione applicabile, il Gruppo di lavoro evidenzia che, qualora la decisione sull'adeguatezza del regime dello scudo sia adottata sulla base della direttiva 95/46/CE, essa dovrà essere coerente, quanto a terminologia e a campo di applicazione, con il quadro giuridico dell'Unione in materia di protezione dei dati. Il Gruppo ritiene sia necessario procedere a un riesame subito dopo l'entrata in applicazione del regolamento generale sulla protezione dei dati, al fine di garantire che il maggiore livello di protezione dei dati offerto dal regolamento si rifletta nella decisione sull'adeguatezza e nei relativi allegati.

In merito agli aspetti commerciali del regime dello scudo

Il principale obiettivo perseguito dal Gruppo di lavoro è assicurare che i cittadini continuino a beneficiare di un livello di protezione sostanzialmente equivalente quando i loro dati sono trattati ai sensi delle disposizioni dello scudo. Il Gruppo non si aspetta che lo scudo sia destinato meramente a duplicare sotto ogni aspetto il quadro giuridico dell'Unione ma ritiene comunque che esso debba racchiudere l'essenza dei principi fondamentali e, pertanto, garantire un livello di protezione "sostanzialmente equivalente".

Nonostante i miglioramenti introdotti dallo scudo, il Gruppo di lavoro ritiene che alcuni principi fondamentali in materia di protezione dei dati, quali delineati nella legislazione europea, non siano stati ripresi nel progetto di decisione sull'adeguatezza e nei relativi allegati, o siano sostituiti in maniera inadeguata da concetti alternativi.

Ad esempio il principio di conservazione dei dati non è esplicitamente menzionato, né lo si può chiaramente desumere dalla formulazione attuale del principio sull'integrità dei dati e la limitazione della finalità. Inoltre non vi è alcun accenno alla protezione che dovrebbe essere garantita contro singole decisioni automatizzate basate unicamente sul trattamento automatizzato. Poco chiara risulta altresì l'applicazione del principio sulla limitazione della finalità al trattamento dei dati. Al fine di apportare maggiore chiarezza nell'uso di vari concetti importanti, il Gruppo di lavoro ritiene che l'Unione e gli USA debbano concordare definizioni chiare e inserirle in un glossario di termini a corredo delle "domande più frequenti" (FAQ) relative al regime dello scudo.

Poiché lo scudo sarà utilizzato anche per il trasferimento di dati al di fuori degli Stati Uniti, il Gruppo di lavoro ribadisce che l'ulteriore trasferimento da un soggetto aderente allo scudo a destinatari di paesi terzi dovrebbe offrire lo stesso livello di protezione per quanto riguarda tutti gli aspetti dello scudo (compresa la sicurezza nazionale) e non determinare l'indebolimento o l'elusione dei principi dell'UE in materia di protezione dei dati. Nel caso in cui sia previsto un ulteriore trasferimento verso un paese terzo nell'ambito dello scudo, ogni organizzazione aderente allo scudo dovrebbe avere l'obbligo di valutare, prima del trasferimento, gli eventuali requisiti obbligatori, previsti dalla legislazione nazionale del paese

terzo, applicabili all'importatore dei dati. In generale, il Gruppo di lavoro conclude che l'ulteriore trasferimento di dati personali dell'UE non è sufficientemente definito, soprattutto per quanto attiene alla sua portata, alla limitazione della sua finalità e alle garanzie applicabili ai trasferimenti verso i procuratori.

Infine pur constatando che le persone fisiche dispongono ora di ulteriori mezzi di ricorso per esercitare i propri diritti, il Gruppo di lavoro teme che il nuovo meccanismo di ricorso possa risultare, nella pratica, troppo complesso e di difficile impiego per i cittadini dell'Unione e dunque rivelarsi inefficace. Sono pertanto necessari ulteriori chiarimenti sulle varie procedure di ricorso; in particolare le autorità di protezione dei dati dell'UE, qualora diano la loro disponibilità, potrebbero essere considerate un naturale punto di contatto per i cittadini dell'Unione nelle varie procedure, giacché possono agire per conto di questi ultimi.

Deroghe per scopi di sicurezza nazionale

Per quanto riguarda l'accesso ai dati da parte delle autorità pubbliche, sia nell'Unione sia nei paesi terzi, il Gruppo di lavoro richiama la propria analisi dei diritti fondamentali pertinenti esposta nel documento di lavoro relativo alla giustificazione delle ingerenze nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati attraverso misure di sorveglianza nei casi di trasferimento di dati personali (garanzie essenziali europee) (WP237).

Un importante passo avanti rispetto alla decisione sull'approdo sicuro è costituito dal fatto che la questione dell'eventuale accesso ai dati trattati nell'ambito dello scudo per finalità di sicurezza nazionale e di contrasto è ampiamente trattata nel progetto di decisione sull'adeguatezza dello scudo. Il Gruppo di lavoro riconosce l'importanza di questo aspetto, oltre alla maggiore trasparenza offerta dall'amministrazione USA per quanto riguarda la legislazione applicabile alla raccolta di informazioni di intelligence (allegato VI).

Il Gruppo di lavoro rileva tuttavia che le dichiarazioni dell'Ufficio del Direttore dell'intelligence nazionale degli Stati Uniti (ODNI) non escludono la raccolta in massa o indiscriminata di dati personali provenienti dall'Unione. Il Gruppo di lavoro rammenta che da tempo ha assunto la posizione secondo la quale la sorveglianza indiscriminata e in massa sui cittadini non può mai essere considerata proporzionata e strettamente necessaria in una società democratica e dunque non soddisfa le condizioni di tutela previste nell'ambito dei diritti fondamentali applicabili. Inoltre il controllo globale di tutti i programmi di sorveglianza è di importanza vitale. Il Gruppo di lavoro rileva la tendenza a raccogliere, in maniera indiscriminata e su larga scala, una quantità di dati ancora maggiore alla luce della lotta contro il terrorismo. Date le preoccupazioni che tale aspetto solleva per quanto riguarda la tutela dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati, il Gruppo di lavoro attende di conoscere le prossime sentenze della Corte di giustizia in alcune cause vertenti sulla raccolta indiscriminata e in massa di dati.

Per quanto riguarda i mezzi di ricorso, il Gruppo di lavoro accoglie con favore l'istituzione del mediatore quale nuovo meccanismo di ricorso, che potrebbe rappresentare un notevole miglioramento sul piano dei diritti dei cittadini dell'UE nell'ambito delle attività di

intelligence statunitensi. Il Gruppo di lavoro teme, tuttavia, che questa nuova istituzione non sia sufficientemente indipendente e dotata di poteri adeguati per potere assolvere efficacemente i propri compiti e che non garantisca un rimedio soddisfacente in caso di disaccordo.

Analisi comune

Il meccanismo dell'analisi annuale comune citato nel progetto di decisione sull'adeguatezza è un fattore chiave per la credibilità generale dello scudo; il Gruppo di lavoro constata con viva soddisfazione che tale esercizio offrirà l'occasione di riesaminare la decisione sull'adeguatezza. A tale proposito, il Gruppo di lavoro deduce che rappresentanti nazionali del Gruppo di lavoro avranno la possibilità di partecipare a pieno titolo al processo di analisi ma chiede chiarimenti in merito agli accordi presi. Le modalità di esecuzione di tale analisi (compresa la relazione successiva, la sua divulgazione al pubblico e le possibili ripercussioni, nonché il finanziamento) devono essere concordate con largo anticipo rispetto alla data della prima analisi.

Conclusione

Il Gruppo di lavoro prende atto dei principali miglioramenti introdotti dallo scudo rispetto alla decisione invalidata sull'approdo sicuro. Alla luce delle preoccupazioni espresse e dei chiarimenti richiesti, il Gruppo di lavoro sollecita la Commissione a dare risposta alle questioni sollevate, a individuare opportune soluzioni e a fornire i chiarimenti richiesti al fine di migliorare il progetto di decisione sull'adeguatezza e di assicurare che la protezione offerta dallo scudo sia davvero sostanzialmente equivalente a quella garantita nell'Unione.

INDICE

1. INTRODUZIONE

In seguito alla sentenza della Corte di giustizia dell'Unione europea (di seguito "Corte di giustizia") del 6 ottobre 2015 nella causa Schrems[1], il Gruppo di lavoro "articolo 29" (di seguito "Gruppo di lavoro") ha invitato gli Stati membri dell'Unione europea (di seguito "UE" o "Unione") e le altre istituzioni europee ad avviare discussioni con le autorità degli Stati Uniti (di seguito "USA" o "Stati Uniti") al fine di trovare soluzioni politiche, giuridiche e tecniche volte a consentire il trasferimento di dati verso il territorio statunitense nel rispetto dei diritti fondamentali.

Il 2 febbraio 2016, dopo più di due anni di negoziati, la Commissione europea e il Dipartimento del Commercio degli Stati Uniti hanno raggiunto un accordo politico su un nuovo regime per gli scambi transatlantici di dati personali a fini commerciali: lo scudo UE-USA per la privacy (di seguito "scudo"), inteso a sostituire il precedente accordo sull'approdo sicuro tra l'UE e gli USA.

Il 29 febbraio 2016 la Commissione ha pubblicato una comunicazione[2], un progetto di decisione sull'adeguatezza e i testi allegati che costituiranno lo scudo. In conformità con l'articolo 30, paragrafo 1, lettera c), della direttiva 95/46/CE (di seguito "direttiva"), il Gruppo di lavoro ha valutato tali documenti al fine di fornire il proprio parere attuale sul progetto di decisione sull'adeguatezza preparato dalla Commissione, compresi i documenti di base che costituiscono lo scudo. Il Gruppo di lavoro ha effettuato una valutazione della componente commerciale dello scudo e, in parallelo, un'analisi delle garanzie istituite riguardo alle deroghe ai principi dello scudo per finalità di sicurezza nazionale, applicazione della legge e interesse pubblico.

In seguito alla sentenza nella causa Schrems, il Gruppo di lavoro ha avuto diversi incontri con delegazioni dell'amministrazione statunitense, rappresentanti delle organizzazioni della società civile dell'UE e degli USA e studiosi, al fine di preparare la valutazione delle conseguenze della sentenza Schrems. Nel corso della valutazione dello scudo, si sono svolti ulteriori incontri con la Commissione europea e con rappresentanti dell'amministrazione statunitense, in occasione dei quali sono stati forniti chiarimenti, di cui si è parimenti tenuto conto nella formulazione del presente parere. Il Gruppo di lavoro sottolinea che, a questo stadio, tali chiarimenti sono stati puramente informali e non possono essere considerati parte integrante del progetto di decisione sull'adeguatezza, in quanto non sono ancora stati formalizzati per iscritto.

Nondimeno il Gruppo di lavoro apprezza in particolare che, durante gli incontri, il Dipartimento del Commercio si sia impegnato a collaborare con le autorità per la protezione dei dati degli Stati membri dell'UE per quanto riguarda l'applicazione dello scudo e a provvedere affinché sui loro siti web siano pubblicate istruzioni e un'interpretazione giuridica riguardo all'applicazione di tale regime.

[1] Sentenza del 6 ottobre 2015 nella causa C-362/14, Maximilian Schrems contro Data Protection Commissioner (di seguito "Schrems").
[2] COM(2016)117 final, 29 febbraio 2016.

1.1 Osservazioni generali

1.1.1 Portata della valutazione del Gruppo di lavoro

In primo luogo il Gruppo di lavoro ha preso in considerazione il quadro in materia di protezione dei dati applicabile negli Stati membri dell'Unione europea, compreso l'articolo 8 della Convenzione europea dei diritti dell'uomo (di seguito "CEDU") che tutela il diritto al rispetto della vita privata e familiare e gli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea (di seguito "Carta") che tutelano rispettivamente il diritto al rispetto della vita privata e familiare, il diritto alla protezione dei dati personali e il diritto a un ricorso effettivo e a un giudice imparziale. Il Gruppo di lavoro ha inoltre preso in considerazione la giurisprudenza pertinente, nonché le prescrizioni della direttiva.

L'obbligo di un paese terzo di assicurare un livello adeguato di protezione dei dati è stato ulteriormente definito dalla Corte di giustizia nella sentenza Schrems. La Corte non si è limitata a spiegare che le disposizioni della direttiva devono essere interpretate "alla luce dei diritti fondamentali garantiti dalla Carta"[3], e in particolare degli articoli 7 e 8, ma ha anche indicato che l'espressione "livello di protezione adeguato" deve essere intesa 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 della direttiva […], letta alla luce della Carta"[4]. Nel caso della precedente decisione "Approdo sicuro", una siffatta valutazione non è mai stata condotta in maniera sufficientemente dettagliata. Il Gruppo di lavoro ha pertanto valutato il progetto di decisione sull'adeguatezza alla luce del requisito che impone di esaminare se il livello di protezione dei diritti e delle libertà fondamentali sia *sostanzialmente equivalente* a quello garantito all'interno dell'UE. Il Gruppo di lavoro evidenzia che il presente parere contiene le principali preoccupazioni da esso espresse ma che, considerato il breve lasso di tempo trascorso dalla pubblicazione del progetto di decisione sull'adeguatezza, potrebbero emergere successivamente altre questioni problematiche.

Il Gruppo di lavoro riconosce che, definendo il termine "adeguato" figurante all'articolo 25, paragrafo 6, della direttiva, come "sostanzialmente equivalente", la Corte ha precisato ulteriormente il concetto di adeguatezza nella causa Schrems. La Corte ha sottolineato che l'espressione "livello di protezione adeguato", pur non esigendo che il paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione, deve essere intesa 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 della direttiva, letta alla luce della Carta.

[3] Schrems, punto 38.
[4] Schrems, punto 73.

1.1.2 Valutazione della componente commerciale del progetto di decisione sull'adeguatezza

Il Gruppo di lavoro ha già illustrato la modalità con cui ha applicato i principi basilari dell'UE in materia di protezione dei dati ai trasferimenti di dati personali verso paesi terzi nel suo documento di lavoro 12 "Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati"[5]. Il Gruppo ha cercato di individuare le misure di salvaguardia equivalenti che garantiscono un livello di protezione equivalente ai principi garantiti dalla direttiva, segnatamente per quanto riguarda la limitazione della finalità, la qualità e la proporzionalità dei dati, la trasparenza, la sicurezza, i diritti di accesso, rettifica e opposizione, la conservazione dei dati e le restrizioni ai trasferimenti successivi. Un metodo analogo è stato utilizzato nei pareri emessi dal Gruppo di lavoro all'epoca della valutazione della decisione originaria sull'adeguatezza dei principi dell'approdo sicuro[6] nonché nelle raccomandazioni formulate dal Gruppo nella sua lettera indirizzata all'ex vicepresidente della Commissione e commissaria per la giustizia Viviane Reding, pubblicata il 10 aprile 2014[7].

1.1.3 Valutazione delle deroghe per l'accesso da parte delle autorità pubbliche e relative garanzie

La valutazione delle deroghe concernenti l'accesso da parte delle autorità pubbliche ai dati personali contemplati dal regime dello scudo è complessa, soprattutto se si tiene conto che, dopo le rivelazioni di Snowden, le autorità di protezione dei dati e i cittadini sono diventati più consapevoli dei programmi di sorveglianza statunitensi. Il Gruppo di lavoro riconosce e apprezza gli sforzi compiuti dall'amministrazione statunitense per garantire una maggiore trasparenza sui programmi di controllo, nonché la sua disponibilità a includere nel regime dello scudo ulteriori garanzie. Al contempo il Gruppo di lavoro evidenzia che qualunque ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati deve trovare giustificazione in una società democratica. La Corte di giustizia ha criticato il fatto che la decisione "Approdo sicuro" non contenesse dichiarazioni sufficienti quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze. Inoltre la decisione non menziona l'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di tale natura[8].

Il Gruppo di lavoro ha dunque analizzato l'attuale quadro normativo statunitense e le pratiche attuate dai servizi di intelligence statunitensi quali descritte negli allegati del progetto di decisione, nonché le condizioni alle quali sono ammesse ingerenze nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati, che sono tutelati dalla normativa europea.

[5] Adottato dal Gruppo di lavoro il 24 luglio 1998; cfr. in particolare pag, 6.
[6] Cfr. WP62, WP32, WP27, WP23, WP21, WP19, WP15 e WP7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf
[8] Schrems, punti 87 e 88.

Al fine di stabilire se un'eventuale ingerenza possa trovare giustificazione in una società democratica, la valutazione è stata condotta alla luce della giurisprudenza europea in materia di diritti fondamentali che stabilisce quattro garanzie essenziali[9] per le attività di intelligence:

A. il trattamento dovrebbe avvenire in conformità della legge e sulla base di regole chiare, precise e accessibili: ciò significa che chiunque sia ragionevolmente informato dovrebbe essere in grado di prevedere ciò che potrebbe accadere ai dati una volta trasferiti;
B. la necessità e la proporzionalità rispetto ai legittimi obiettivi perseguiti devono essere dimostrate: è necessario trovare un equilibrio tra l'obiettivo per il quale i dati sono raccolti e consultati e i diritti della persona;
C. dovrebbe esistere un meccanismo di vigilanza indipendente che sia efficace e al contempo imparziale: tale funzione potrebbe essere svolta da un giudice o da un altro organo indipendente, purché sufficientemente in grado di espletare i controlli necessari;
D. la persona deve potersi avvalere di mezzi di ricorso efficaci: tutti dovrebbero avere il diritto di difendere i propri diritti dinanzi un organo indipendente.

1.2 Il progetto di decisione sull'adeguatezza

In primo luogo il Gruppo di lavoro si rallegra che sia possibile avviare una nuova procedura di valutazione dell'adeguatezza a meno di sei mesi di distanza dalla sentenza con la quale la Corte di giustizia ha dichiarato invalida la decisione "Approdo sicuro". Dati i massicci trasferimenti di dati che sono effettuati quotidianamente tra l'UE e gli USA e che, secondo il Gruppo di lavoro, sono fondamentali per l'economia di entrambe le sponde dell'Atlantico, occorre creare al più presto chiarezza giuridica.

Tuttavia il Gruppo di lavoro deplora il fatto che, contrariamente alla prassi abitualmente seguita in passato nell'ambito di procedure analoghe, il progetto di decisione sull'adeguatezza pubblicato dalla Commissione non contempli una valutazione globale della legislazione nazionale e degli impegni internazionali degli USA sotto forma di una relazione sull'adeguatezza in linea con l'articolo 25 della direttiva. Per tale ragione il Gruppo di lavoro non è stato in grado di svolgere un'analisi esaustiva del contesto giuridico nel quale lo scudo funzionerà. Il Gruppo di lavoro rileva, ad esempio, che l'attuale progetto di decisione sull'adeguatezza non comprende constatazioni sulla normativa in materia di protezione dei dati e della vita privata vigente negli Stati Uniti, sia a livello federale sia a livello statale, compresa la legislazione settoriale, né sulla normativa che autorizza forme di accesso pubblico non correlate alla sorveglianza. Non è inoltre definito il rapporto esistente fra i trasferimenti di dati nell'ambito dello scudo e quelli effettuati nel quadro di altri meccanismi di accertamento dell'adeguatezza esistenti, quali l'accordo tra l'UE e gli USA sullo scambio dei dati del codice di prenotazione (Passenger Name Records — PNR) e l'accordo concernente il programma di controllo delle transazioni finanziarie dei terroristi (Terrorist Finance Tracking Program — TFTP).

[9] Le garanzie essenziali europee si basano sulla giurisprudenza della Corte di giustizia e della Corte europea dei diritti dell'uomo e sono esposte in maggior dettaglio nel documento del Gruppo di lavoro WP237, pubblicato il 13 aprile 2016.

1.2.1 Ambito d'applicazione del quadro normativo dell'UE in materia di protezione dei dati e, in particolare, dei principi della direttiva 95/46/CE

Il Gruppo di lavoro ricorda che, ai sensi della normativa dell'UE in materia di protezione dei dati, e in particolare, della direttiva (articolo 4, paragrafo 1), la legislazione degli Stati membri si applica non soltanto ai trattamenti effettuati dai titolari del trattamento stabiliti nel loro territorio ma anche laddove i titolari del trattamento (seppur non stabiliti nell'UE), ricorrono a strumenti situati nel territorio dell'Unione, in particolare ai fini della raccolta di dati personali. Pertanto, la legislazione degli Stati membri dell'Unione si applica a qualsiasi trattamento che avvenga prima del trasferimento verso gli Stati Uniti, nel contesto delle attività di un'organizzazione stabilita nel territorio dell'Unione oppure con strumenti situati nell'Unione e usati da un'organizzazione non stabilita nell'UE. Il Gruppo di lavoro chiede che tale aspetto sia esplicitato nel progetto di decisione sull'adeguatezza.

Deve essere chiaro che i principi dello scudo si applicheranno dal momento in cui è effettuato il trasferimento dei dati. Inoltre il Gruppo di lavoro ricorda che i titolari del trattamento che sono stabiliti nell'UE e che trasferiscono dati a un responsabile del trattamento situato negli USA rimangono assoggettati alla normativa dell'UE sulla protezione dei dati.

1.2.2 Mancanza di chiarezza riscontrata nei documenti dello scudo

Poiché i principi e le garanzie previsti dallo scudo sono esposti sia nella decisione sull'adeguatezza sia nei relativi allegati, le informazioni risultano difficili da reperire e sono talvolta incoerenti. Ciò contribuisce a determinare, in generale, una mancanza di chiarezza sul nuovo regime e a complicare l'accesso da parte degli interessati, delle organizzazioni e delle autorità di protezione dei dati. Si ravvisa parimenti una mancanza di chiarezza nel linguaggio utilizzato. Il Gruppo di lavoro esorta pertanto la Commissione a renderlo chiaro e comprensibile su entrambe le sponde dell'Atlantico.

Il Gruppo di lavoro propone di inserire un allegato a se stante nel quale sia fornita la definizione di alcuni termini di base utilizzati nei documenti dello scudo. Un'interpretazione comune e inequivocabile degli obblighi imposti dalla decisione sull'adeguatezza dello scudo è essenziale per il funzionamento efficace di tale regime su entrambe le sponde dell'Atlantico. A tale proposito il Gruppo di lavoro teme che, a causa dei molteplici riferimenti incrociati e del mancato allineamento delle formulazioni e data la complessità dei documenti, possano sorgere difficoltà per quanto riguarda la coerenza, l'intelligibilità e la chiarezza dell'attuazione dello scudo.

In particolare la terminologia usata nei documenti dello scudo non è coerente con il vocabolario generalmente utilizzato nell'UE nel settore della protezione dei dati. Ciò non costituisce necessariamente un problema, purché sia chiaro quale sarebbe la terminologia corrispondente nel diritto dell'Unione (e degli USA). Il Gruppo di lavoro constata con rammarico che tale condizione non è soddisfatta nemmeno nel progetto di decisione sull'adeguatezza. Ad esempio il termine "accesso" è utilizzato nella sezione 3 del progetto di decisione sull'adeguatezza in un'accezione che implica la raccolta di dati personali, anziché la

possibilità di visionare dati già raccolti. L'accesso delle imprese ai dati e il diritto di accesso della persona sono due concetti distinti che non dovrebbero essere confusi.

Il Gruppo di lavoro evidenzia inoltre che la terminologia dovrebbe essere utilizzata in maniera coerente all'interno di tutti i documenti, compreso il progetto di decisione sull'adeguatezza. Attualmente tale requisito non è soddisfatto, ad esempio per quanto riguarda i concetti di "trattamento" e "dati personali", dei quali è fornita, in linea di massima, una corretta definizione nell'allegato II che tuttavia non è applicata in maniera coerente nei vari documenti, con conseguenti lacune nella protezione[10], [11].

Il Gruppo di lavoro apprezza che nei documenti costitutivi dello scudo sia fornita la definizione di alcuni dei termini utilizzati. Manca invece la definizione di altri termini ed espressioni essenziali, quali "procuratore" o "responsabile del trattamento", "dati codificati" "dati resi anonimi" e "persona dell'UE" che, secondo il parere del Gruppo di lavoro, dovrebbero essere chiaramente definiti di comune accordo tra l'UE e gli USA; ciò eviterebbe, ad uno stadio successivo, di creare confusione per i titolari e per i responsabili del trattamento che utilizzano lo scudo, per le autorità di vigilanza e per i cittadini. Una soluzione semplice potrebbe consistere nell'inserimento di un glossario dei termini nelle "domande più frequenti" (FAQ) dello scudo.

Il Gruppo di lavoro richiama inoltre l'attenzione sul principio supplementare 1 (allegato II, punto III.1) con riferimento ai motivi legittimi che giustificano il trattamento di dati sensibili nei casi in cui l'organizzazione non è obbligata a ottenere il consenso esplicito (facoltà di accettazione). Tale principio supplementare 1 può essere interpretato nel senso che esso elenca i motivi legittimi per la raccolta di dati nell'Unione, in quanto tale elenco è simile a quello figurante all'articolo 8 della direttiva. Il Gruppo di lavoro desidera rammentare che qualsiasi trattamento (compresi la raccolta e il trasferimento) di dati sensibili ai sensi della normativa dell'Unione deve essere effettuato per motivi legittimi a norma dell'articolo 8 della direttiva. Lo scudo non può essere interpretato nel senso che esso contempla motivi alternativi a giustificazione di tale trattamento. Ad esempio il Gruppo di lavoro è del parere che un'organizzazione statunitense non possa raccogliere dati soggetti al diritto dell'Unione in

[10] Alcune disposizioni si limitano a elencare alcuni tipi di trattamento dei dati, anziché utilizzare il termine "trattamento". Ciò determina lacune nella protezione. Ad esempio in base alla formulazione del punto III.6.f dell'allegato II, i principi dello scudo sarebbero applicabili soltanto laddove l'organizzazione "conserva, usa o divulga" i dati ricevuti (ovvero non per altre operazioni che rientrano nel "trattamento", quali la raccolta, la registrazione, la modifica, l'estrazione, la consultazione e la cancellazione). La sicurezza dei dati sarebbe imposta soltanto in caso di creazione, detenzione, uso o diffusione di informazioni personali (allegato II, punto II.4). Anche la definizione di dati personali è limitata ai dati "ricevuti" e "registrati". Un ulteriore esempio è costituito dal principio sull'informativa (allegato II, punto II.1.a.iv), il quale stabilisce che l'organizzazione certificata deve informare le persone delle finalità alle quali "raccoglie e usa" i dati che le riguardano. L'allegato II, punto III.9.a.11 menziona unicamente i dati oggetto di "trasferimento" o di "accesso". Sebbene sia evidente che, nella maggioranza dei casi, non si intenda limitare l'ambito di applicazione dei principi o creare lacune nella protezione, la mancanza di coerenza nella terminologia usata rischia di compromettere la protezione offerta. Poiché nei principi è fornita una definizione del termine "trattamento", è indispensabile che tale termine sia utilizzato in maniera coerente, per evitare le carenze attualmente riscontrate. In caso contrario si lascerebbe troppo spazio a un'interpretazione presumibilmente non voluta, che potrebbe condurre a interpretare in modo errato il testo della decisione.

[11] Secondo la definizione di cui all'allegato II, punto I.8.a, per "dati personali" si intendono dati "riguardanti singoli individui (identificati o identificabili)". Il principio supplementare stabilisce tuttavia che, in relazione ai dati sulle risorse umane, i principi dello scudo trovano applicazione solo "per il trasferimento di dati identificati […] o per l'accesso agli stessi". Il Gruppo di lavoro ritiene che tale formulazione lasci aperta la possibilità che il trattamento di dati personali sia effettuato in maniera non conforme ai principi di protezione dei dati sanciti dal diritto dell'Unione e in contrasto con la definizione generale di dati personali nell'ambito dello scudo.

base alla legislazione statunitense sul lavoro (cfr. allegato II, punto III.1.a.v). Il Gruppo di lavoro evidenzia pertanto che qualunque interpretazione del principio supplementare 1 deve determinarne l'applicazione soltanto ai dati sensibili che sono già stati oggetto di trasferimento dopo essere stati raccolti nell'Unione per i motivi legittimi di cui all'articolo 8 della direttiva.

Il Gruppo di lavoro rileva infine una mancanza di chiarezza quanto alla questione di stabilire se possano essere considerati persone dell'UE, e dunque beneficiare della protezione nell'ambito dello scudo, tutti i cittadini dell'Unione oppure tutti coloro che risiedono sul territorio dell'Unione. Tale aspetto è di particolare importanza in relazione al diritto di ricorso, compreso l'accesso al meccanismo di mediazione. Inoltre la decisione sull'adeguatezza dovrebbe chiarire in che misura lo scudo si applicherà anche ai cittadini / residenti dei paesi del SEE e della Svizzera, che in passato erano coperti dal regime dell'approdo sicuro.

1.2.3 Riesame comune e sospensione

Il Gruppo di lavoro si rallegra che la Commissione europea e l'amministrazione statunitense abbiano convenuto di procedere a un riesame periodico dell'applicazione pratica dello scudo. Tale riesame comune è una ben nota prassi seguita da vari anni dai soggetti dell'UE attivi nella protezione dei dati, soprattutto in relazione agli accordi sullo scambio dei dati del codice di prenotazione (PNR) con paesi terzi e all'accordo sul TFTP. Il Gruppo di lavoro apprezza inoltre il fatto che la partecipazione a tale riesame comune sia consentita a un numero imprecisato di rappresentanti delle autorità di protezione dei dati.

Sulla base dell'esperienza che ha maturato negli ultimi anni in relazione a questo tipo di attività, il Gruppo di lavoro si aspetta che il riesame comune dello scudo sia di portata più vasta rispetto alle analisi previste nell'ambito degli accordi PNR e TFTP. In particolare esso auspica che il riesame comune comporti non soltanto riunioni con i rappresentanti di enti, organizzazioni e imprese statunitensi ma anche verifiche in loco di taluni elementi dello scudo. I rappresentanti delle autorità di protezione dei dati che vi partecipano dovrebbero avere la possibilità di presentare proposte in merito a tali verifiche in loco.

Il Gruppo di lavoro ritiene che il riesame comune esiga una valutazione congiunta delle constatazioni. Finora i risultati delle analisi comuni sono stati presentati in un documento di lavoro dei servizi della Commissione che non era soggetto ad approvazione da parte dei membri dell'equipe di riesame esterni alla Commissione. Per quanto riguarda il riesame comune dello scudo, il Gruppo di lavoro auspica che la relazione sulle risultanze possa essere davvero frutto di una consultazione tra le parti. In alternativa le autorità di protezione dei dati potrebbero pubblicare una relazione a se stante sui risultati di tale attività.

Il Gruppo di lavoro ricorda infine che la Commissione ha promesso di rimborsare i costi sostenuti dai rappresentanti del Gruppo nel corso degli esercizi di riesame. Il Gruppo presume che tale principio sarà applicato anche per il riesame comune dello scudo e comunque per un numero ragionevole di rappresentanti delle autorità di protezione dei dati.

Il Gruppo di lavoro raccomanda che, almeno tre mesi prima della data in cui si svolgerà la prima analisi comune dello scudo, la Commissione, l'amministrazione USA e il Gruppo di lavoro ne concordino per iscritto le modalità di esecuzione.

1.2.4 Normativa dell'Unione in corso di revisione

La decisione sull'adeguatezza dello scudo è la prima decisione di adeguatezza che è stata redatta a seguito dell'accordo di principio sul testo del regolamento generale sulla protezione dei dati. Il Gruppo di lavoro ha tuttavia appurato che lo scudo non riflette ancora la situazione futura. Ad esempio non sono stati inclusi nello scudo nuovi importanti concetti quali il diritto alla portabilità dei dati e gli obblighi supplementari imposti ai titolari del trattamento, compresa la necessità di svolgere valutazioni d'impatto sulla protezione dei dati e di osservare i principi della "privacy by design" (tutela della vita privata fin dalla progettazione) e della "privacy by default" (tutela della vita privata per impostazione predefinita). Il Gruppo di lavoro propone pertanto, come per qualsiasi decisione di adeguatezza esistente, di procedere a un riesame dello scudo subito dopo l'entrata in vigore del regolamento generale sulla protezione dei dati. Si auspica che nella decisione finale sull'adeguatezza figuri un riferimento esplicito a tale processo di riesame.

2. VALUTAZIONE DELLA COMPONENTE COMMERCIALE DEL PROGETTO DI DECISIONE SULL'ADEGUATEZZA

2.1 Osservazioni di carattere generale

2.1.1 Miglioramenti

Il Gruppo di lavoro plaude ai miglioramenti apportati dallo scudo e alla volontà dei suoi negoziatori di provare ad affrontare le carenze che il Gruppo aveva riscontrato nel regime dell'approdo sicuro. In particolare, rispetto all'approdo sicuro, nel nuovo regime sono state inserite alcune definizioni chiave quali "dati personali", "trattamento" e "titolare del trattamento", sono stati istituiti meccanismi volti a garantire il controllo dell'elenco degli aderenti allo scudo ed è stato introdotto l'obbligo di effettuare controlli esterni o interni della conformità. I miglioramenti riguardano anche il principio sull'accesso; il Gruppo di lavoro rileva che il nuovo regime riconosce il diritto di rettifica e il diritto alla cancellazione quando i dati sono usati in maniera incompatibile con i principi dello scudo. È inoltre stato chiarito che la persona deve sapere se sono trattati dati che la riguardano e ottenerne la comunicazione.

Il Gruppo di lavoro apprezza inoltre il rafforzamento delle tutele giuridiche in caso di ulteriore trasferimento nonché gli impegni assunti dal Dipartimento del Commercio e dalla Commissione federale del Commercio (Federal Trade Commission — FTC) per fare rispettare gli obblighi imposti dallo scudo.

2.1.2 Applicazione dello scudo alle organizzazioni che agiscono in qualità di responsabili del trattamento (procuratore)

Purtroppo è ancora poco chiaro in che misura i principi dello scudo siano applicabili alle organizzazioni certificate che ricevono dati personali dall'Unione a fini esclusivi di trattamento (i cosiddetti "procuratori" o "responsabili del trattamento"). Sebbene le disposizioni di cui all'allegato II, punto III.10.a., menzionino effettivamente i trasferimenti di dati ad organizzazioni certificate per tali finalità, ossia facciano riferimento all'obbligo di concludere un contratto, non vi è alcuna indicazione quanto alla modalità di applicazione dei principi dello scudo ai responsabili del trattamento (procuratori). Ciò è fonte di incertezza sia per le organizzazioni statunitensi certificate che ricevono dati a fini di trattamento sia per le imprese dell'Unione che trasferiscono dati verso organizzazioni certificate che agiscono in qualità di responsabili del trattamento, nonché per le persone i cui dati sono trattati. Pertanto sarà difficile stabilire quali siano effettivamente i compiti delle organizzazioni aderenti allo scudo che trattano dati personali ricevuti dall'UE in qualità di responsabili del trattamento. È dunque evidente che servono chiarimenti a riguardo.

Occorre tenere presente che diversi obblighi contemplati dai principi non sono pertinenti per i responsabili del trattamento, in quanto è sempre il titolare del trattamento a stabilire le finalità e i mezzi del trattamento dei dati (cfr. la definizione di "titolare del trattamento" di cui all'allegato II, punto I.8.c). Proprio per tale ragione alcuni degli obblighi previsti dai principi, se applicati a un'organizzazione che agisca in qualità di procuratore, potrebbero essere in contrasto con il contratto obbligatorio sul trattamento dei dati previsto dal diritto dell'Unione (il contratto di cui all'allegato II, punto III.10.a.). Ad esempio solitamente il contratto sul trattamento dei dati non autorizza il responsabile del trattamento (procuratore) ad effettuare l'ulteriore trasferimento dei dati ad un terzo titolare del trattamento, nemmeno nelle circostanze menzionate all'allegato II, punto II.3.a. L'ulteriore trasferimento a un terzo procuratore dovrebbe essere autorizzato soltanto previa approvazione del titolare del trattamento. Inoltre, conformemente alle prescrizioni del diritto dell'Unione, il responsabile del trattamento (procuratore) non sarà in grado di fornire agli interessati tutte le indicazioni previste dal principio sull'informativa (allegato II, punto II.1), ad esempio perché l'organizzazione non stabilisce le finalità del trattamento.

È dunque di fondamentale importanza chiarire nei principi che, in caso di discordanze, prevalgono le disposizioni del contratto sul trattamento dei dati e, in particolare, le istruzioni dell'organizzazione che effettua il trasferimento dei dati all'esterno dell'Unione. In assenza di tale precisazione, i principi potrebbero essere interpretati e applicati in maniera tale da attribuire un'eccessiva capacità di controllo al procuratore; in tal caso l'esportatore dei dati dell'UE correrebbe il rischio di non adempiere agli obblighi che gli incombono in quanto titolare del trattamento in base alla normativa dell'UE sulla protezione dei dati cui è assoggettato quando trasferisce dati verso un'organizzazione aderente allo scudo che agisce in qualità di procuratore. Inoltre questa mancanza di chiarezza induce a ritenere che il responsabile del trattamento possa riutilizzare i dati a suo piacimento.

Inoltre dovrebbero essere fornite regole precise per i casi nei quali un'organizzazione agisce in qualità di responsabile del trattamento (procuratore), al fine di garantire che essa segua le istruzioni del titolare del trattamento. Occorrerebbe precisare che le organizzazioni statunitensi che ricevono dati a fini esclusivi di trattamento non possono decidere di effettuarne il trattamento per proprio conto. In assenza di norme specifiche applicabili alle organizzazioni che agiscono in qualità di responsabili del trattamento è difficile stabilire in base a quali regole il responsabile del trattamento (procuratore) possa autocertificarsi.

2.1.3 Limitazione dell'obbligo di aderire ai principi

L'allegato II, punto I.5., prevede, tra l'altro, alcune deroghe ai principi nei casi in cui i dati coperti dallo scudo siano utilizzati per motivi di sicurezza nazionale[12], interesse pubblico o amministrazione della giustizia ovvero in virtù di disposizioni legislative o regolamentari o decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti o autorizzazioni esplicite. In mancanza di una conoscenza approfondita della normativa statunitense a livello federale e statale, per il Gruppo di lavoro è difficile valutare l'ambito di applicazione di tale deroga e stabilire se tali limitazioni possano trovare giustificazione in una società democratica. Si ritiene essenziale che la Commissione europea includa nel suo progetto di decisione sull'adeguatezza anche un'analisi del livello di protezione nei casi in cui si applicano tali deroghe. Il Gruppo di lavoro invita la Commissione a garantire che l'Unione sia informata in merito a qualsiasi disposizione legislativa o regolamentare, attualmente in vigore o adottata in futuro negli USA, in grado di influire sull'adesione ai principi.

2.1.4 Assenza di un principio di limitazione della conservazione dei dati

Il principio della durata limitata della conservazione dei dati (articolo 6, paragrafo 1, lettera e), della direttiva) costituisce un principio essenziale della legislazione dell'Unione in materia di protezione dei dati; esso stabilisce che i dati personali devono essere conservati soltanto per il periodo necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati.

Tuttavia nei documenti costitutivi dello scudo il Gruppo di lavoro non ravvisa alcun riferimento alla necessità che i responsabili del trattamento garantiscano la cancellazione dei dati non appena le finalità della raccolta o del successivo trattamento vengano meno. Sembra pertanto che i principi non impongano alle organizzazioni certificate un limite temporale per la conservazione dei dati paragonabile a quello previsto dal principio della durata limitata della conservazione dei dati sancito dal diritto dell'Unione.

La formulazione del principio sull'integrità dei dati e la limitazione della finalità (allegato II, punto II.5) non può in alcun modo essere intesa nel senso che essa impone all'organizzazione che agisce come titolare del trattamento l'obbligo di cancellare i dati una volta che gli stessi non sono più necessari per le finalità della loro raccolta o del loro successivo trattamento o, se

[12] Per ulteriori osservazioni sull'uso dei dati personali coperti dallo scudo a fini di sicurezza nazionale e per esigenze di amministrazione della giustizia, cfr. rispettivamente il capitolo 3 e il capitolo 4.

l'organizzazione agisce come responsabile del trattamento, l'obbligo di cancellare i dati dopo la cessazione dell'accordo di servizi.

Il Gruppo di lavoro sottolinea che l'assenza di disposizioni volte a limitare la durata della conservazione dei dati nell'ambito dello scudo offre alle organizzazioni la possibilità di conservare i dati finché lo desiderano, anche dopo avere abbandonato lo scudo; ciò è in contrasto con il principio fondamentale della durata limitata della conservazione dei dati.

2.1.5 Mancanza di garanzie per le decisioni automatizzate che producono effetti giuridici o hanno effetti significativi nei confronti di una persona

Lo scudo non offre alcuna garanzia giuridica nei casi in cui la persona è sottoposta a una decisione che produce effetti giuridici o ha effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento ecc.

La necessità di fornire garanzie giuridiche per le decisioni automatizzate (che producono effetti giuridici o che hanno effetti significativi nei confronti di una persona) al fine di garantire un livello di protezione adeguato è già stata sottolineata dal Gruppo di lavoro nel documento 12.

Tale necessità diventa tanto più evidente in quanto le nuove tecnologie in continua evoluzione consentono a un maggior numero di imprese di contemplare la possibile introduzione di sistemi decisionali automatizzati che potrebbero avere per effetto di indebolire la posizione delle persone, privandole di ogni possibilità di ricorso contro tali decisioni. Laddove le decisioni emananti soltanto da tali sistemi automatizzati incidono sulla situazione giuridica delle persone o hanno effetti significativi nei loro confronti (ad esempio tramite l'inserimento della persona in una lista nera e la conseguente privazione dei suoi diritti), è essenziale fornire garanzie sufficienti, compreso il diritto di conoscere la logica su cui si basa il trattamento e di chiedere che venga riconsiderata la possibilità di una decisione su base non automatizzata.

2.1.6 Periodo di transizione per le relazioni commerciali in essere

I principi dello scudo si applicano immediatamente alla data di certificazione. Tuttavia le organizzazioni che si certificano nei primi due mesi successivi alla data di efficacia del regime dello scudo sono tenute a conformare al più presto eventuali rapporti commerciali preesistenti con terzi al principio sulla responsabilità in caso di ulteriore trasferimento; in ogni caso esse dovranno assicurare tale conformità trascorsi non oltre nove mesi dall'autocertificazione.

Ciò significa che, per quanto necessario, i contratti esistenti devono essere allineati ai principi in un arco di tempo compreso tra due e nove mesi dopo la certificazione. Nel corso di tale periodo di transizione, è sufficiente applicare i principi di informativa e di scelta. Il Gruppo di lavoro insiste sul fatto che i trasferimenti possono avere luogo sulla base dello scudo soltanto dal momento in cui l'organizzazione è in grado di assicurare la piena conformità con tutti gli

obblighi dello scudo. La possibilità di inviare dati durante il periodo di transizione senza che il destinatario sia nelle condizioni di potere rispettare appieno i principi dello scudo non soddisfa le condizioni per il trasferimento legittimo ed è pertanto inaccettabile.

2.2 Osservazioni specifiche

2.2.1 Trasparenza

a) Osservazioni di carattere generale sull'informativa

Il Gruppo di lavoro accoglie positivamente le prescrizioni più esaustive e dettagliate stabilite nel quadro del principio sull'informativa, segnatamente l'obbligo di fornire, nell'ambito dell'informativa, un collegamento ipertestuale o un indirizzo Internet in cui reperire l'elenco degli aderenti allo scudo e di informare le persone in merito al loro diritto di accesso, nonché ai meccanismi di risoluzione alternativa delle controversie[13]. Tuttavia il Gruppo di lavoro suggerisce di esplicitare maggiormente gli altri diritti contemplati (rettifica o cancellazione quando le informazioni non sono accurate o sono trattate in violazione dei principi).

I documenti costitutivi dello scudo sollevano preoccupazioni per quanto riguarda il momento nel quale un'organizzazione aderente deve informare l'interessato. L'allegato II, punto II.1.b, chiarisce che queste "indicazioni vanno formulate […] quando si tratta del primo invito a fornire informazioni personali alle organizzazioni rivolto ad una persona oppure non appena ciò risulti successivamente possibile, ma comunque prima che le organizzazioni utilizzino o rivelino per la prima volta a terzi tali informazioni per finalità diverse da quelle per le quali le informazioni stesse erano state originariamente raccolte". Il Gruppo di lavoro ritiene che in molte situazioni le organizzazioni aderenti allo scudo non provvederanno direttamente alla raccolta dei dati presso gli interessati e pertanto le indicazioni dovrebbero essere trasmesse all'interessato nel momento in cui l'organizzazione aderente allo scudo registra i dati.

Il Gruppo di lavoro rileva che l'attuazione effettiva degli obblighi in relazione al principio sull'informativa e alla politica della privacy dovrebbe essere valutata in occasione del primo riesame annuale dello scudo.

b) Politica pubblica di tutela della sfera privata

Il Gruppo di lavoro constata con soddisfazione che è oramai esplicito che il Dipartimento del Commercio provvederà a verificare se le imprese, ove dispongano di un sito web pubblico, vi abbiano pubblicato la politica della privacy seguita o se, qualora non dispongano di un sito web pubblico, abbiano indicato il luogo in cui il pubblico può consultare la loro politica della privacy[14].

[13] Allegato II, punto II.1; il Gruppo di lavoro rinvia inoltre alla seconda raccomandazione formulata dalla Commissione nella comunicazione COM(2103)847 nonché alla lettera del Gruppo di lavoro, del 10 aprile 2041, indirizzata alla vicepresidente Reding, con particolare riferimento al quarto punto della raccomandazione relativa alla trasparenza.

[14] Cfr. la prima raccomandazione formulata dalla Commissione europea nella sua comunicazione COM(2013)847 e la lettera del Gruppo di lavoro, del 10 aprile 2014, indirizzata alla vicepresidente Reding, con particolare riferimento al terzo punto della raccomandazione relativa alla trasparenza.

c) Pubblicazione delle condizioni di tutela della privacy figuranti nei contratti conclusi con i responsabili del trattamento

Tra le condizioni alle quali l'organizzazione aderente allo scudo può trasferire dati al responsabile del trattamento (procuratore), lo scudo prevede che le organizzazioni autocertificate debbano "a richiesta del Dipartimento, fornirgli un sunto o un estratto rappresentativo delle pertinenti disposizioni sulla tutela della vita privata contenute nel contratto concluso con il procuratore" (cfr. allegato II, punto II.3.b.v). Il Gruppo di lavoro accoglie con favore l'inserimento di questo obbligo di trasparenza nei confronti del Dipartimento del Commercio.

2.2.2 Scelta

Lo scudo prevede il diritto di scegliere (facoltà di rifiuto) se le informazioni personali possano essere rivelate a terzi ovvero usate per finalità sostanzialmente diverse[15] (allegato II, parte III, punto 2). La persona può inoltre esercitare in qualunque momento la facoltà di rifiuto in rapporto all'uso delle informazioni personali che la riguardano a fini di marketing diretto (Allegato II, punto III.12.a)[16].

Fatta eccezione per i casi di uso delle informazioni a fini di marketing diretto, non sono fornite indicazioni particolareggiate sulla modalità o sui tempi di esercizio di tale facoltà di rifiuto. Il Gruppo di lavoro ritiene che il solo riferimento all'esistenza di tale diritto nella politica della privacy non possa essere sufficiente e che la *singola persona* dovrebbe essere posta in condizione di esercitare tale diritto *prima* che le informazioni personali siano divulgate o riutilizzate.

Inoltre il Gruppo di lavoro evidenzia che lo scudo dovrebbe prevedere un diritto di opposizione generale (per motivi cogenti che attengono alla situazione particolare dell'interessato), inteso come il diritto della persona di chiedere la cessazione del trattamento dei dati che la riguardano ogni qual volta esistano motivi legittimi cogenti che attengono alla sua situazione particolare[17]. Il Gruppo di lavoro raccomanda vivamente che il progetto di decisione sull'adeguatezza stabilisca in modo chiaro che il diritto di opposizione dovrebbe esistere in qualsiasi momento; raccomanda inoltre di non circoscrivere la facoltà di opposizione al solo ambito d'uso dei dati per finalità di marketing diretto[18].

Il Gruppo di lavoro teme che la mancanza di una definizione di ciò che può essere considerato una finalità "sostanzialmente diversa" possa creare confusione e incertezza giuridica. Occorrerebbe precisare che il principio sulla scelta non può comunque essere utilizzato per eludere il principio di limitazione della finalità[19]. Il principio sulla scelta dovrebbe essere

[15] Il principio supplementare 14.c.i prevede la possibilità di ritirarsi da una sperimentazione clinica; tale facoltà può essere interpretata come la facoltà di rifiutare o revocare il consenso.
[16] Tale facoltà è identica a quella prevista nel regime Approdo sicuro (F.A.Q. 12); nessuna modifica è stata apportata a tale riguardo.

[18] Cfr. la lettera indirizzata dal Gruppo di lavoro alla vicepresidente Reding, raccomandazione relativa alla scelta.
[19] Un esempio concreto di ulteriore trattamento incompatibile che è autorizzato in base al principio sulla scelta è costituito dal principio supplementare 9.b.i (cfr. a tale riguardo l'osservazione del Gruppo di lavoro relativa ai dati sulle risorse umane).

applicabile soltanto quando la finalità è sostanzialmente diversa ma comunque compatibile, in quanto il trattamento per finalità incompatibili non è consentito (allegato II, punto II.5.a). Deve essere chiaro che la facoltà di rifiuto non può consentire all'organizzazione di utilizzare i dati per finalità incompatibili. Pertanto il Gruppo di lavoro raccomanda di armonizzare la relativa formulazione utilizzando un'unica espressione definita (ad esempio "finalità sostanzialmente diverse ma comunque compatibili").

Sarebbe utile fornire precisazioni riguardo ai casi nei quali la decisione di trattare i dati per una finalità diversa o per comunicare informazioni ricade nella sfera di applicazione del diritto dell'Unione. In tale situazione i requisiti giuridici dell'Unione che normalmente riguardano tale trattamento (quali il divieto di trattare dati per finalità incompatibili, l'esistenza di un motivo legittimo per procedere al trattamento e la necessità di informare l'interessato) saranno direttamente applicabili anche all'organizzazione statunitense che ricade nella sfera di applicazione del diritto dell'UE. In pratica ciò significa che spetta all'esportatore dell'UE che adotta tale decisione garantire la trasparenza e la liceità del trattamento in conformità del diritto dell'Unione. Pertanto il principio sulla scelta si applica soltanto laddove la decisione sia adottata unicamente dall'organizzazione statunitense aderente allo scudo non assoggettata al diritto dell'Unione.

2.2.3 Ulteriore trasferimento

a) Ambito di applicazione

Il Gruppo di lavoro esprime preoccupazione riguardo all'ulteriore trasferimento di dati personali da parte di un'organizzazione certificata come aderente allo scudo negli USA verso un destinatario situato in un paese terzo.

Lo scudo non dovrebbe essere considerato soltanto uno strumento per il trasferimento di dati dell'UE dall'Unione verso gli Stati Uniti; esso sarà utilizzato anche per il trasferimento di dati dagli Stati Uniti verso paesi terzi. Le disposizioni relative all'ulteriore trasferimento sono dunque una componente importante dello scudo che dovrebbe fornire garanzie sufficienti e un livello di protezione adeguato in caso di ulteriore trasferimento di dati fuori dagli Stati Uniti. Sorge in particolare un problema per quanto riguarda la sicurezza nazionale e l'applicazione della legge.

Il principio sulla responsabilità in caso di ulteriore trasferimento previsto dallo scudo non è limitato ai titolari del trattamento o ai responsabili del trattamento o procuratori stabiliti negli USA che ricevono i dati. Pertanto l'ulteriore trasferimento verso un paese terzo potrebbe avvenire sulla base dello scudo anche qualora la legislazione del paese terzo preveda il pubblico accesso ai dati personali, ad esempio per finalità di controllo. Tale possibilità espone i dati dell'UE a un rischio di ingerenze ingiustificate nella tutela dei diritti fondamentali.

In tutti i casi di ulteriore trasferimento verso un paese terzo, ciascuna organizzazione aderente allo scudo dovrebbe avere l'obbligo di valutare, prima del trasferimento, le disposizioni vincolanti della legislazione nazionale del paese terzo applicabile all'importatore dei dati.

Qualora vi sia il rischio che il trasferimento pregiudichi le garanzie, gli obblighi e il livello di protezione offerto dallo scudo, l'organizzazione statunitense aderente allo scudo che agisce in qualità di responsabile del trattamento (procuratore) ne dà immediata comunicazione al titolare del trattamento dell'Unione prima di effettuare qualsiasi ulteriore trasferimento. In questi casi l'esportatore dei dati ha facoltà di sospendere il trasferimento dei dati e/o di risolvere il contratto. Ove sussista un siffatto rischio, l'organizzazione aderente allo scudo che agisce in qualità di responsabile del trattamento non dovrebbe essere autorizzata all'ulteriore trasferimento dei dati, in quanto ciò avrebbe per effetto di compromettere l'assolvimento del suo obbligo di offrire lo stesso livello di protezione previsto dai principi in caso di ulteriore trasferimento (cfr. allegato II, punto II.3.a).

Analogamente, nel caso di una modifica della normativa del paese terzo che possa pregiudicare le garanzie, gli obblighi e il livello di protezione previsti dallo scudo, l'organizzazione statunitense aderente allo scudo che agisce in qualità di responsabile del trattamento (procuratore) dovrebbe avere l'obbligo, nell'ambito dello scudo, di comunicare all'esportatore dei dati, non appena ne abbia conoscenza, la modifica intervenuta; in tal caso l'esportatore dei dati ha facoltà di sospendere il trasferimento dei dati e/o di risolvere il contratto. Pertanto in tale circostanza l'organizzazione aderente allo scudo che agisce in qualità di titolare del trattamento non dovrebbe essere autorizzata all'ulteriore trasferimento in quanto ha l'obbligo di offrire lo stesso livello di protezione previsto dai principi (cfr. allegato II, punto II.3.a).

Il Gruppo di lavoro rammenta la sua posizione secondo cui qualora il titolare del trattamento dell'Unione sia a conoscenza di un ulteriore trasferimento verso terzi ubicati al di fuori degli Stati Uniti ancora prima che il trasferimento verso gli USA abbia luogo, o qualora il titolare del trattamento dell'UE sia corresponsabile della decisione che autorizza ulteriori trasferimenti, il trasferimento dovrebbe essere considerato un trasferimento diretto dall'Unione verso il paese terzo rispetto agli Stati Uniti. Ciò significa che si applicano al trasferimento gli articoli 25 e 26 della direttiva, anziché il principio sull'ulteriore trasferimento previsto dallo scudo.

b) Trasferimenti dall'organizzazione aderente allo scudo al terzo titolare del trattamento

Il Gruppo di lavoro accoglie con favore l'obbligo di stipulare contratti (allegato II, punto II.3.a) al fine di garantire che il terzo titolare del trattamento offra almeno lo stesso livello di protezione della privacy previsto dai principi dello scudo. L'obiettivo è assicurare che i dati personali continuino a beneficiare di una protezione adeguata, anche dopo il loro ulteriore trasferimento. Il Gruppo di lavoro formula tuttavia alcune osservazioni sulle condizioni proposte.

<u>Assenza di un riferimento al principio sulla limitazione della finalità</u>

Il Gruppo di lavoro raccomanda di inserire un chiaro riferimento al principio sulla limitazione della finalità (allegato II, punto II.5) tra le condizioni che regolano l'ulteriore trasferimento al terzo titolare del trattamento (allegato II, punto II.3.a). Ciò servirebbe a precisare che

l'ulteriore trasferimento non è consentito se il terzo titolare del trattamento si appresta a trattare i dati per finalità incompatibili.

Esenzione dall'obbligo di contratto per i trasferimenti tra titolari del trattamento all'interno di un gruppo di società

È prevista un'esenzione dall'obbligo di contratto per i trasferimenti infragruppo tra titolari del trattamento. In tale scenario, i principi stabiliscono che la continuità della protezione può essere garantita dalle norme vincolanti d'impresa o da "altri strumenti infragruppo (ad esempio, i programmi di conformità e controllo)" (allegato II, punto III.10.b). Il Gruppo di lavoro ritiene che il riferimento ad "altri strumenti infragruppo" non garantisca l'assunzione di impegni giuridicamente vincolanti da parte degli altri membri del gruppo. Poiché il Gruppo di lavoro e la legislazione dell'Unione[20] tendono a privilegiare gli impegni vincolanti quale presupposto per i trasferimenti infragruppo, è importante evitare che lo scudo sia utilizzato in maniera tale da eludere tale obbligo. Il Gruppo di lavoro ricorda che, in ogni caso, l'ulteriore trasferimento dagli Stati Uniti verso paesi terzi programmato ancora prima che abbia luogo il trasferimento verso gli Stati Uniti, o soggetto a controllo congiunto con il titolare del trattamento dell'UE[21], deve essere considerato un trasferimento diretto dall'Unione al paese terzo rispetto agli Stati Uniti. Al trasferimento si applicano pertanto gli articoli 25 e 26 della direttiva.

c) Trasferimenti dall'organizzazione aderente allo scudo al terzo responsabile del trattamento (procuratore)

Il Gruppo di lavoro si rallegra che la conclusione di un contratto in caso di ulteriore trasferimento sia ora obbligatoria per i soggetti che ricevono i dati in qualità di responsabili del trattamento (procuratori), indipendentemente dalla loro partecipazione allo scudo o dal fatto che essi rientrino nell'ambito di applicazione di un altro meccanismo di accertamento dell'adeguatezza. Il Gruppo plaude inoltre alle garanzie supplementari che accompagnano questi ulteriori trasferimenti (allegato II, punti II.3.a.i, II.3.a.iii, II.3.a.iv, II.3.a.v e II.7.d). L'ultimo punto (allegato II, punto II.7.d) riguarda l'obbligo di mantenere la responsabilità quando i dati sono inoltrati a un procuratore. Sembra tuttavia che tale garanzia non si applichi nel caso in cui l'organizzazione abbia scelto di collaborare con un'autorità di protezione dei dati (cfr. allegato II, punto III.5.a in fine). Il Gruppo di lavoro non comprende il motivo di tale esenzione e ritiene che la responsabilità debba valere anche in questo caso.

Assenza di riferimenti al principio sulla limitazione della finalità

Il Gruppo di lavoro rileva che, in base al principio sulla responsabilità, in caso di ulteriore trasferimento (allegato II, punto II.3) i dati personali possono essere trasferiti a un terzo che agisce come procuratore soltanto per finalità determinate e limitate ma tale principio non stabilisce esplicitamente che tali finalità determinate e limitate debbano essere compatibili

[20] La necessità di impegni vincolanti e azionabili è sottolineata anche nel regolamento generale sulla protezione dei dati qualunque sia lo strumento utilizzato (norme vincolanti d'impresa, clausole contrattuali, codici di condotta o certificazione).
[21] Ad esempio per i dati sulle risorse umane.

con le finalità per le quali i dati sono stati inizialmente raccolti e con le istruzioni del titolare del trattamento. Serve maggiore chiarezza a tale riguardo. Il Gruppo di lavoro ritiene pertanto che la decisione sull'adeguatezza debba fornire indicazioni più dettagliate, ad esempio attraverso un chiaro riferimento al principio sulla limitazione della finalità (allegato II, punto II.5), in base al quale i dati non possono essere trattati (e comunicati) per finalità incompatibili con il principio sull'ulteriore trasferimento (in aggiunta al principio sulla scelta).

Necessità di ulteriori obblighi supplementari per le organizzazioni aderenti allo scudo che, in qualità di responsabili del trattamento (procuratori), effettuano l'ulteriore trasferimento di dati a un altro responsabile del trattamento (procuratore)

L'assenza di norme chiare applicabili ai casi nei quali l'organizzazione aderente allo scudo agisce in qualità di procuratore (ovvero per conto di un titolare del trattamento dell'Unione) implica una lacuna e potrebbe impedire al titolare del trattamento dell'UE di mantenere il controllo delle operazioni. L'organizzazione aderente allo scudo che riceve i dati in quanto procuratore di un titolare del trattamento dell'Unione è tenuta a rispettare le istruzioni di quest'ultimo. Tale obbligo dovrebbe essere enunciato esplicitamente nei principi, in modo da garantire che il mancato rispetto di tali istruzioni comporti non soltanto l'inadempimento del contratto (allegato II, punto III.10.a.ii) ma anche una violazione dei principi dello scudo.

La possibilità che un'organizzazione aderente allo scudo la quale agisca come procuratore effettui un ulteriore trasferimento di dati verso un terzo procuratore deve essere resa trasparente nei confronti del titolare del trattamento e deve essere soggetta alla previa approvazione di quest'ultimo. Pertanto occorrerebbe precisare che è il contratto concluso tra il procuratore e il titolare del trattamento dell'UE (contratto che nella FAQ 10 è indicato come "contratto a norma dell'articolo 17") a stabilire se l'ulteriore trasferimento è consentito[22].

Le condizioni attualmente applicabili all'ulteriore trasferimento dei dati a un procuratore presuppongono che l'organizzazione aderente allo scudo agisca in qualità di titolare del trattamento e possa pertanto decidere in autonomia l'eventuale intervento di un terzo procuratore. Tuttavia ciò non dovrebbe essere possibile quando l'organizzazione aderente allo scudo agisce in qualità di procuratore, perché in tal caso il titolare del trattamento dell'UE sarebbe privato della sua capacità di controllo.

Le pertinenti disposizioni riguardanti la tutela della sfera privata contenute nel contratto concluso con il terzo procuratore devono essere rese note al titolare del trattamento e assicurare almeno lo stesso livello di protezione offerto dal contratto concluso con il titolare del trattamento.

2.2.4 Integrità dei dati e limitazione della finalità

a) Proporzionalità

[22] Cfr. la lettera del Gruppo di lavoro, del 10 aprile 2014, indirizzata alla vicepresidente Reding, punto 4 della raccomandazione relativa all'ulteriore trasferimento.

In ordine a una questione di minore rilevanza, il Gruppo di lavoro rinvia alla sua lettera indirizzata alla vicepresidente Reding nella quale ha osservato che il trattamento di dati personali potrebbe, anche in caso di rigoroso rispetto dei principi sull'informativa e sulla scelta, non essere proporzionato rispetto agli interessi, ai diritti e alle libertà dell'interessato o della società. Il Gruppo di lavoro ha aggiunto che il principio della proporzionalità o ragionevolezza deve essere rispettato in tutte le fasi del trattamento e dovrebbe essere applicabile in aggiunta ai principi sull'informativa e sulla scelta[23].

Lo scudo (allegato II, punto II.5.a) stabilisce che le informazioni devono essere limitate alle informazioni pertinenti ai fini del trattamento. Il Gruppo di lavoro preferirebbe che tale formulazione fosse modificata nella decisione finale sull'adeguatezza, in quanto il solo fatto che i dati siano pertinenti ai fini del trattamento non è sufficiente a garantire la proporzionalità del trattamento. Per soddisfare il principio di proporzionalità, il trattamento dovrebbe essere limitato ai dati che sono necessari ai fini del trattamento in questione.

b) Accuratezza

Il principio sull'integrità dei dati e la limitazione della finalità (allegato II, punto II.5) stabilisce inoltre quanto segue: "Per quanto necessario al conseguimento di tali finalità, l'organizzazione deve adottare misure ragionevoli per assicurare che i dati personali siano affidabili per l'uso previsto, accurati, completi e aggiornati". Il Gruppo di lavoro rileva che questa formulazione è esattamente identica a quella utilizzata nell'accordo sull'approdo sicuro. Il Gruppo di lavoro dubita che sia opportuno inserire il testo "per quanto necessario al conseguimento di tali finalità", in quanto a suo parere l'accuratezza dei dati non dovrebbe dipendere dalla finalità del trattamento. Il Gruppo di lavoro auspica che tale nesso non sia stabilito nella decisione finale sull'adeguatezza.

c) Limitazione della finalità

Quando un titolare del trattamento stabilito nell'Unione trasferisce dati personali a un'organizzazione statunitense, l'esportatore dei dati dovrebbe informare esplicitamente l'organizzazione statunitense in merito alle finalità per le quali i dati erano stati originariamente raccolti. Tale requisito è essenziale per stabilire se dopo il trasferimento si verifichi un cambiamento di finalità che determini l'applicazione dei principi sull'informativa e sulla scelta e inoltre contribuirebbe alla ripartizione di rischi e responsabilità.

Il principio sull'integrità dei dati e la limitazione della finalità (allegato II, punto II.5) stabilisce che l'organizzazione non può trattare le informazioni personali in modo incompatibile con le finalità per cui sono state raccolte o con quelle successivamente autorizzate dalla persona. Il principio sulla scelta (allegato II, punto II.2) prevede tuttavia il consenso esplicito (facoltà di accettazione) all'"utilizzo" di informazioni sensibili (ossia informazioni personali concernenti condizioni mediche o sanitarie, origine etnica o razziale, opinioni politiche, credenze filosofiche o religiose, appartenenza a sindacati o informazioni concernenti la vita sessuale dell'individuo, nonché informazioni sui precedenti

[23] Cfr. la lettera del Gruppo di lavoro, del 10 aprile 2014, indirizzata alla vicepresidente Reding, pag. 8.

penali) per finalità sostanzialmente diverse da quelle per cui erano state originariamente raccolte o da quelle successivamente autorizzate dalla persona. L'obbligo di ottenere il consenso esplicito della persona non è previsto nelle situazioni menzionate nel principio supplementare 1.a (allegato II, punto III.1.a). Per quanto riguarda le informazioni personali non sensibili, è contemplata la facoltà di rifiuto.

Il Gruppo di lavoro rileva che l'ambito di applicazione del principio sulla limitazione della finalità è diverso nel quadro dei principi sull'informativa, sulla scelta e sull'integrità dei dati e la limitazione della finalità. In effetti il termine "incompatibile" riferito alla finalità e l'espressione "finalità sostanzialmente diverse" sono utilizzati nello stesso testo senza una definizione chiara dei due concetti[24].

Il Gruppo di lavoro teme seriamente che, data la mancanza di coerenza, possa essere molto difficile conciliare il principio sull'integrità dei dati e la limitazione della finalità (allegato II, punto II.5) con il principio sulla scelta (allegato II, punto II.2), in quanto il primo stabilisce che non si possono trattare i dati in modo incompatibile con le finalità per cui sono stati raccolti, mentre il secondo prevede un meccanismo con il quale la persona può esercitare la facoltà di rifiuto nel caso in cui i dati siano trattati per finalità sostanzialmente diverse da quelle originarie.

Pertanto il principio sulla scelta può essere interpretato nel senso che autorizza un ulteriore trattamento incompatibile[25]. Secondo il Gruppo di lavoro, è necessario esplicitare che un'organizzazione non è autorizzata a trattare dati per finalità sostanzialmente diverse quando tali finalità risultino incompatibili in base al principio sulla limitazione della finalità. In altri termini deve essere chiaro che il principio sulla scelta non costituisce una deroga al principio sulla limitazione della finalità.

Inoltre se l'ulteriore trattamento può essere considerato compatibile, allora dovrebbero comunque applicarsi anche i principi sull'informativa e sulla scelta.

2.2.5 Eccezioni giornalistiche

Le eccezioni giornalistiche al trattamento di dati personali sono contemplate dal principio supplementare 2 (allegato II, punto III.2). Tali disposizioni sembrano riflettere la tutela della libertà di espressione garantita dalla Costituzione degli Stati Uniti. Pertanto i documenti costituitivi dello scudo stabiliscono che "non sottostanno agli obblighi dello scudo […] le informazioni personali […] rinvenute in materiale già pubblicato e divulgate a partire da archivi di mezzi di informazione" (allegato II, punto III.2.b). Tale esenzione sembra includere qualsiasi ulteriore trattamento da parte di qualsiasi titolare o responsabile del trattamento, ovvero non sembra essere limitata all'ulteriore trattamento per finalità giornalistiche.

[24] Il Gruppo di lavoro ha inoltre rilevato l'uso di altre espressioni: "uso non compatibile" (allegato II, punto III.14.b.ii), uso "per finalità differenti" (allegato II, punto III. 9.b.i), uso "per finalità diverse da quelle per le quali le informazioni stesse erano state originariamente raccolte" (allegato II, punto II.1.b). Data la mancanza di chiarezza, potrebbero non sussistere garanzie sufficienti in relazione al principio sulla limitazione della finalità.

[25] Cfr. anche l'osservazione relativa al principio sulla scelta. Secondo il Gruppo di lavoro il fatto che le norme riguardanti l'ulteriore trasferimento (allegato II, punto II.3) si riferiscano unicamente al principio sulla scelta e non al principio sulla limitazione della finalità rende più probabile una siffatta interpretazione.

Come già precisato nella lettera del 10 aprile 2014 indirizzata alla vicepresidente Reding, il Gruppo di lavoro avrebbe preferito riscontrare un approccio più restrittivo alle eccezioni giornalistiche che fosse maggiormente in linea con il principio applicato nell'Unione, nonché con il diritto alla deindicizzazione ("delisting") riconosciuto nella sentenza Google Spain[26].

2.2.5 Diritti di accesso, rettifica e cancellazione dell'interessato

In base allo scudo, la persona ha diritto di *sapere* dall'organizzazione se questa tratti dati che la riguardano così come ha il diritto che tali dati *le siano comunicati* (allegato II, punto III.8.a.i). Tuttavia l'obbligo per le organizzazioni di rispondere alla persona che chiede spiegazioni sulle finalità del trattamento, sulle categorie di dati personali interessati e sui destinatari o sulle categorie di destinatari cui i dati personali sono comunicati non è ribadito con sufficiente forza. Il Gruppo di lavoro ritiene che gli elementi da fornire all'interessato debbano essere menzionati nel corpo del testo, anziché soltanto in una nota a piè di pagina, e debbano essere enunciati sotto forma di un obbligo chiaro (collegato all'allegato II, punto III.8.a.i.1).

In base al principio supplementare 8, "[l']accesso deve essere concesso solo se ed in quanto l'organizzazione conserva informazioni personali" (allegato II, punto III.8.d.ii). Tale regola dovrebbe essere interpretata in maniera non restrittiva, nel senso che, in linea di massima, deve essere possibile accedere ai dati che l'organizzazione sottopone a qualsiasi tipo di trattamento, e non soltanto ai dati conservati. Pertanto ai fini dell'efficacia del diritto di accesso è importante precisare che in questo caso per "conservazione" si intende "trattamento" secondo la definizione di cui all'allegato II, punto I.8.b. L'applicazione di tale norma dovrebbe essere oggetto di un'attenta disamina nel corso del riesame comune dello scudo.

Permangono preoccupazioni per quanto riguarda l'elenco di eccezioni di cui all'allegato II, punto III.8.e.i., che è simile a quello fornito nella risposta alla FAQ 8 della decisione "Approdo sicuro" e che tende a privilegiare gli interessi delle organizzazioni. In tal senso la persona non avrà la possibilità di accedere ai dati personali che la riguardano per i seguenti motivi: "violazione del segreto professionale […] o di altro obbligo professionale" (allegato II, punto III.8.e.3), "pregiudizio all'indagine di sicurezza o alla vertenza aziendale nei confronti di un dipendente ovvero in relazione alla programmazione dell'avvicendamento del personale e alla riorganizzazione societaria" (allegato II, punto III.8.e.4) e "pregiudizio alla riservatezza necessaria per l'espletamento delle funzioni di controllo, ispezione o regolamentazione previste dalla sana gestione ovvero a trattative in corso o future che coinvolgono l'organizzazione" (allegato II, punto III.8.e.5). Tali motivi dovrebbero essere letti in combinazione con l'esenzione generale riguardante le informazioni commerciali riservate di cui all'allegato II, punto III.8.c. Pertanto la persona non avrà mai accesso ai dati che la riguardano nelle situazioni sopra elencate, giacché non si è trovato un equilibrio tra i diritti e gli interessi della persona e quelli dell'organizzazione per quanto concerne il trattamento delle domande di accesso.

[26] Sentenza del 13 maggio 2014 nella causa C-131/12 — Google Spain contro Agencia Española de Protección de Datos e Mario Costeja González.

Il Gruppo di lavoro rammenta che il diritto della persona di accedere ai dati che la riguardano è sancito all'articolo 8, paragrafo 2, della Carta. Pur non essendo un diritto assoluto, esso è fondamentale per il diritto alla protezione dei dati personali, in quanto facilita l'esercizio degli altri diritti dell'interessato, quali il diritto di rettifica e il diritto alla cancellazione.

Per quanto riguarda il diritto di rettifica e il diritto alla cancellazione, il Gruppo di lavoro si rallegra che i principi dello scudo abbiano introdotto un notevole miglioramento rispetto ai principi dell'approdo sicuro, stabilendo che tali diritti sono conferiti non soltanto nelle situazioni in cui i dati risultano inesatti ma anche quando i dati sono trattati in violazione dei principi (allegato II, punto II.6).

2.2.6 Ricorso, controllo e responsabilità (meccanismi di ricorso)

a) Esercizio effettivo dei diritti di ricorso della persona

Il Gruppo di lavoro riconosce gli impegni assunti dalle autorità statunitensi riguardo ai vari livelli del meccanismo di ricorso. Tuttavia tenuto conto della complessità e della scarsa chiarezza dell'architettura complessiva del meccanismo, il Gruppo di lavoro teme che, nella pratica, l'esercizio effettivo di tale diritto da parte dell'interessato possa essere compromesso. Il Gruppo di lavoro evidenzia che la qualità del meccanismo di ricorso dovrebbe prevalere sulla quantità dei meccanismi a disposizione dei cittadini dell'UE. Esso nutre inoltre preoccupazioni riguardo al fatto che la maggioranza, se non la totalità, dei meccanismi di ricorso preveda una procedura negli Stati Uniti, complicando dunque il controllo della procedura da parte delle autorità di protezione dei dati dell'Unione.

In effetti il meccanismo di ricorso previsto dallo scudo si concentra in primo luogo sulla possibilità offerta all'interessato di far valere i propri diritti e di "sottoporre il caso di inosservanza dei principi direttamente all'*impresa statunitense che si è autocertificata come aderente allo scudo*"[27]. Inoltre l'organizzazione deve designare un organo indipendente di risoluzione delle controversie per esaminare e risolvere i casi di reclamo individuale. Il Gruppo di lavoro constata con soddisfazione che tale mezzo di ricorso sarà messo a disposizione della persona gratuitamente.

In alternativa è possibile sporgere reclamo direttamente alla Commissione federale del Commercio (FTC), anche se quest'ultima non ha l'obbligo di trattare il reclamo. Anche l'autorità di protezione dei dati può sottoporre un caso di reclamo; il Dipartimento del Commercio si è impegnato ad esaminare i reclami e ad adoperarsi al massimo per favorire la soluzione dei casi (allegato I) che saranno esaminati "in via prioritaria" dalla FTC (allegato II, punto III.7.e). Tuttavia l'esame in via prioritaria dei casi di reclamo da parte della FTC non garantisce all'interessato che essi saranno effettivamente trattati.

Come extrema ratio l'interessato può chiedere l'arbitrato vincolante. Il collegio arbitrale si riunisce negli Stati Uniti ed è soggetto al controllo dei giudici statunitensi.

[27] Commissione europea, progetto di decisione sull'adeguatezza, considerando 30.

Lo scudo offre inoltre alle organizzazioni la possibilità di scegliere di collaborare con le autorità di protezione dei dati dell'UE (allegato II, punto III.5.a). La collaborazione è addirittura obbligatoria nel caso di dati sulle risorse umane raccolti nel contesto di un rapporto di lavoro (allegato II, punto III.9.d.ii). In tale scenario la risoluzione alternativa delle controversie non sarà un'opzione percorribile (allegato II, punto III.5.a). Lo scudo non precisa con quali modalità sarà organizzata, nella pratica, la collaborazione con le autorità di protezione dei dati dell'UE. In particolare non è chiaro se il collegio arbitrale si occuperà di tutti i casi o se ogni singolo caso sarà trattato da un collegio diverso.

Il Gruppo di lavoro ritiene che la decisione di adeguatezza debba fornire indicazioni più precise circa la competenza delle autorità di trattamento dei dati a trattare i casi di reclamo. A tale riguardo l'intervento delle autorità di trattamento dei dati risulta dipendere dal ruolo nel quale l'organizzazione agisce ma tale relazione merita un approfondimento.

Se l'organizzazione agisce in qualità di procuratore per conto di un titolare del trattamento dell'UE, la persona avrà in ogni caso la possibilità di sporgere reclamo presso l'autorità di trattamento dei dati competente dell'UE. La situazione sarà analoga sia per il trattamento dei dati sulle risorse umane sia per il trattamento di altri dati commerciali.

Se l'organizzazione aderente allo scudo agisce in qualità di titolare del trattamento, l'autorità di protezione dei dati sarà competente a trattare il reclamo soltanto in relazione ai trattamenti che rientrano nel campo di applicazione del diritto dell'Unione (trattamento effettuato sotto la responsabilità del titolare del trattamento dell'UE, anche in caso di controllo congiunto con l'organizzazione statunitense, oppure trattamento in relazione al quale l'organizzazione aderente allo scudo sarebbe direttamente assoggettata alla normativa dell'UE, ad esempio perché utilizza strumenti situati nell'Unione). Tuttavia per i trattamenti di dati effettuati soltanto in base alla normativa statunitense, si applicheranno unicamente i meccanismi dello scudo. Al fine di superare le barriere linguistiche e la scarsa conoscenza del sistema giuridico statunitense, sarebbe utile che le autorità di protezione dei dati dell'UE avessero facoltà di agire in qualità di intermediari per il trattamento del reclamo o di assistere l'interessato nei procedimenti per la risoluzione alternativa delle controversie con organizzazioni statunitensi o nei contatti tra l'interessato e le autorità statunitensi, ove l'autorità di trattamento dei dati lo ritenga opportuno.

Il Gruppo di lavoro sottolinea che il meccanismo descritto nello scudo non segue la precedente raccomandazione secondo la quale è necessario che le persone dell'UE possano chiedere un risarcimento nell'Unione europea e che sia loro concesso il diritto di sporgere reclamo dinanzi a un giudice nazionale competente dell'UE[28]. Il Gruppo di lavoro auspica che le politiche della privacy delle organizzazioni aderenti allo scudo prevedano tale possibilità.

Al fine di garantire l'efficacia, il Gruppo di lavoro raccomanda, quale soluzione preferibile, che nell'ambito del regime le autorità di protezione dei dati dell'UE possano rappresentare l'interessato e agire per suo conto oppure possano fungere da intermediari. In alternativa il

[28] Cfr. la lettera del Gruppo di lavoro, del 10 aprile 2014, indirizzata alla vicepresidente Reding.

regime dovrebbe contenere specifiche clausole attributive di competenza che consentano all'interessato di esercitare i suoi diritti in Europa.

b) Arbitrato

Le procedure di arbitrato non sono ancora del tutto definite, il che complica la valutazione dal parte del Gruppo di lavoro. Poiché sembra che l'arbitrato sarà regolato dalle leggi statunitensi e che il procedimento si svolgerà unicamente in lingua inglese, è probabile che le autorità di protezione dei dati dell'UE manifestino l'intenzione di prestare assistenza agli interessati.

Inoltre la procedura arbitrale è stata instituita in quanto non vi era alcuna garanzia che il reclamo sarebbe stato trattato, in quanto la FTC non ha l'obbligo di trattare ogni singolo caso. Il Gruppo di lavoro rileva che qualora la persona dell'UE senta la necessità di avvalersi dell'assistenza di un legale, dovrà sopportarne le spese; ciò potrebbe disincentivare il ricorso all'arbitrato per la risoluzione dei casi di reclamo.

c) Controllo, esecuzione ed efficacia dei meccanismi di ricorso

Condizioni per l'adesione allo scudo

Secondo la Corte di giustizia "l'affidabilità di un [sistema di autocertificazione] […] poggia essenzialmente sulla predisposizione di meccanismi efficaci di accertamento e di controllo che consentano di individuare e sanzionare […] eventuali violazioni delle norme che assicurano la protezione dei diritti fondamentali […]"[29].

Il Gruppo di lavoro rileva che, nell'ambito dello scudo, il ruolo del Dipartimento del Commercio nel processo di certificazione risulta ridotto a un mero controllo della completezza dei documenti. Sebbene il Gruppo di lavoro riconosca che l'autocertificazione non comporta un controllo sistematico a priori dell'attuazione delle politiche in materia di privacy, il Dipartimento del Commercio dovrebbe almeno impegnarsi a verificare in modo sistematico che le politiche della privacy integrino tutti i principi dello scudo. Tale impegno è menzionato nel progetto di decisione sull'adeguatezza ma non è chiaramente ravvisabile nella dichiarazione del Dipartimento del Commercio[30].

Una violazione dei principi dello scudo potrebbe passare inosservata per molto tempo ed essere rilevata soltanto dopo avere arrecato un pregiudizio grave e probabilmente irreparabile ai diritti fondamentali dell'interessato. Pertanto tale approccio potrebbe essere in contrasto con il principio di precauzione europeo.

Trasparenza mediante l'elenco degli aderenti allo scudo e il registro delle organizzazioni depennate dall'elenco

Sono stati introdotti notevoli miglioramenti per quanto riguarda la trasparenza nei confronti dell'interessato. Oltre alle organizzazioni statunitensi che si sono autocertificate presso il

[29] Corte di giustizia dell'Unione europea, sentenza Schrems, punto 81.
[30] Commissione europea, progetto di decisione sull'adeguatezza, considerando 34.

Dipartimento del Commercio, il nuovo elenco degli aderenti allo scudo conterrà anche un registro di tutte le organizzazioni depennate dall'elenco degli aderenti allo scudo, nel quale sarà indicato anche il motivo che ne ha determinato l'esclusione[31]. Il sito web del Dipartimento del Commercio dedicato allo scudo sarà maggiormente concentrato sui gruppi di destinatari in modo tale da facilitare la verifica del tipo di informazioni contemplate dall'autocertificazione e della politica della privacy che si applica alle informazioni in questione, nonché del metodo con cui l'organizzazione accerta il rispetto dei principi[32]. Il Gruppo di lavoro constata con soddisfazione che è ormai esplicito che il Dipartimento del Commercio provvederà a verificare se le imprese, ove dispongano di un sito web pubblico, vi abbiano pubblicato la politica della privacy seguita o se, qualora non dispongano di un sito web pubblico, abbiano indicato il luogo in cui il pubblico può consultare la loro politica della privacy[33]. Inoltre i documenti forniscono maggiori indicazioni sul contenuto della politica della privacy[34].

Il Gruppo di lavoro ritiene che potrebbe sorgere un problema laddove un'organizzazione già inclusa nell'elenco degli aderenti allo scudo estenda successivamente la propria certificazione ad altre categorie di dati. In tali casi l'elenco non rifletterà i diversi periodi di applicabilità dei principi alle diverse categorie di dati. Ciò crea il rischio che le persone e le imprese dell'UE non possano valutare appieno se e da quale momento uno specifico insieme di dati ricada effettivamente nel campo di applicazione dei principi dello scudo. Per ovviare a tale lacuna, il Gruppo di lavoro raccomanda di predisporre, all'interno dell'elenco degli aderenti allo scudo, un registro delle organizzazioni che precisi l'entrata in vigore dell'autocertificazione per ogni categoria di dati personali.

Il Gruppo di lavoro si rallegra del fatto che il Dipartimento del Commercio manterrà un registro delle organizzazioni depennate dall'elenco degli aderenti allo scudo e che tale registro riporterà una dichiarazione in cui è precisato che tali organizzazioni non possono più contare sui benefici derivanti dallo scudo ma devono comunque continuare ad applicare i principi ai dati personali ricevuti quando vi aderivano come organizzazioni certificate, fintantoché li conserveranno (allegato I, pag. 3). Tuttavia poiché alcune organizzazioni che sono state depennate dall'elenco degli aderenti allo scudo possono scegliere se restituire o cancellare i dati ricevuti nell'ambito del regime, mentre altre organizzazioni conserveranno i dati che hanno ricevuto in tale ambito, è importante garantire alle persone una maggiore trasparenza su tale questione. Pertanto il registro delle società tenuto dal Dipartimento del Commercio dovrebbe precisare se l'organizzazione continua a conservare dati personali ricevuti nell'ambito dello scudo o se invece ha restituito o cancellato tali dati.

[31] Allegato I, pag. 5 e allegato II, punto II.1; il Gruppo di lavoro rinvia inoltre alla quarta raccomandazione della Commissione nella sua comunicazione COM(2103)847 e alla lettera del Gruppo di lavoro, del 10 aprile 2014, indirizzata alla vicepresidente Reding, con particolare riferimento al quinto punto della raccomandazione relativa alla trasparenza.
[32] Allegato I, pag. 8; il Gruppo di lavoro rinvia inoltre alla sua lettera del 10 aprile 2014 indirizzata alla vicepresidente Reding, con particolare riferimento al secondo punto della raccomandazione relativa alla trasparenza.
[33] Allegato I, pagg. 3 e 4; il Gruppo di lavoro rinvia inoltre alla prima raccomandazione della Commissione nella comunicazione COM(2103)847 nonché alla lettera del Gruppo di lavoro, del 10 aprile 2014, indirizzata alla vicepresidente Reding, con particolare riferimento al terzo punto della raccomandazione relativa alla trasparenza.
[34] Allegato I, pagg. 5 e 6 e allegato II, punto III.6.

Qualora l'organizzazione conservi ancora tali dati, il registro dovrebbe prevedere esplicitamente l'obbligo per l'organizzazione di continuare ad applicare ad essi i principi.

Inoltre il registro tenuto dal Dipartimento del Commercio dovrebbe menzionare che queste organizzazioni non possono più contare sui benefici derivanti dallo scudo per i nuovi trasferimenti, ossia che non sono più autorizzate a ricevere dati personali dall'UE nel quadro dei principi.

Procedure di verifica

Al fine di appurare l'efficacia pratica dell'autocertificazione, le organizzazioni possono effettuare un'autovalutazione o predisporre una verifica esterna della compatibilità. Il Gruppo di lavoro deplora che la formazione dei dipendenti sia obbligatoria soltanto quando l'organizzazione sceglie di procedere alla verifica mediante autovalutazione (allegato II, punto III.7.c). Sembra inoltre che l'obbligo di accertare che le politiche siano accurate, complete, poste in evidenza, attuate e accessibili sussista soltanto se l'organizzazione sceglie la verifica interna (autovalutazione) e che la verifica mediante un meccanismo esterno sia limitata soltanto all'accertamento della conformità con la politica della privacy seguita dall'organizzazione.

A posteriori

Il Gruppo di lavoro accoglie positivamente il fatto che la FTC e il Dipartimento del Commercio siano dotati di poteri di indagine in caso di reclamo. Il Gruppo di lavoro constata inoltre che il Dipartimento del Commercio potrà eseguire verifiche d'ufficio, in particolare tramite l'invio di questionari. Esso, tuttavia, vorrebbe avere la certezza che tale approccio sia sufficiente a soddisfare il requisito, fissato dalla Corte di giustizia, relativo alla predisposizione di meccanismi efficaci di accertamento e di controllo. In realtà permangono perplessità circa i poteri di cui le autorità di esecuzione statunitense sono realmente investiti per l'esecuzione di ispezioni presso i locali delle organizzazioni autocertificate ai fini dell'accertamento di violazioni dello scudo, la modalità di ottenimento dell'*exequatur* della decisione di un'autorità dell'UE nel territorio degli Stati Uniti e la possibilità che le sanzioni previste dallo scudo abbiano un effetto dissuasivo nella pratica.

2.2.7 Trattamento dei dati sulle risorse umane

Ambito di applicazione

Il principio supplementare 9 (allegato II, punto III.9) si applica alle informazioni personali sui dipendenti (presenti o passati), raccolte nell'ambito del rapporto di lavoro. In base alla formulazione del principio supplementare 9, lettera a., punto ii, i principi dello scudo trovano applicazione solo per "il trasferimento di dati identificati […] o per l'accesso agli stessi". L'espressione "dati identificati" non è in linea con la definizione di "dati personali" di cui all'allegato II, punto I.8.a., che si riferisce ai dati "riguardanti singoli individui (identificati o identificabili)" e pertanto non rispecchia la definizione utilizzata nella direttiva[35].

Il principio supplementare 9, lettera a., punto ii, stabilisce quanto segue: "Non si pongono questioni di privacy per le relazioni statistiche basate su dati aggregati sull'occupazione e prive di dati personali né per l'uso di dati resi anonimi". Tale enunciato è in contrasto con una serie di pareri emessi dal Gruppo di lavoro. Il Gruppo desidera evidenziare che i dati

[35] Come già sottolineato, anche la limitazione del campo di applicazione dei principi al solo trasferimento dei dati e all'accesso agli stessi non è in linea con la definizione del termine "trattamento" (allegato II, punto I.8.b).

aggregati possono comunque essere reidentificati e dovrebbero pertanto essere considerati dati personali[36].

[36] Cfr. il parere 4/2007 sul concetto di dati personali e il parere 05/2014 sulle tecniche di anonimizzazione.

Informativa, scelta e limitazione della finalità

Il Principio supplementare 9, lettera b., punto i., offre un esempio di applicazione dei principi sull'informativa e sulla scelta quando i dati sulle risorse umane sono utilizzati per finalità differenti. L'esempio si riferisce al caso di un'organizzazione statunitense che intenda "usare a fini non occupazionali (comunicazioni commerciali, ecc.) informazioni personali raccolte nell'ambito di un rapporto di lavoro". In questo scenario il cambiamento di finalità è autorizzato a condizione che siano rispettati i principi sull'informativa e sulla scelta. Secondo il Gruppo di lavoro, l'ulteriore trattamento dei dati sulle risorse umane a fini di marketing diretto dovrà essere considerato, nella maggioranza dei casi, una finalità incompatibile e dunque in contrasto con il principio sulla limitazione della finalità (allegato II, II.5.a). Il Gruppo di lavoro ritiene inoltre che il principio sulla scelta non possa costituire una base adeguata perché il dipendente "acconsenta" (facoltà di rifiuto) a un cambiamento di finalità nel contesto del rapporto di lavoro, in cui tale consenso potrebbe non essere realmente frutto di una libera scelta.

Il Gruppo di lavoro dubita seriamente che la preminenza attribuita dallo scudo al principio sulla scelta quale condizione per l'ulteriore uso dei dati per finalità diverse soddisfi gli orientamenti dell'OCSE sulla protezione della sfera privata, in quanto non vi sono garanzie sufficienti ad impedire che il meccanismo della "scelta" (facoltà di rifiuto) possa essere usato anche per l'ulteriore trattamento dei dati per finalità incompatibili. Il principio supplementare 9, lettera b., punto iv., prevede esplicitamente una vasta deroga ai principi sull'informativa e sulla scelta "in quanto e fino a che ciò risulti necessario per non ledere la capacità dell'organizzazione di procedere a promozioni e nomine o prendere decisioni analoghe relative al personale". In primo luogo l'uso di dati sulle risorse umane per tali finalità dovrebbe sempre essere esplicitato al momento della raccolta. Inoltre l'espressione "decisioni analoghe relative al personale" è troppo vaga e generica; di conseguenza i dati sulle risorse umane saranno totalmente esentati dall'applicazione dei principi sull'informativa e sulla scelta quando sono trattati nel contesto del rapporto di lavoro. L'espressione è talmente generica da non consentire di valutare se l'ulteriore uso sia compatibile con la finalità originaria. Il Gruppo di lavoro raccomanda la cancellazione di tale deroga.

Diritto di accesso

Il principio supplementare 9, lettera e., punto i. prevede anche una deroga all'applicazione del principio sull'accesso o alla conclusione di un contratto con un terzo titolare del trattamento per i dati sulle risorse umane; tale deroga autorizza il trasferimento dei dati personali che riguardano un numero esiguo di dipendenti per esigenze operative occasionali di natura occupazionale, quali la prenotazione di un volo o di una stanza d'albergo o la copertura assicurativa, a condizione che siano rispettati i principi sull'informativa e sulla scelta. Il Gruppo di lavoro non ravvisa alcun ragionevole motivo che giustifichi tale deroga e raccomanda la cancellazione del paragrafo in questione.

2.2.8 Medicinali e prodotti farmaceutici

Ambito di applicazione

In base allo scudo il trasferimento dall'Unione europea agli Stati Uniti di dati codificati nel contesto di medicinali e prodotti farmaceutici non costituisce un trasferimento per cui valgono i principi dello scudo (allegato II, punto III.14.g.i). Tuttavia il trasferimento di dati codificati è tutelato dalla normativa europea in materia di protezione dei dati. Ciò significa che, nella pratica, questi trasferimenti non possono essere contemplati dallo scudo. Il Gruppo di lavoro invita la Commissione europea a stabilire in maniera esplicita che il progetto di decisione sull'adeguatezza non riguarderà il trasferimento di dati codificati per motivi medici o farmaceutici, che pertanto deve essere contemplato da altre misure di salvaguardia, quali le clausole contrattuali tipo o le norme vincolanti d'impresa. Il Gruppo di lavoro propone di chiarire tale aspetto nella decisione finale sull'adeguatezza.

Trasferimento per motivi di regolamentazione e di vigilanza (allegato II, punto III.14.d)

Il Gruppo di lavoro teme che in virtù di tali disposizioni i dati personali che, per via del contesto medico, sono prevalentemente di natura sensibile possano essere trasmessi ad enti regolatori statunitensi. Poiché lo scudo è stato elaborato per il trasferimento di dati tra enti privati, è evidente che un ente pubblico quale un'autorità di regolamentazione statunitense non è ammissibile all'autocertificazione nell'ambito dello scudo, il che solleva la questione di garantire una protezione adeguata dei dati che sono oggetto di questo tipo di trasferimento. Qualora questi trasferimenti siano necessari a fini di regolamentazione, occorrerà adottare misure volte a garantire la tutela ininterrotta dei diritti fondamentali dell'interessato dell'UE. Il Gruppo di lavoro sottolinea che il progetto di decisione sull'adeguatezza non contiene alcuna constatazione a tale riguardo. Pertanto il Gruppo non ha alcuna garanzia del fatto che i dati sensibili dell'interessato dell'UE beneficeranno di una protezione adeguata in tale contesto.

Il Gruppo di lavoro inoltre non comprende per quale motivo la "commercializzazione" sia citata come esempio di finalità della ricerca scientifica futura. Inoltre non è chiaro il motivo per il quale l'ulteriore trasferimento verso centri della medesima impresa o altri ricercatori (allegato II, punto III.14.d) sia stato inserito nel paragrafo "Trasferimento per motivi di regolamentazione e di vigilanza". Tali questioni dovranno essere chiarite nella decisione finale sull'adeguatezza.

Controllo della sicurezza e efficacia dei prodotti (compresa la segnalazione ad enti pubblici) e tracciabilità dei pazienti che usano determinati medicinali o dispositivi medici

Lo scudo prevede una deroga all'applicazione dei principi relativamente agli aspetti di informativa, scelta, ulteriore trasferimento e accesso nella misura in cui l'osservanza dei principi interferisca nell'osservanza degli obblighi normativi. Il progetto di decisione sull'adeguatezza non contiene alcuna constatazione riguardo ai casi in cui i principi interferiscono nell'osservanza degli obblighi normativi. Per quanto sia comprensibile che le

indagini da parte di enti pubblici possano giustificare limiti all'informativa e al diritto di accesso ai fini della tutela delle attività di indagine, il Gruppo non ravvisa alcun motivo che possa giustificare deroghe così ampie quando il trattamento è effettuato dall'organizzazione o da terzi nel settore privato. Ad esempio poiché i trattamenti dei pazienti sono sempre più personalizzati, una deroga così ampia ai principi nel caso della tracciabilità dei pazienti che usano determinati medicinali o dispositivi medici è inaccettabile, in quanto questo tipo di cure diventerà una pratica generalizzata. Lo stesso vale per i dati che sono usati da aziende farmaceutiche per il controllo della sicurezza e dell'efficacia dei prodotti (sperimentazione o vendita di nuovi medicinali).

2.2.9 Informazioni di pubblico dominio

La deroga al diritto di accesso nel caso delle informazioni di pubblico dominio e dei documenti pubblici (allegato II, punto III.15., lettere d. e e.) solleva preoccupazioni nella misura in cui la persona, nell'esercitare il proprio diritto di accesso, è interessata a sapere se i dati che la riguardano sono trattati da un determinato titolare e quali sono i dati trattati, in modo da poterne verificare il trattamento. Il Gruppo di lavoro ha più volte ribadito che, in base al diritto dell'Unione, indipendentemente dalla pubblicazione o meno dei dati a carattere personale, l'interessato ha sempre il diritto di accedere ai dati che lo riguardano e il diritto di esigere, se necessario, la correzione o cancellazione di dati trattati in maniera illecita ovvero di carattere incompleto o inesatto[37]. Se la domanda di accesso dell'interessato fosse respinta a motivo dell'ottenimento dei dati da fonti di pubblico dominio o da documenti pubblici, l'interessato non sarebbe più in grado di verificare l'accuratezza dei dati e di accertare in primo luogo che i dati siano stati resi pubblici in maniera lecita.

Lo scudo, tuttavia, prevede una deroga all'applicazione dei principi sull'informativa, sulla scelta, sull'accesso e sulla responsabilità in caso di ulteriore trasferimento per quanto riguarda i documenti pubblici e le informazioni di pubblico dominio (allegato II, punto II.15.b). Tali esenzioni sembrano troppo vaste rispetto alla direttiva e sollevano preoccupazioni, in quanto compromettono, tra l'altro, la possibilità della persona di verificare l'accuratezza dei dati che la riguardano e di limitarne la diffusione.

2.3 Conclusioni

Il Gruppo di lavoro riconosce che le autorità statunitensi e la Commissione europea hanno apportato notevoli miglioramenti agli aspetti commerciali del trasferimento di dati tra i due continenti. Alla luce della suddetta analisi, il Gruppo di lavoro constata tuttavia che la componente commerciale dello scudo esige ulteriori chiarimenti su molti punti. Ad esempio suscita preoccupazione l'assenza di un principio esplicito sulla conservazione dei dati. Il Gruppo di lavoro, pertanto, nutre seri dubbi sulla capacità dello scudo di assicurare un livello di protezione che sia sostanzialmente equivalente a quello garantito nell'Unione.

La decisione sull'adeguatezza deve chiarire ulteriormente i principi sulla scelta e sulla limitazione della finalità. Permane il rischio di lacune per quanto riguarda vari principi,

[37] Cfr. WP20, pag. 5.

segnatamente il principio sull'ulteriore trasferimento, il meccanismo di gestione dei reclami e il trattamento dei dati sulle risorse umane o delle informazioni farmaceutiche. Inoltre la modalità di applicazione dei principi dello scudo ai responsabili del trattamento (procuratori) deve essere ulteriormente definita ed è necessario porre particolare attenzione per garantire un'applicazione chiara e inequivocabile della terminologia.

3. VALUTAZIONE DELLE GARANZIE IN MATERIA DI SICUREZZA NAZIONALE PREVISTE DAL PROGETTO DI DECISIONE SULL'ADEGUATEZZA

3.1 Garanzie e limitazioni applicabili alle autorità di sicurezza nazionale degli Stati Uniti

Le ingerenze nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati possono essere ammesse a condizione che esse trovino giustificazione in una società democratica. Ciò significa che i principi non sono assoluti e che sono possibili deroghe ma soltanto a condizione che siano rispettate le garanzie (essenziali) applicabili. Coerentemente con l'obiettivo di una maggiore tutela della sfera privata, le organizzazioni devono inoltre fare il possibile per attuare i principi integralmente e in modo trasparente, anche specificando, nelle rispettive politiche in materia di tutela della sfera privata, in quali casi saranno regolarmente applicate le eccezioni ai principi ammesse dalla normativa statunitense. Per lo stesso motivo, quando i principi e/o la legislazione statunitense consentono tale scelta, le organizzazioni sono tenute a scegliere, per quanto possibile, la protezione più elevata.

L'allegato II, punto I.5, stabilisce che l'"adesione ai principi può essere limitata: a) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia; b) da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione, oppure c) se la direttiva o la legislazione degli Stati membri rendono possibili eccezioni o deroghe, a condizione che tali eccezioni o deroghe si applichino in contesti comparabili".

Si tratta di stabilire se le deroghe di cui all'allegato II possano trovare giustificazione in una società democratica. Nel progetto di decisione sull'adeguatezza dello scudo, la Commissione è giunta alla conclusione che "negli Stati Uniti vigono regole intese a limitare a quanto strettamente necessario per conseguire l'obiettivo legittimo ricercato qualsiasi ingerenza per motivi di sicurezza nazionale nei diritti fondamentali della persona i cui dati personali sono trasferiti dall'Unione europea verso gli Stati Uniti nell'ambito dello scudo"[38].

Utilizzando il quadro di cui al punto 1.2 del presente parere e alla luce delle dichiarazioni delle autorità statunitensi e delle constatazioni della Commissione, il Gruppo di lavoro ha valutato il quadro normativo vigente negli Stati Uniti e le prassi dei servizi di intelligence

[38] Progetto di decisione di esecuzione della Commissione a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy, considerando 75.

statunitensi, nonché le condizioni alle quali sono ammesse ingerenze nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati, che sono garantiti dalla normativa europea. Tale valutazione è basata sull'analisi della direttiva presidenziale 28 (PPD-28), del decreto presidenziale 12333 (EO 12333) e delle diverse basi giuridiche stabilite nella legge relativa alla vigilanza sull'intelligence esterna (FISA — articoli 104, 402, 215, 501 e 702). Il Gruppo di lavoro si è basato sull'allegato VI dello scudo, costituito da una lettera dell'Ufficio del direttore dell'intelligence nazionale (ODNI) sulle garanzie e limitazioni applicabili alle autorità di sicurezza nazionale degli USA, che sintetizza le informazioni fornite alla Commissione europea sulle attività di raccolta dati tramite l'intelligence dei segnali condotte dagli Stati Uniti.

3.2 Garanzia A — Il trattamento dovrebbe essere conforme alla legge e basato su norme chiare, precise e accessibili

A norma del diritto europeo, qualsiasi ingerenza deve essere conforme alle leggi, alle politiche e alle procedure consolidate ed essere sufficientemente chiara ed accessibile (entro il margine di discrezionalità concesso ai singoli paesi) per offrire ai cittadini un'indicazione chiara delle circostanze nelle quali, e delle condizioni alle quali, le autorità pubbliche hanno il potere di ricorrere a misure di sorveglianza[39].

Il Gruppo di lavoro rileva che le attività di raccolta dati tramite l'intelligence dei segnali sono condotte sulla base di un quadro giuridico accessibile. Tutte le leggi citate nell'allegato VI (PPD-28, FISA, legge USA FREEDOM, legge sulla libertà di informazione) sono consultabili online dai cittadini (all'interno e all'esterno degli USA). L'allegato VI offre una sintesi della disciplina giuridica vigente, delle limitazioni applicabili alla raccolta, delle limitazioni applicabili alla conservazione e alla divulgazione, della garanzia della conformità e vigilanza, della trasparenza e dei mezzi di ricorso. Il sistema giuridico statunitense in materia di attività di intelligence è composto da una serie di documenti diversi, ovvero relazioni, politiche e procedure dei singoli enti, di cui è necessaria un'analisi che consenta di comprendere meglio le modalità di svolgimento delle attività, sia sul piano teorico sia su quello pratico. A tale riguardo il Gruppo di lavoro si è concentrato su alcuni punti che ritiene fondamentali.

3.2.1 Decreto presidenziale 12333 e direttiva presidenziale 28

Il decreto presidenziale 12333 ha un vasto campo di applicazione; in linea di massima, la raccolta di dati di intelligence esterna può essere effettuata a discrezione del presidente USA sulla base del decreto. Tuttavia è stato osservato che, dall'introduzione della FISA, l'EO 12333 può essere utilizzato soltanto per la raccolta di dati al di fuori del territorio

[39] Nella sentenza Zakharov, punto 247, la Corte europea dei diritti dell'uomo precisa di avere precedentemente rilevato che il requisito della "prevedibilità" della legge non può giungere fino a costringere gli Stati a emanare disposizioni giuridiche che definiscano in dettaglio tutti i comportamenti che possono indurre a sottoporre una persona a sorveglianza secreta per motivi di "sicurezza nazionale". Le minacce alla sicurezza nazionale possono essere, per forza di cose, di varia natura ed essere impreviste o difficili da definire in anticipo (cfr. la sentenza Kennedy citata sopra, punto 159). Al contempo la Corte ha evidenziato che nelle questioni che incidono sui diritti fondamentali sarebbe contrario allo stato di diritto, uno dei principi basilari di una società democratica sanciti nella Convenzione, che il potere discrezionale conferito al potere esecutivo nella sfera della sicurezza nazionale fosse illimitato. Pertanto la legge deve definire con sufficiente chiarezza l'estensione e la modalità di esercizio di un siffatto potere discrezionale conferito alle autorità competenti, in considerazione del legittimo obiettivo della misura in questione, per offrire alla persona una protezione adeguata contro l'arbitrio.

statunitense. Il Gruppo di lavoro rileva che l'EO 12333 non fornisce molte indicazioni per quanto riguarda il suo ambito geografico di applicazione e la misura in cui è possibile effettuare la raccolta, la conservazione o l'ulteriore divulgazione dei dati, né precisa la natura dei reati che possono determinare un'attività di sorveglianza o la tipologia di informazioni che possono essere raccolte o utilizzate.

Il Gruppo di lavoro è dell'avviso che lo scopo principale della direttiva presidenziale 28 (PPD-28) sia quello di prescrivere le limitazioni applicabili alla raccolta e al trattamento dei dati personali, indipendentemente dal programma di sorveglianza utilizzato e dal luogo di ottenimento dei dati.

La PPD-28 è una direttiva del Presidente degli Stati Uniti che fissa alcuni principi di coerenza in base ai quali deve essere autorizzata e effettuata la raccolta di dati di intelligence dei segnali; tuttavia la PPD-28 non costituisce una base giuridica per la raccolta. La PPD-28 esplica la sua efficacia imponendo tali principi alla comunità di intelligence affinché essa li applichi nelle proprie politiche e procedure. La direttiva si applica alle attività di intelligence dei segnali indipendentemente dal luogo in cui si trovano i dati al momento della loro raccolta, ovvero all'interno o all'esterno degli Stati Uniti. Essa pertanto si applica anche ai dati raccolti a fini di intelligence dei segnali quando tali dati sono trasferiti dall'Unione agli Stati Uniti.

In particolare la PPD-28 prevede che le attività di intelligence dei segnali siano il più possibile mirate[40]. Per quanto riguarda l'uso dei dati, la direttiva stabilisce procedure per la minimizzazione della raccolta (comprese condizioni per la conservazione e la divulgazione dei dati), la sicurezza dei dati e l'accesso da parte del personale pertinente (ovvero regole contenenti garanzie atte a limitare i rischi di abuso e di uso improprio), la qualità dei dati e i controlli. Tali garanzie si applicano a prescindere dalla nazionalità dell'interessato, ovvero tanto ai cittadini statunitensi o residenti negli USA quanto ai cittadini stranieri.

Le garanzie previste dalla PPD-28 si applicano anche durante la trasmissione dei dati verso gli Stati Uniti. Nell'allegato VI l'ODNI sottoscrive un impegno secondo cui, se la comunità dell'intelligence statunitense dovesse raccogliere dati dai cavi transatlantici durante la loro trasmissione verso gli USA, "varrebbero comunque le limitazioni e le tutele previste dalle norme applicabili, comprese le condizioni imposte dalla PPD-28"[41]. Il Gruppo di lavoro rileva la persistente mancanza di una giurisprudenza consolidata che stabilisca la liceità delle intercettazioni via cavo qualora le stesse siano effettuate da qualsiasi paese. Ad ogni modo gli Stati Uniti non confermano né negano di utilizzare le intercettazioni via cavo come mezzo di raccolta dei dati di intelligence.

[40] A norma dell'articolo 1, lettera d), le attività di intelligence dei segnali sono il più possibile mirate. Per stabilire se debbano essere raccolti dati nell'ambito dell'intelligence dei segnali, gli Stati Uniti vagliano la disponibilità di altre informazioni, anche di fonte diplomatica o pubblica. Le alternative adeguate e fattibili all'intelligence dei segnali devono essere privilegiate.

[41] Allegato VI dello scudo, lettera dell'Ufficio del direttore dell'intelligence nazionale (ODNI) sulle garanzie e limitazioni applicabili alle autorità di sicurezza nazionale statunitensi, pag. 3.

Il concetto di "intelligence dei segnali" non è definito né nella PPD-28 né in nessun altro testo applicabile.

3.2.2 Legge relativa alla vigilanza sull'intelligence esterna

Nel complesso il testo della FISA risulta più chiaro e più preciso. Tuttavia l'interpretazione di molte disposizioni alla luce della PPD-28 e dunque la loro applicazione pratica dipendono in gran parte dall'attuazione da parte dei vari enti. Sebbene non sia ancora disponibile una relazione completa sull'attuazione delle nuove tutele, i delegati statunitensi hanno comunicato ai rappresentanti del Gruppo di lavoro che di fatto le tutele previste dalla PPD-28 sono ormai attuate, peraltro in modo simile da parte dei vari servizi della comunità dell'intelligence statunitense.

Più esattamente, l'articolo 501 è piuttosto chiaro quanto al tipo di operazioni di intelligence che possono essere rese obbligatorie: l'acquisizione di beni materiali (compresi libri, dati, carte, documenti e altri beni). Occorre tuttavia osservare che la definizione di "beni materiali", comprendendo "altri beni", rende piuttosto ampio l'ambito di esercizio di tale potere.

L'articolo 702, che autorizza la raccolta dei dati di cittadini stranieri che si può ragionevolmente presumere siano ubicati al di fuori degli Stati Uniti al fine di ottenere informazioni di intelligence esterna[42], non offre indicazioni altrettanto dettagliate di quelle contenute all'articolo 501. Per quanta riguarda il suo ambito di applicazione, l'articolo 702 si concentra sui fornitori di servizi di comunicazione elettronica stabiliti negli Stati Uniti per la raccolta di informazioni di intelligence esterna riguardanti cittadini situati al di fuori degli Stati Uniti. La definizione di "informazioni di intelligence esterna" è ampia e comprende, tra l'altro, le informazioni relative a una potenza straniera o a un territorio straniero che riguardano la conduzione degli affari esteri degli Stati Uniti[43]; ciò solleva incertezze in ordine al tipo di informazioni che possono essere effettivamente raccolte.

Nonostante la declassificazione dei documenti, delle relazioni al Congresso e delle relazioni di vigilanza dell'Autorità per la tutela della vita privata e delle libertà civili (di seguito "PCLOB"), l'applicazione della FISA, compresi la portata e l'uso di selettori specifici, rimane poco chiara e confusa. L'uso di selettori specifici ("selettori attivati") è menzionato in un rapporto PCLOB[44], ma il Gruppo di lavoro è dell'avviso che ciò non corrisponda alle norme per la rilevazione mirata dei dati previste dall'articolo 702[45]. Per quanto il Gruppo di lavoro abbia potuto confermare, non ne è fatta menzione nelle norme generalmente accessibili.

[42] Codice degli Stati Uniti d'America, titolo 50, articolo 1881a (D)(1).
[43] Codice degli Stati Uniti d'America, titolo 50, articolo 1801 (e) (2).
[44] Autorità per la tutela della vita privata e delle libertà civili, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", pag. 32.
[45] Codice degli Stati Uniti d'America, titolo 50, articolo 1881a(D).

3.2.3 Conclusione

Nel complesso il Gruppo di lavoro rileva che i testi di riferimento relativi alle attività di intelligence sono disponibili online e che le autorità statunitensi hanno compiuto importanti passi avanti nel campo della trasparenza.

Il Gruppo di lavoro prende atto che dal 2013 sono stati pubblicati numerosi documenti quali politiche, procedure, decisioni della Corte FISA e altra documentazione declassificata. Inoltre la PCLOB ha pubblicato importanti relazioni sulle attività condotte sulla base dell'articolo 702 e della legge USA FREEDOM. È prevista la pubblicazione di una relazione analoga sulle attività condotte ai sensi dell'EO 12333.

Vari allegati di atti legislativi che potrebbero gettare luce sulle implicazioni del decreto presidenziale per coloro che si trovano al di fuori degli Stati Uniti e sulle eventuali tutele applicabili sono documenti classificati e dunque non accessibili al pubblico o a persone potenzialmente interessate dalla loro applicazione. I testi declassificati sono di scarsa utilità e forniscono poche informazioni sulle attività di intelligence.

Nonostante gli sforzi profusi per spiegare il funzionamento dell'EO 12333 in seguito alle rivelazioni di Snowden, in particolare con l'adozione della PPD-28, l'attuale applicazione pratica dell'EO 12333 è tuttora poco chiara. Il Gruppo di lavoro rileva che l'allegato VI dello scudo non fornisce indicazioni dettagliate sul funzionamento di tale decreto.

Sebbene il Gruppo di lavoro accolga con favore le limitazioni introdotte dalla PPD-28, è difficile valutare se il quadro giuridico statunitense che disciplina le attività di sorveglianza sia sufficientemente prevedibile, ovvero se contenga indicazioni adeguate delle circostanze nelle quali e delle condizioni alle quali le autorità pubbliche hanno il potere di ricorrere a siffatte misure di sorveglianza; si attendono infatti ulteriori chiarimenti, compresa la pubblicazione del rapporto PCLOB sull'EO 12333.

3.3 Garanzia B — La necessità e la proporzionalità rispetto ai legittimi obiettivi perseguiti devono essere dimostrate

3.3.1 Direttiva presidenziale 28

La PPD-28 ha introdotto limitazioni relative alle finalità per le quali i dati personali possono essere usati e alle condizioni della loro divulgazione e ha ripercussioni sulla raccolta dei dati nell'ambito dell'intelligence dei segnali, a prescindere dalla base giuridica utilizzata.

In particolare l'articolo 1 della PPD-28 stabilisce che l'attività di intelligence dei segnali condotta dagli USA dev'essere sempre quanto più possibile mirata. Pur prendendo atto di tale limitazione, è difficile stabilire se con l'espressione "quanto più possibile mirata" si intenda che tutte le attività di raccolta dati devono essere necessarie e proporzionate.

La PPD-28 riconosce che la raccolta di dati in blocco continua ad essere autorizzata al fine di individuare una minaccia nuova o emergente o di ricavare altre informazioni di rilevanza

fondamentale per la sicurezza nazionale, che spesso si nascondono nelle dimensioni e nella complessità del sistema moderno di comunicazione globale[46]. Il Gruppo di lavoro rileva che la PPD-28 definisce la raccolta dati in blocco nell'ambito dell'intelligence dei segnali come la raccolta autorizzata di grandi quantità di dati di intelligence dei segnali che, in base a considerazioni tecniche o operative, è effettuata senza il filtro di discriminanti (dispositivi specifici, selettori ecc.).

La PPD-28 fissa limiti alle finalità d'uso dei dati di intelligence dei segnali raccolti in blocco. I dati raccolti in "blocco" possono essere usati per sei finalità, tra cui l'antiterrorismo e la lotta contro altre forme gravi di criminalità (transnazionale). L'analisi del Gruppo di lavoro indica che la limitazione della finalità è piuttosto ampia (probabilmente troppo) perché possa essere considerata mirata.

La PPD-28 non scongiura la possibilità che la rilevazione in blocco dei dati personali sia effettuata in maniera indiscriminata; inoltre la portata di questo tipo di raccolta resta poco chiare e potenzialmente vasta. A tale riguardo, il Gruppo di lavoro osserva che nell'allegato VI l'ODNI afferma che qualsiasi attività di raccolta in blocco condotta sulle comunicazioni via Internet dalla comunità dell'intelligence statunitense nell'ambito dell'intelligence dei segnali interessa una bassa percentuale dell'intera rete[47]; il Gruppo di lavoro auspica pertanto che siano forniti ulteriori elementi di prova attraverso misure di trasparenza.

3.3.2 Legge relativa alla vigilanza sull'intelligence esterna (FISA)

Le procedure atte a minimizzare la raccolta dati a norma dell'articolo 215 e dell'articolo 702 della FISA sono state introdotte al fine di tutelare i cittadini statunitensi o residenti negli USA limitando l'accesso del governo ai dati che li riguardano. Ufficialmente tali limitazioni non si applicano agli stranieri, sebbene gli agenti del governo statunitense abbiano più volte ribadito, in occasione di incontri pubblici e privati con rappresentanti del Gruppo di lavoro, che l'ambito di applicazione delle procedure di minimizzazione sia stato esteso, nella pratica, a tutte le persone, a prescindere dalla loro cittadinanza o dal luogo in cui risiedono abitualmente.

L'articolo 702 precisa che l'acquisizione autorizzata è condotta nel rispetto del quarto emendamento della Costituzione degli Stati Uniti, che limita la rilevazione dei dati a quanto ritenuto conforme al principio della perquisizione giustificata. A tale riguardo non è operata alcuna distinzione tra imprese statunitensi e imprese straniere. In altri termini, se il

[46] PPD-28, articolo 2 e allegato VI dello scudo, lettera dell'Ufficio del Direttore dell'intelligence nazionale (ODNI) sulle garanzie e limitazioni applicabili alle autorità di sicurezza nazionale statunitensi, pag. 3.

[47] Allegato VI dello scudo, lettera dell'Ufficio del Direttore dell'intelligence nazionale (ODNI) sulle garanzie e limitazioni applicabili alle autorità di sicurezza nazionale statunitensi, pag. 4; il Gruppo di lavoro richiama, a tale proposito, la relazione contenente le conclusioni dei copresidenti dell'UE del gruppo di lavoro ad hoc UE-USA sulla protezione dei dati ("Report on the Findings by the EU Co-Chairs of the ad hoc EU-US Working Group on Data Protection"), nella quale si afferma che i dati sulle comunicazioni costituiscono una minima parte del traffico internet mondiale, che difatti consiste prevalentemente in elevati volumi di dati scambiati tramite streaming e download, ad esempio serie televisive, film e programmi sportivi (punto 3.1.2 della relazione)44

quarto emendamento si applicasse a tutti i dati raccolti negli Stati Uniti, la raccolta "in blocco" effettuata negli Stati Uniti sarebbe "ingiustificata" e dunque incostituzionale.

Il Gruppo di lavoro plaude alle conclusioni contenute nel rapporto PCLOB, secondo le quali nella pratica anche i cittadini stranieri beneficiano delle restrizioni applicabili all'accesso ai dati e alla loro conservazione che sono previste dalle procedure attuate dai diversi enti per rendere mirata e/o ridurre al minimo la raccolta dati. Secondo il suddetto rapporto, considerati i costi e le difficoltà associati all'individuazione e alla cancellazione di informazioni concernenti cittadini statunitensi o residenti negli USA all'interno di un ampio corpus di dati, solitamente l'intero insieme di dati sarà trattato nel rispetto dei massimi standard di tutela applicabili ai cittadini statunitensi.

Il Gruppo di lavoro rileva inoltre che, in base alle conclusioni della PCLOB, il programma non opera attraverso la raccolta in blocco di dati sulle comunicazioni. La relazione "Statistical Transparency Report" pubblicata dall'ODNI nel 2014 conferma tale constatazione. Sempre secondo il rapporto PCLOB, per rendere mirata l'attività di sorveglianza si utilizzano selettori attivati, quali gli indirizzi di posta elettronica o i numeri di telefono[48].

Le corrispondenti norme accessibili al pubblico relative all'individuazione degli obiettivi della raccolta non prevedono tuttavia siffatte disposizioni mirate e sono intese unicamente ad evitare che siano presi a obiettivo cittadini statunitensi o domiciliati negli Stati Uniti. Inoltre i benefici concreti di cui, secondo la PCLOB, godono i cittadini stranieri non sono giuridicamente vincolanti o stabiliti per legge, in quanto la legislazione vigente in materia di individuazione degli obiettivi non prevede questo tipo di norme mirate ed è unicamente intesa ad evitare che siano presi a obiettivo cittadini statunitensi o domiciliati negli Stati Uniti.

Il Gruppo di lavoro ricorda inoltre che, ai fini dell'articolo 702, per "persone" si intendono non soltanto le persone fisiche ma anche gruppi, enti, associazioni, società o potenze straniere. Inoltre il fatto che la raccolta sia giustificata dal perseguimento di uno degli scopi rilevanti dell'acquisizione, che dev'essere quello di ottenere informazioni di intelligence esterna, lascia un certo margine di incertezza quanto alla finalità e alla necessità della raccolta stessa. Il Gruppo di lavoro, tuttavia, apprezza l'indicazione fornita nell'allegato VI, nel quale si precisa che, nel 2014, hanno costituito obiettivi a norma dell'articolo 702 circa 90 000 persone[49]. Il primo riesame dello scudo offrirà l'occasione di presentare ulteriori elementi di prova riguardo alle regole che disciplinano l'individuazione degli obiettivi della raccolta.

Ad oggi non esiste una giurisprudenza consolidata sulla legalità della rilevazione indiscriminata e in massa dei dati e del successivo uso di dati personali a fini di lotta contro la criminalità, compresa la questione di stabilire in quali circostanze si possa procedere alla raccolta e all'uso di dati personali per tali scopi. La Corte di giustizia dovrebbe pronunciarsi, almeno in parte, su tale questione nel corso del 2016, sia nell'ambito delle cause congiunte

[48] Autorità per la tutela della vita privata e delle libertà civili, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", pag. 32.
[49] Allegato VI, pag. 11.

Tele2 Sverige AB contro Post- och telestyrelsen e Secretary of State for the Home Department contro Davis e altri[50] sia tramite il parere che dovrà emettere sulla validità dell'accordo PNR con il Canada[51]. Nel frattempo il Gruppo di lavoro ricorda di avere più volte ribadito che la raccolta di dati indiscriminata e in massa non è da considerarsi in alcun caso proporzionata[52].

3.3.3 Conclusione

Nonostante le limitazioni imposte con l'introduzione della PPD-28, le preoccupazioni del Gruppo di lavoro permangono, soprattutto per quanto riguarda la proporzionalità della raccolta dati. In primo luogo vi sono indicazioni del fatto che gli Stati Uniti continuano ad acquisire dati in massa e in maniera indiscriminata, o perlomeno gli elementi emersi non consentono di escludere che tale attività proseguirà anche in futuro. Il Gruppo di lavoro ha costantemente sostenuto che una siffatta raccolta di dati non è conforme al diritto dell'Unione ed è pertanto inaccettabile.

In secondo luogo il Gruppo di lavoro osserva che anche il trattamento di dati rilevati in maniera mirata, o il trattamento "quanto più possibile mirato", può comunque essere considerato un trattamento in massa. La questione di stabilire se si debba autorizzare o meno una siffatta rilevazione in massa è attualmente oggetto di procedimenti dinanzi alla Corte di giustizia. Per tale ragione il Gruppo di lavoro non intende effettuare una valutazione definitiva in ordine alla legalità del trattamento di dati in massa, seppur mirato. Tuttavia esso sottolinea che qualora il trattamento mirato e in massa dei dati fosse consentito, i principi di individuazione degli obiettivi dovrebbero applicarsi tanto alla raccolta quanto al successivo uso dei dati e non potrebbero essere limitati al solo uso. In ogni caso è necessario che il progetto di decisione sull'adeguatezza fornisca chiarimenti in ordine alle sei finalità per le quali i dati possono essere raccolti "in blocco", quali menzionate nella PPD-28. A questo stadio il Gruppo di lavoro non è convinto che tali finalità siano sufficientemente ristrette da poter garantire che la raccolta dati sia effettivamente limitata a quanto necessario e proporzionato.

3.4 Garanzia C — Necessità di un meccanismo di vigilanza indipendente

Gli Stati Uniti non dispongono di un unico organo di vigilanza a livello federale incaricato di vigilare sulle implicazioni che i programmi di intelligence e sorveglianza hanno in termini di privacy e di protezione dei dati. Le attività di intelligence condotte dagli Stati Uniti sono invece soggette a un processo di vigilanza multilivello, articolato in una vigilanza interna e in una vigilanza esterna. Il Gruppo di lavoro riconosce che la prassi di comunicazione degli organi di vigilanza statunitensi è molto dettagliata e prevalentemente accessibile al pubblico.

[50] Corte di giustizia, cause riunite C-203/15 e C-698/15.
[51] Corte di giustizia, causa A-1/15.
[52] WP215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_it.pdf.

3.4.1 Vigilanza interna

Tutti i servizi di intelligence e di sicurezza statunitensi vantano la presenza, nel proprio organico, di addetti cui spetta il compito di assicurare la conformità con il quadro legislativo; tra questi figurano gli ispettori generali, incaricati principalmente di valutare se i vari servizi operino nel rispetto della normativa, comprese a titolo esemplificativo ma non limitativo le leggi in materia di privacy e protezione dei dati. Gli ispettori generali sono istituiti per legge e sono (o saranno a breve) tutti nominati dal Presidente e successivamente confermati dal Senato, nel tentativo di garantire la loro indipendenza organizzativa e di assicurare che riferiscano al Congresso. Il Gruppo di lavoro ritiene pertanto che gli ispettori generali potrebbero soddisfare il criterio dell'indipendenza organizzativa, quale definito dalla Corte di giustizia e dalla Corte europea dei diritti dell'uomo, perlomeno a partire dal momento in cui sarà estesa a tutti la nuova procedura di nomina. Nel frattempo permangono perplessità per quanto riguarda gli ispettori generali la cui nomina compete tuttora al direttore del servizio sul quale vigilano.

Gli ispettori generali possono formulare raccomandazioni che successivamente possono essere sottoposte al Dipartimento della Giustizia e alla PCLOB o addirittura alla commissione del Congresso che può imporne l'attuazione. Qualora l'ispettore generale rilevi una violazione, essa potrà essere gestita mediante misure interne e di politica e sarà segnalata al Congresso. L'ispettore generale ha il potere, ad esempio, di effettuare verifiche e indagini.

Il Gruppo di lavoro rileva che l'accesso pubblico ai rapporti emessi dall'ispettore generale può essere negato; rileva inoltre che all'ispettore generale può essere vietato di trasmettere i suoi rapporti se le informazioni su cui svolge indagini risultano classificate. Ad ogni modo i rapporti emessi saranno sempre sottoposti alla vigilanza del Congresso, il che rappresenta una tutela fondamentale, pur non creando i presupposti per un ricorso individuale.

Presso tutti i servizi lavorano addetti alla tutela della vita privata e alle libertà civili, che coadiuvano l'attività di preparazione delle relazioni sotto la vigilanza del Congresso.

Nel complesso i meccanismi di vigilanza interna esistenti possono essere ritenuti piuttosto solidi; tuttavia al fine di giustificare l'ingerenza nei diritti fondamentali alla tutela della vita privata e alla protezione dei dati personali, la vigilanza deve essere totalmente indipendente. Inoltre, pur rispettando e apprezzando l'operato dei vari addetti alla tutela della vita privata e alle libertà civili, il Gruppo di lavoro non può concludere che essi abbiano il grado di indipendenza necessario per potere esercitare un controllo indipendente.

3.4.2 Vigilanza esterna

La vigilanza esterna è attuata attraverso una molteplicità di meccanismi diversi: il controllo giurisdizionale da parte della Corte FISA a norma degli articoli 501 e 702, la vigilanza esercitata dalle commissioni scelte del Congresso per i servizi di intelligence (Select Intelligence Committees) e le attività espletate dalla PCLOB.

Il Gruppo di lavoro ricorda che, idealmente, come stabilito peraltro dalla Corte di giustizia e dalla Corte europea dei diritti dell'uomo, il controllo dovrebbe spettare ad un giudice, al fine di garantire l'indipendenza e l'imparzialità del procedimento. Fino a poco tempo fa, la procedura dinanzi alla Corte FISA era ex parte, ovvero gli interessati non avevano la possibilità di essere ascoltati e nemmeno di essere informati del procedimento. Tale procedura rimane tuttora ex parte; tuttavia a seguito dell'adozione della legge USA FREEDOM è stata introdotta la figura dell'amicus curiae. Gli amici curiae agiscono in maniera indipendente ma non sono chiamati a difendere persone specifiche che potrebbero essere parte in causa.

La legge USA FREEDOM ha istituito un gruppo di amici curiae incaricati di presentare alla Corte FISA una memoria sui casi importanti. La Corte ha scelto cinque avvocati che hanno ottenuto l'adeguato nulla osta di sicurezza e che forniscono consulenza tecnica, presenziano alle udienze della Corte FISA e trasmettono memorie, oltre a fornire una valutazione di merito nell'ottica della tutela della privacy e dei diritti civili. Tuttavia essi intervengono soltanto nei procedimenti importanti o quando emergono nuove questioni giuridiche[53].

L'articolo 215 è quasi interamente soggetto a controllo giurisdizionale ex ante (ma non ex post), in quanto tutti i programmi che ricorrono all'articolo 215 come base per la raccolta dei dati sono soggetti all'approvazione della Corte FISA. Il rapporto PCLOB precisa che l'articolo 702 differisce dalla disciplina FISA sulla sorveglianza elettronica tradizionale sia per quanto riguarda i criteri applicati sia perché la Corte FISA non esprime una valutazione sull'individuazione personalizzata dei singoli obiettivi della sorveglianza. In base a tale articolo, il Procuratore generale e il Direttore dell'intelligence nazionale preparano certificazioni annuali che consentono di prendere a obiettivo cittadini stranieri che si ritiene ragionevolmente si trovino al di fuori degli Stati Uniti, al fine di acquisire informazioni di intelligence esterna, senza specificare alla Corte FISA quali siano i singoli cittadini stranieri presi a obiettivo. Inoltre il governo non ha l'obbligo di dimostrare un motivo plausibile per ritenere che l'obiettivo della raccolta a norma dell'articolo 702 sia una potenza straniera o l'agente di una potenza straniera, come invece prevede la disciplina FISA tradizionale[54].

In seno al Congresso anche le commissioni scelte sui servizi di intelligence hanno competenze di vigilanza riguardo all'approvazione delle attività di intelligence, in particolare attraverso il voto del bilancio. Le commissioni Intelligence del Senato e della Camera dei rappresentanti ricevono memorie classificate sulle attività di intelligence. Ogni sei mesi il Procuratore generale deve riferire a queste commissioni in merito alla sorveglianza elettronica a norma della FISA. Il Gruppo di lavoro attende di conoscere in che misura tali commissioni possono esaminare il trattamento dei dati concernenti singole persone, soprattutto quando si tratta di cittadini stranieri.

La PCLOB è un ente indipendente, inquadrato nell'esecutivo statunitense, al quale sono conferiti due poteri fondamentali; 1) verificare ed esaminare le azioni intraprese dall'esecutivo

[53] Legge USA FREEDOM, TITOLO IV--FOREIGN INTELLIGENCE SURVEILLANCE COURT REFORMS, articolo 401. "Appointment of amici curiae".
[54] Autorità per la tutela della vita privata e delle libertà civili, "Report on the Surveillance Program Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", pagg. 24 e 25.

per proteggere gli Stati Uniti dal terrorismo, accertando che vi sia un equilibrio fra la necessità di tali interventi e l'esigenza di tutelare la vita privata e le libertà civili, e 2) provvedere a che l'elaborazione e l'attuazione delle leggi, dei regolamenti e delle politiche riguardanti gli sforzi per proteggere il paese dal terrorismo tengano adeguatamente conto delle considerazioni legate alle libertà. Il Gruppo di lavoro rileva che la PCLOB dispone anche del potere di emanare inviti a comparire e ha inoltre accesso alle informazioni classificate. Nello svolgimento dei suoi compiti, la PCLOB verifica inoltre l'efficacia dei programmi. Essa esercita una vigilanza ex post e non ex ante. La PCLOB ha dimostrato i suoi poteri indipendenti ponendosi in contrasto con il Presidente degli Stati Uniti riguardo ad alcune questioni giuridiche. In particolare essa ha constatato come il programma sui metadati telefonici basato sull'articolo 215 fosse illegalmente autorizzato, concludendo che esso era inefficace in quanto non vi erano prove di attacchi tali da causare effetti perturbanti. La PCLOB ha inoltre effettuato uno studio della durata di un anno concernente il programma a norma dell'articolo 702 e ha constatato che tale programma è legale e chiaramente autorizzato per legge e che l'articolo 702 si è rivelato assai efficace anche in materia di terrorismo. La PCLOB è inoltre intervenuta sull'obbligo di trasparenza, rilevando che per vari elementi classificati la classificazione non era necessaria. La PCLOB dovrebbe presentare a breve una relazione sull'attuazione della PPD-28. A tale proposito, essa ritiene che il semplice fatto che una persona sia straniera non è di per sé sufficiente a giustificare la conservazione delle informazioni che la riguardano.

Il Gruppo di lavoro osserva infine che l'EO 12333 non prevede nessun meccanismo di ricorso, vigilanza o controllo giurisdizionale per i programmi sorveglianza condotti sulla base del decreto stesso.

3.4.3 Conclusione

Il progetto di decisione sull'adeguatezza dimostra che negli Stati Uniti esistono meccanismi di vigilanza interna ed esterna a più livelli. Sebbene il funzionamento di tali meccanismi possa creare confusione, il Gruppo di lavoro constata con soddisfazione che, in generale, i meccanismi di vigilanza interna predisposti sono sufficienti. Esso tuttavia esprime preoccupazione per la scarsa vigilanza sui programmi di sorveglianza condotti sulla base dell'EO 12333.

Il Gruppo di lavoro rileva che la critica che aveva precedentemente mosso in ordine al carattere non contraddittorio dei procedimenti dinanzi alla Corte FISA è solo parzialmente attenuata dall'introduzione dell'istituto dell'amicus curiae, che è incaricato di agire "a difesa della privacy e delle libertà civili". Tuttavia la Corte FISA non esercita un controllo giurisdizionale efficace sull'individuazione dei cittadini stranieri da sottoporre a sorveglianza. Permangono inoltre alcuni dubbi quanto alla capacità della Corte FISA di valutare efficacemente le procedure atte a rendere mirata e a ridurre al minimo la raccolta dei dati, come affermato peraltro dalla PCLOB[55].

[55] Autorità per la tutela della vita privata e delle libertà civili, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", pag. 11.

3.5 Garanzia D — Necessità di mettere a disposizione della persona mezzi di ricorso efficaci

3.5.1 Mezzi di ricorso giurisdizionale

3.5.1.1 Obbligo della legittimazione ad agire

Il regime dei ricorsi giurisdizionali statunitense contiene un'importante limitazione: la Costituzione degli Stati Uniti obbliga la persona a dimostrare la propria legittimazione ad agire; è cioè necessario che il ricorrente abbia subito o sia destinato a subire un danno o pregiudizio diretto e che tale danno sia riparabile. A livello federale, non è possibile intentare un'azione legale semplicemente a motivo del fatto che una persona o un gruppo è insoddisfatto di un'azione o di una legge del governo[56]. Tale requisito risulta vanificato dalla mancata notifica alle persone sottoposte a sorveglianza anche dopo la cessazione delle misure. La Corte di giustizia e la Corte europea dei diritti dell'uomo hanno più volte affermato che la persona deve potersi avvalere di rimedi amministrativi o giurisdizionali. Nella sentenza pronunciata nella causa Zakharov, la Corte europea dei diritti dell'uomo ha confermato che, in base alla giurisprudenza, può ricorrere in giudizio chiunque abbia un motivo legittimo per sospettare un'ingerenza nei suoi diritti fondamentali[57],

Inoltre secondo la giurisprudenza della Corte suprema degli Stati Uniti d'America[58] gli stranieri che si trovano al di fuori degli Stati Uniti non godono della piena tutela costituzionale negli Stati Uniti. Questo vale in particolare per il quarto emendamento, che tutela i cittadini statunitensi, ma non gli stranieri, contro le perquisizioni e i sequestri ingiustificati e dal quale deriva in massima parte il diritto alla tutela della sfera privata negli Stati Uniti. I cittadini europei e gli altri europei che vivono fuori dagli Stati Uniti sono semplicemente esclusi dalla tutela prevista dal quarto emendamento[59]

L'applicazione limitata del Judicial Redress Act o legge sul ricorso giurisdizionale (sia dal punto di vista sostanziale, in quanto esclude la sicurezza nazionale, sia in relazione alle persone che possono invocarne le disposizioni), nonché le numerose esenzioni e l'incertezza giuridica riguardo agli enti ai quali la legge si applicherà non soddisfano il requisito di offrire un meccanismo di ricorso efficace a tutte le persone interessate da misure di sorveglianza per la raccolta di informazioni di intelligence a fini di sicurezza nazionale.

3.5.1.2 Direttiva presidenziale PPD-28

Il Gruppo di lavoro osserva che la PPD-28 è solo una direttiva e dunque non può attribuire diritti alla persona. Il conferimento di diritti può avvenire soltanto attraverso atti legislativi. Pertanto la persona non può rivolgersi al giudice sulla base di una presunta violazione delle tutele previste dalla PPD-28.

---

[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing; Clapper contro Amnesty International USA

[57] Corte europea dei diritti dell'uomo, sentenza Zakharov, punto 171.

[58] U.S. contro Verdugo - Urquidez , pagg. 264-266.

[59] Relazione dei copresidenti dell'UE, punto 2.

3.5.1.3 Foreign Intelligence Surveillance Act

La FISA offre alla persona alcune possibilità di ricorso in caso di sorveglianza illecita. A norma della FISA, la persona lesa, diversa da una potenza straniera o da un agente di una potenza straniera, che è stata sottoposta a sorveglianza elettronica o i cui dati, ottenuti da un'attività di sorveglianza elettronica, sono stati usati o divulgati in violazione dell'articolo 1809 ha la possibilità di intentare un'azione contro chiunque abbia commesso tale violazione. Tuttavia, ciò esclude esplicitamente la potenza straniera o l'agente di una potenza straniera cui sono state applicate le misure. Ad ogni modo, come già precisato, il ricorrente dovrà dimostrare la propria legittimazione ad agire, il che non sarà possibile nella pratica.

La legge USA FREEDOM ha istituito il comitato consultivo degli amici curiae, incaricato di coadiuvare la Corte FISA formulando un parere (facoltativo) nei casi che comportano un'interpretazione rilevante e inedita della legge. Questo comitato, tuttavia, ha il compito di esprimere un parere imparziale e non di difendere gli interessi di una persona specifica su istanza di quest'ultima.

3.5.2 Ricorsi amministrativi

3.5.2.1 Ispettori generali

Un'altra via di ricorso è rappresentata dalla possibilità di presentare un reclamo all'ispettore generale. Gli ispettori generali, tuttavia, non hanno l'obbligo di esaminare ogni singolo reclamo: non è previsto il diritto di essere ascoltati, ma gli ispettori generali dispongono di un potere discrezionale. L'ispettore generale può inoltre presentare rapporti sulle violazioni constatate se le informazioni sono declassificate. Qualora una persona presuma che il rapporto la riguardi, potrà rivolgersi al giudice sulla base della constatazione riguardante la violazione della legge.

3.5.2.2 Legge sulla libertà di informazione (Freedom of Information Act, FOIA)

Tra i vari mezzi di ricorso a disposizione di tutti i cittadini, è possibile presentare una domanda ai sensi della legge sulla libertà di informazione (FOIA). Secondo il governo degli Stati Uniti, in genere qualunque cittadino (statunitense o straniero) può presentare una domanda a norma della FOIA semplicemente chiedendo l'accesso ai dati di qualsiasi ente, compresi i dati riguardanti la persona, anche se in questo caso è obbligatorio presentare un documento che certifichi l'identità. Se tuttavia le informazioni richieste sono classificate per tutelare la sicurezza nazionale, è improbabile che la domanda a norma della FOIA sia accolta, in quanto è prevista un'esenzione in base alla quale gli enti non hanno l'obbligo di fornire l'accesso alle informazioni classificate, anche qualora dette informazioni riguardino la persona che ha inoltrato la domanda. Non possono formare oggetto di una domanda a norma della FOIA le informazioni relative a indagini dei servizi di contrasto. Infine il Gruppo di lavoro ritiene che la domanda a norma della FOIA non conferisca il diritto di ottenere che la legalità del trattamento sia verificata da un'autorità indipendente.

3.5.3 Mediatore dello scudo

3.5.3.1 Istituzione del Mediatore

Il regime dello scudo istituisce un nuovo meccanismo attraverso il quale le "persone dell'UE" possono presentare domande relative alle "attività di intelligence dei segnali condotte dagli Stati Uniti" al nuovo Mediatore dello scudo. Come spiegato nel memorandum allegato alla lettera del segretario di Stato John Kerry del 22 febbraio 2016, il ruolo di Mediatore sarà rivestito dalla Sottosegretaria C. Novelli, che eserciterà tale funzione mantenendo l'incarico di "Prima coordinatrice della diplomazia internazionale per le tecnologie dell'informazione", istituito dall'articolo 4, lettera d), della PPD-28. Nella lettera e nel memorandum si sottolinea che la Sottosegretaria "riferisce direttamente al segretario di Stato" ed è "indipendente dalla comunità dell'intelligence".

Il memorandum chiarisce che, nonostante il nome, il Mediatore dello scudo non si limiterà a trattare le domande relative all'accesso, per motivi di sicurezza nazionale, ai dati trasmessi dall'Unione europea agli Stati Uniti nell'ambito dello scudo ma si occuperà anche di quelle relative ai dati che sono stati trasmessi nell'ambito delle clausole contrattuali tipo, delle norme vincolanti d'impresa, delle deroghe (ai sensi dell'articolo 26 della direttiva 95/46/CE) o delle "eventuali deroghe future", quali definite nella nota in calce 2 del memorandum.

In sintesi, il meccanismo dovrebbe funzionare con la seguente modalità: una persona dell'UE presenta una domanda a un ente di uno Stato membro competente della vigilanza sui servizi di sicurezza nazionale, oppure a un organo centralizzato "di trattamento e trasmissione dei reclami presentati da persone dell'UE", ove creato o designato. L'autorità che inoltra la domanda al Mediatore dovrà dapprima verificarne la completezza, come precisato al punto 3, lettera b., della lettera[60]. Una volta che la domanda è stata trasmessa al Mediatore e risulta conforme alla parte 3, punto b., il Mediatore risponde, ovvero conferma in modo definitivo "i) che il reclamo è stato esaminato adeguatamente e ii) che sono stati rispettati le leggi, i regolamenti, i decreti e le direttive presidenziali e le politiche degli enti che negli Stati Uniti disciplinano le limitazioni e le garanzie esposte nella lettera dell'Ufficio del direttore dell'intelligence nazionale (ODNI) oppure, se non sono stati rispettati, che l'inosservanza è stata nel frattempo sanata"[61]. La risposta "non conferma né nega che la persona sia stata sottoposta a sorveglianza né indica la specifica misura correttiva applicata"[62]. Quanto alla modalità con cui il Mediatore svolgerà le indagini, è precisato che il Mediatore "opera in

[60] b. L'organo di trattamento e trasmissione dei reclami presentati da persone dell'UE accerta che la domanda sia completa:
i) verificando l'identità della persona e il fatto che agisca per proprio conto e non in rappresentanza di un governo o di un'organizzazione intergovernativa.
ii) verificando che la domanda sia redatta per iscritto e includa almeno le seguenti indicazioni:
• tutte le informazioni che ne costituiscono il fondamento,
• la natura delle informazioni o della riparazione richieste,
• eventualmente, l'ente o gli enti dell'amministrazione degli Stati Uniti che si ritiene siano implicati,
• le altre misure attuate per ottenere le informazioni o la riparazione richieste e la risposta ricevuta in tale contesto;
iii) verificando che la domanda verta su dati che si può ragionevolmente presumere siano stati trasferiti dall'UE agli USA nell'ambito dello scudo, delle clausole contrattuali tipo, delle norme vincolanti d'impresa, delle deroghe o delle eventuali deroghe future;
iv) accertando *prima facie* che la domanda non sia futile, vessatoria o in malafede.
[61] Allegato III, parte 4., lettera e. dello scudo.
[62] Allegato III, parte 4., lettera e. dello scudo.

stretta collaborazione con altri enti dell'amministrazione statunitense, compresi i competenti organi indipendenti di vigilanza"[63] e, più specificamente, "ha facoltà di operare in stretto coordinamento con l'Ufficio del direttore dell'intelligence nazionale, il Dipartimento della Giustizia e, secondo i casi, altri dipartimenti e enti statunitensi attivi nel settore della sicurezza nazionale degli Stati Uniti, così come con gli ispettori generali, gli addetti alla legge sulla libertà d'informazione e i funzionari che si occupano delle libertà civili e del rispetto della vita privata"[64]. Tale coordinamento deve assicurare che la risposta del Mediatore contenga tutte le conferme di cui sopra.

3.5.3.2 Valutazione del nuovo meccanismo di mediazione

Il Gruppo di lavoro riconosce gli sforzi profusi dalla Commissione europea e dal governo statunitense per introdurre un nuovo meccanismo inteso a migliorare le possibilità di ricorso in relazione alle attività di sorveglianza condotte dagli Stati Uniti. È evidente che la valutazione di tale meccanismo, che rappresenta un elemento di novità nelle relazioni internazionali per quanto riguarda l'intelligence dei segnali o la sicurezza nazionale, riveste particolare importanza.

Nella presente sezione il Gruppo di lavoro valuta il rapporto tra l'istituzione del meccanismo di mediazione e i requisiti necessari affinché la persona possa chiedere riparazione attraverso le vie legali, quali previsti nella Carta, nella CEDU e nella giurisprudenza degli organi giurisdizionali europei.

3.5.3.3 L'istituzione del meccanismo di mediazione può essere di per sé sufficiente?

In primo luogo occorre chiedersi se l'istituzione del "Mediatore" possa essere ritenuta conforme all'articolo47 della Carta, che fa riferimento a un ricorso effettivo davanti a un giudice imparziale[65], almeno nel caso in cui non siano disponibili altri mezzi di ricorso efficaci. Tale questione è rilevante in quanto nella sentenza Schrems la Corte di giustizia, nell'importante considerazione di cui al punto 95, cita l'articolo 47 della Carta, e lo fa senza fornire alcuna indicazione del fatto che l'articolo 47 debba presumibilmente essere oggetto di un'interpretazione modificata nel contesto delle misure di sorveglianza. Viceversa nella causa Kadi II[66] la Corte di giustizia aveva già applicato l'articolo 47 della Carta alle misure di sorveglianza per motivi di sicurezza nazionale e internazionale[67].

La giurisprudenza della Corte europea dei diritti dell'uomo, tuttavia, ha stabilito con molta chiarezza che il ricorso dinanzi al giudice ordinario non è una condizione perché i programmi

[63] Allegato III, parte 2, lettera a., dello scudo.
[64] Allegato III, parte 2, lettera a., dello scudo.
[65] Nelle spiegazioni relative alla Carta dei diritti fondamentali è inoltre precisato che l'articolo 47 dovrebbe essere interpretato nel senso che esso garantisce il diritto a un ricorso effettivo dinanzi a un giudice (Spiegazioni relative alla Carta dei diritti fondamentali, spiegazione relativa all'articolo 47 (2007/C 303/02)).
[66] Sentenza del 18 luglio 2013 nelle cause riunite C-584/10 P, C-593/10 P e C-595/10 P, Commissione europea e Regno Unito contro Kadi.
[67] Kadi II, punti 97 e 100: tutti gli atti dell'Unione, compresi quelli che mirano ad attuare risoluzioni adottate dal Consiglio di Sicurezza in base al capitolo VII della Carta delle Nazioni Unite, sono sottoposti a un controllo di legittimità da parte dei giudici dell'Unione europea (il capitolo VII riguarda le azioni rispetto alle minacce alla pace, alle violazioni della pace ed agli atti di aggressione).

di sorveglianza possano essere considerati conformi all'articolo 8 (e all'articolo 13 della CEDU)[68]. Al contrario la Corte ha stabilito in base all'articolo 8, quale necessaria tutela dalle attività di sorveglianza, che può essere opportuno il ricorso dinanzi ad altre autorità. La Corte europea dei diritti dell'uomo ha comunque alte aspettative nei confronti delle altre autorità chiamate a garantire un ricorso effettivo, affermando che esse devono essere indipendenti dalle autorità che effettuano la sorveglianza ed essere dotate di poteri e competenze sufficienti per esercitare un controllo continuo ed efficace[69].

Nelle sentenze Kennedy e Klass la Corte europea dei diritti dell'uomo ha fornito indicazioni sul significato che tali aspettative potrebbero avere nel contesto della sorveglianza segreta, quando l'interessato non è informato del trattamento dei dati che lo riguardano. In entrambe le sentenze la Corte europea dei diritti dell'uomo ha ritenuto che le autorità fossero indipendenti, soprattutto rispetto agli enti che svolgono le attività di sorveglianza, ma anche indipendenti rispetto alle istruzioni[70] impartite da qualunque altra autorità. Più specificamente nella sentenza Kennedy la Corte ha approvato un'autorità indipendente e imparziale che aveva adottato il proprio regolamento interno e i cui componenti esercitavano, o avevano esercitato, un'alta funzione giurisdizionale o erano giuristi esperti[71].

Nel procedere all'esame dei reclami dei cittadini, le autorità citate nelle due sentenze avevano inoltre avuto accesso a tutte le informazioni pertinenti, compresi elementi secretati. Infine entrambe disponevano dei poteri necessari per sanare le non conformità[72].

Oltre alla questione se il Mediatore possa essere considerato un "giudice", l'applicazione dell'articolo 47, paragrafo 2, della Carta comporta un'ulteriore difficoltà, in quanto prevede che il giudice sia "costituito per legge". Tuttavia un memorandum che illustra il funzionamento di un nuovo meccanismo difficilmente può essere considerato "legge".

Di conseguenza, tenendo presente il principio della sostanziale equivalenza, anziché valutare se il Mediatore possa essere formalmente considerato un giudice costituito per legge, il Gruppo di lavoro ha deciso di esaminare in maggior dettaglio le sfumature della giurisprudenza per quanto riguarda i requisiti specifici necessari per poter ritenere che i rimedi giuridici e i mezzi di ricorso rispettino i diritti fondamentali sanciti dagli articoli 7, 8 e 47 della Carta e dall'articolo 8 (e dall'articolo 13) della CEDU. Nella sua ulteriore analisi, esaminando il campo di applicazione del nuovo meccanismo, il Gruppo di lavoro si concentrerà pertanto sui seguenti criteri: il requisito che consiste nella presentazione di una domanda al Mediatore e nel ricevimento di una risposta (legittimazione ad agire), l'indipendenza del Mediatore, il potere di indagine di cui dispone per accedere al materiale

[68] L'articolo 13 della Convenzione europea dei diritti dell'uomo obbliga gli Stati membri a garantire che "[o]gni persona i cui diritti e le cui libertà […] siano stati violati, ha diritto a un ricorso effettivo davanti a un'istanza nazionale". Tale istanza non deve essere necessariamente un'autorità giurisdizionale, come è stato chiarito dalla Corte europea dei diritti dell'uomo nella sentenza Klass, punti 56 e 67.
[69] Sentenza Klass, punti 56 e 67.
[70] Corte europea dei diritti dell'uomo, sentenza Klass, punti 21 e 53.
[71] La commissione G 10 (all'epoca della sentenza) è composta da tre membri, tra cui il presidente, che deve essere idoneo all'esercizio delle funzioni giudiziarie (sentenza Klass, punti 21 e 53).
[72] Corte europea dei diritti dell'uomo, sentenza Kennedy, punto 167, e sentenza Klass, punti 21 e 53.

necessario, compresi documenti classificati, e per chiedere assistenza ad altri enti e, infine, il potere di sanare le non conformità.

3.5.3.4 Campo di applicazione del meccanismo di mediazione

Per quanto riguarda l'accesso al Mediatore, il Gruppo di lavoro ritiene che tutti coloro che sono assoggettati al diritto dell'Unione dovrebbero beneficiare delle tutele offerte dallo scudo. Sarebbe inaccettabile operare un distinguo sulla base della cittadinanza, soprattutto dato che i diritti fondamentali nell'Unione europea si applicano a chiunque, e non soltanto a chi è in possesso di un passaporto dell'UE. L'allegato III fa riferimento alle "persone dell'UE" senza precisare chi siano. Il Gruppo di lavoro deplora tale incertezza e propone di chiarire che tutti i soggetti ricadenti nella sfera di applicazione del diritto dell'UE hanno diritto al trattamento della domanda presentata al Mediatore in base alle condizioni stabilite nel memorandum. Inoltre la Commissione e gli Stati Uniti dovrebbero affrontare la questione della misura in cui lo scudo si applicherà anche ai cittadini / residenti dei paesi del SEE e della Svizzera, che in passato beneficiavano della copertura offerta dal regime dell'approdo sicuro.

Il Gruppo di lavoro rileva inoltre qualche incertezza in ordine all'ambito di applicazione del meccanismo di mediazione. Se da un lato il memorandum precisa che il Mediatore è incaricato del trattamento delle domande relative all'accesso motivato dalla sicurezza nazionale ai dati trasmessi dall'Unione europea agli Stati Uniti nell'ambito di tutti gli strumenti di trasferimento disponibili in base al diritto dell'UE, dall'altro è precisato che il memorandum istituisce un meccanismo "in materia di intelligence dei segnali". Quest'ultima espressione indica che sono coperti soltanto i trasferimenti di dati che sono stati raccolti tramite attività di intelligence dei segnali. Ciò porta a chiedersi se la raccolta di dati ai sensi della FISA sia considerata "intelligence dei segnali". La risposta è affermativa per quanto riguarda l'articolo 702, come spiegato nella dichiarazione dell'ODNI, a pagina 10[73]. Il Gruppo di lavoro deplora tuttavia il fatto che l'uso dell'espressione "intelligence dei segnali" crei un'inutile incertezza in tale contesto.

Secondo il gruppo di lavoro, un'altra conseguenza è che il meccanismo di mediazione non sembra contemplare le domande relative all'accesso da parte degli enti preposti all'applicazione della legge[74]. Se tale interpretazione è corretta, non è chiaro se le domande provenienti da alcuni enti, in particolare la CIA, siano contemplate dal meccanismo.

3.5.3.5 Legittimazione ad agire e procedura di inoltro della domanda

Promuovere un'azione dinanzi i giudici ordinari degli Stati Uniti contro le misure di sorveglianza del governo statunitense è molto difficile. Il Gruppo di lavoro è consapevole che la Corte Suprema ha negato la legittimazione ad agire in alcuni casi relativi all'intelligence nei quali il richiedente non era stato in grado di dimostrare un pregiudizio individuale concreto, dettagliato, ed effettivo o imminente[75]. A tale riguardo l'istituzione della figura del Mediatore

[73] Allegato VI, pag. 10, dello scudo.
[74] Memorandum relativo all'istituzione del meccanismo di mediazione, pag. 1.
[75] Clapper contro Amnesty International USA, 568 U.S. ___ (2013) II. pag. 10.

rappresenta un passo importante, in quanto offre un'ulteriore possibilità di ricorso che altrimenti non esisterebbe. Il Gruppo di lavoro accoglie dunque con favore le precisazioni contenute nella parte 3, lettera c., in base alla quale per presentare una domanda nell'ambito del nuovo meccanismo non è necessario dimostrare che l'accesso ai dati riguardanti il richiedente sia effettivamente avvenuto attraverso attività di intelligence dei segnali.

Il Gruppo di lavoro approva in massima parte la procedura di identificazione del reclamante nel quadro del meccanismo di mediazione. È assolutamente sensato che l'identificazione sia effettuata nel territorio dell'Unione, come avviene peraltro per il meccanismo di accesso nell'ambito dell'accordo TFTP2 tra l'UE e gli USA. Tuttavia il Gruppo di lavoro non comprende perché la verifica nell'UE debba essere effettuata da un'autorità degli Stati membri "competente della vigilanza sui servizi di sicurezza nazionale". In primo luogo, sembra improbabile che, ai sensi dell'articolo 4, paragrafo 2, del trattato sull'Unione europea la Commissione europea sia nella posizione di attribuire a tali enti compiti che rientrano nella sfera di competenza degli Stati membri.

Inoltre data la presenza, negli Stati membri, di svariati meccanismi di vigilanza sui servizi di sicurezza nazionale, il coinvolgimento delle relative autorità potrebbe compromettere gravemente l'efficacia del sistema per i cittadini degli Stati membri. Ciò potrebbe accadere, ad esempio, se esistono diverse autorità incaricate della vigilanza sui servizi di sicurezza nazionale, nel qual caso il cittadino potrebbe avere difficoltà a individuare l'autorità competente, oppure quando le norme giuridiche nazionali vigenti non offrono alla persona la possibilità di contattare l'autorità di vigilanza competente o quando tali autorità, per loro stessa natura, non sono idonee allo svolgimento dei compiti loro attribuiti nel progetto di decisione sull'adeguatezza[76]. Tenendo conto che le autorità nazionali di protezione dei dati sono coinvolte nell'applicazione dello scudo e nella vigilanza su tale regime e svolgono un ruolo analogo nell'ambito dell'accordo TFTP2, è più sensato attribuire loro tale compito. Il Gruppo di lavoro sottolinea che, a suo giudizio, è improbabile che le informazioni classificate siano trattate nell'ambito di un procedimento dinanzi al Mediatore, in quanto qualsiasi risposta indicherà soltanto che le leggi sono state rispettate oppure, se non sono state rispettate, che l'inosservanza è stata sanata.

3.5.3.6 Indipendenza

Le dichiarazioni del segretario di Stato indicano chiaramente che le funzioni del Mediatore saranno esercitate da un Sottosegretario del Dipartimento di Stato. Il Mediatore è nominato dal Presidente e confermato dal Senato. Non è necessaria alcuna ulteriore conferma, giacché è sufficiente l'assegnazione dell'incarico. Il Sottosegretario è nominato dal Presidente degli Stati Uniti, investito della funzione di Mediatore dal Segretario di Stato e confermato dal Senato degli Stati Uniti nel ruolo di Sottosegretario. Come evidenziato nella lettera e nelle dichiarazioni contenute nel memorandum, il Mediatore è "indipendente dalla comunità dell'intelligence statunitense". Il Gruppo di lavoro si chiede tuttavia se la figura del Mediatore sia creata in seno al dipartimento più appropriato. Lo svolgimento efficace di tale incarico

[76] Ad esempio in alcuni Stati membri dell'UE i cittadini possono accedere alle informazioni detenute dai servizi di sicurezza nazionale soltanto facendone richiesta a un giudice della Corte suprema.

sembra presupporre una certa conoscenza e comprensione del funzionamento della comunità dell'intelligence; al contempo, però, è evidente che il Mediatore può agire in modo indipendente solo se sufficientemente distante dalla comunità dell'intelligence.

Lo scudo non prevede criteri particolari per la rimozione dall'incarico del Mediatore. Il Gruppo di lavoro presume pertanto che la destituzione possa avvenire con le stesse modalità che regolano la destituzione del Sottosegretario al Dipartimento di Stato; ciò potrebbe compromettere l'indipendenza del Mediatore.

A prima vista la designazione di un Sottosegretario al Dipartimento di Stato come Mediatore è chiaramente diversa, in termini di indipendenza, dall'attribuzione della competenza a un giudice ordinario per i ricorsi presentati dai cittadini. Si tratta dunque di stabilire se il Mediatore possa essere considerato, in termini di indipendenza, alla stregua di altri organi di vigilanza indipendenti che sono risultati conformi. Nel contesto della sorveglianza, tali organi sarebbero, in particolare, l'Investigatory Powers Tribunal (IPT) del Regno Unito e la commissione G10 tedesca.

Tale questione merita un'ulteriore valutazione attraverso l'esame dei poteri conferiti agli organi "indipendenti".

3.5.3.7 Poteri d'indagine

Nella causa Kadi II la Corte di giustizia ha statuito, in relazione all'articolo 47 della Carta, che l'interessato deve poter "conoscere la motivazione della decisione adottata nei suoi confronti, vuoi in base alla lettura della decisione stessa vuoi a seguito di comunicazione della motivazione effettuata su sua istanza, fermo restando il potere del giudice competente di richiedere all'autorità di cui trattasi la comunicazione della motivazione medesima, affinché l'interessato possa difendere i propri diritti nelle migliori condizioni possibili"[77]. I giudici dell'Unione europea devono assicurare che tale decisione si fondi su una base di fatto sufficientemente solida[78]. La Corte stabilisce chiaramente che "non possono essere opposti il segreto o la riservatezza [delle] informazioni o elementi", almeno non dinanzi ai giudici dell'Unione europea[79]. Il Gruppo di lavoro conclude pertanto che, per soddisfare le condizioni poste dalla Corte, debbano essere forniti al Mediatore le informazioni e gli elementi che suffragano i motivi dedotti per giustificare una data misura[80].

Tuttora non è chiaro quale sarà la portata dei poteri d'indagine del Mediatore. Né il progetto di decisione della Commissione né l'allegato III del Dipartimento di Stato sono estremamente chiari a riguardo. Il Gruppo di lavoro presume che il Mediatore debba ricevere informazioni sufficienti per poter stabilire se un'operazione di trattamento di dati da parte dei servizi di sicurezza si svolga nel rispetto della normativa e, in caso contrario, assicurarsi che l'inosservanza sia sanata. Tuttavia né la lettera del Dipartimento di Stato né il progetto di

[77] Kadi II, punto 100.
[78] Kadi II, punto 119.
[79] Kadi II, punto 125.
[80] Kadi II, punto 122, sebbene l'autorità in questione non sia tenuta a produrre tutte le informazioni e gli elementi probatori attinenti ai motivi dedotti per giustificare una data misura.

decisione della Commissione precisano se il Mediatore potrà accedere direttamente ai dati che riguardano l'interessato e dunque svolgere la propria indagine, o se invece potrà basarsi unicamente sulle relazioni trasmesse da altri enti dell'amministrazione statunitense.

3.5.3.8 Poteri correttivi

Dal memorandum risulta poco chiara la modalità con la quale il Mediatore può disporre misure volte a sanare un'inosservanza. Oltre alla mancanza di chiarezza riguardo ai poteri d'indagine, ci si chiede in che misura il Mediatore in quanto tale sarà effettivamente in grado di dare disposizioni affinché le inosservanze siano sanate e che risultato avrebbe l'esercizio di tale potere: un'ipotesi è che i dati ottenuti in maniera non conforme (ovvero illegalmente) non possano più essere utilizzati in nessuna procedura e debbano essere cancellati.

Inoltre il Gruppo di lavoro deduce che lo scudo non preveda la possibilità di ricorso contro la decisione del Mediatore né un riesame della stessa.

Infine per quanto riguarda la risposta trasmessa al reclamante sull'esito del reclamo, il Mediatore non deve rivelare se vi sia stata una condotta illecita da parte della comunità dell'intelligence. La risposta fornita sarà sempre la stessa e sarà generica. Nella causa Kadi II la Corte di giustizia ha statuito che l'autorità competente (in quanto organo di vigilanza) ha un obbligo di motivazione che comprende tutte le circostanze, anche se l'articolo 296 del TFUE non prevede l'obbligo di rispondere in dettaglio[81].

3.5.4 Conclusione

L'esistenza di mezzi di ricorso efficaci per il cittadino rimane fonte di preoccupazione per il Gruppo di lavoro. Innanzitutto il progetto di decisione sull'adeguatezza non chiarisce in quali situazioni e con quali presupposti la persona può proporre ricorso affinché siano stabiliti i suoi diritti.

Il Gruppo di lavoro riconosce e apprezza l'introduzione di un meccanismo di ricorso alternativo attraverso la figura del Mediatore; tale istituto rappresenta uno sviluppo inedito nei rapporti tra l'Unione e i paesi terzi. Sebbene, come osservato sopra, vi sia la necessità di chiarire l'espressione "persone dell'UE", il meccanismo offre all'interessato un'ulteriore possibilità di ricorso contro l'amministrazione statunitense al fine di garantire che i dati personali del richiedente siano trattati conformemente alla legge statunitense.

Al contempo, nel valutare il meccanismo di mediazione alla luce dei criteri che definiscono il giudice indipendente ai sensi dell'articolo 47 della Carta e dei requisiti stabiliti dalla Corte di giustizia dell'Unione europea e dalla Corte europea dei diritti dell'uomo nella propria giurisprudenza in materia di sorveglianza, il Gruppo di lavoro ha rilevato lacune significative. In primo luogo desta preoccupazione la questione se il Mediatore possa essere considerato (formalmente e pienamente) indipendente, soprattutto data la relativa facilità di revoca delle nomine politiche. In secondo luogo, permangono perplessità riguardo al potere del Mediatore

[81] Kadi II, punto 116.

di esercitare un controllo efficace e continuo. Sulla base delle informazioni disponibili nell'allegato III, il Gruppo di lavoro non è in grado di concludere che il Mediatore potrà accedere direttamente, in ogni momento, a tutte le informazioni, agli archivi e ai sistemi informatici necessari per poter compiere la propria valutazione, né che potrà realmente obbligare gli enti di intelligence competenti a porre termine a un eventuale trattamento non conforme dei dati, perlomeno in caso di disaccordo quanto alla conformità o non conformità del trattamento con la normativa. Probabilmente un'ulteriore precisazione della posizione e dei poteri del Mediatore potrà fugare i timori espressi dal Gruppo.

3.6 Osservazioni conclusive sulle garanzie e le limitazioni applicabili alle autorità di sicurezza nazionale degli USA

Il Gruppo di lavoro loda gli sforzi compiuti dalla Commissione e dalle autorità statunitensi per aumentare la trasparenza sull'effetto che i programmi di sorveglianza statunitensi potrebbero avere sui dati trasferiti nell'ambito dello scudo, o di qualunque altro strumento di trasferimento utilizzato a tale scopo. Dalle prime rivelazioni di Snowden del giugno 2013, sono stati realizzati notevoli passi avanti. Nondimeno il Gruppo di lavoro rileva persistenti motivi di preoccupazione. Perlomeno sono necessari chiarimenti e spiegazioni supplementari riguardo a diritti e obblighi contemplati dal regime dello scudo.

Secondo il Gruppo di lavoro destano preoccupazione soprattutto il fatto che la raccolta indiscriminata e in massa di dati non sia totalmente esclusa dalle autorità statunitensi e il fatto che i poteri e la posizione del Mediatore non siano stati definiti in maggior dettaglio. Inoltre il compito di avviare la procedura dinanzi al Mediatore per conto di un cittadino dovrebbe spettare alle autorità nazionali di protezione dei dati e non alle autorità di vigilanza sui servizi di intelligence. Inoltre, sebbene il Gruppo di lavoro riconosca certamente i tentativi compiuti per affrontare le preoccupazioni sollevate dalle autorità di protezione dei dati, sarebbero auspicabili maggiori garanzie, al fine di assicurare che eventuali ingerenze causate dai programmi di sorveglianza statunitensi siano necessarie in una società democratica.

4. VALUTAZIONE DELLE GARANZIE PREVISTE DALLO SCUDO IN ORDINE ALL'ACCESSO AI DATI PER FINALITÀ DI CONTRASTO

4.1 Introduzione

Per quanto riguarda il pubblico accesso ai dati personali per finalità di contrasto, il Gruppo di lavoro rileva che i principi dello scudo di cui all'allegato II contengono una deroga che è identica a quella prevista nei principi dell'approdo sicuro. Il carattere generale della deroga è stato pertanto mantenuto, con il risultato che i nuovi principi dello scudo rendono possibili ingerenze nei diritti fondamentali delle persone i cui dati sono trasferiti dall'Unione verso gli Stati Uniti "fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna degli Stati Uniti"[82].

[82] Schrems, punto 87.

Una delle principali critiche mosse dalla Corte di giustizia alla decisione sull'approdo sicuro nella causa Schrems è tuttavia che essa "non contiene alcuna dichiarazione quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti".

Il Gruppo di lavoro plaude pertanto agli sforzi compiuti dall'amministrazione statunitense nel tentativo di fornire maggiori indicazioni sul quadro giuridico con riguardo all'ingerenza nei dati personali trasferiti nell'ambito dello scudo per finalità di contrasto, comprese le garanzie e limitazioni applicabili. Al contempo esso sottolinea di valutare la questione del pubblico accesso tenendo presente che qualsiasi ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati deve trovare giustificazione in una società democratica. Il Gruppo di lavoro ha dunque esaminato le garanzie fornite dallo scudo in relazione all'accesso a fini di contrasto, utilizzando il quadro delineato al punto 1.2 del presente parere.

4.2 Applicazione delle garanzie essenziali europee all'accesso delle autorità di contrasto ai dati detenuti da imprese

4.2.1 L'accesso delle autorità di contrasto ai dati personali dovrebbe avvenire nel rispetto della legge ed essere basato su regole chiare, precise e accessibili

L'allegato VII dello scudo contiene una lettera del Dipartimento della Giustizia degli Stati Uniti nella quale è fornita "una breve panoramica dei principali strumenti investigativi usati negli USA per ottenere dalle imprese dati commerciali e altre informazioni a fini di applicazione della normativa penale o per scopi (civili e regolamentari) d'interesse pubblico, corredata delle limitazioni di accesso che si applicano ai relativi poteri".

Tutte le procedure menzionate all'allegato VII discendono direttamente dalla Costituzione degli Stati Uniti (quarto emendamento), dalla legislazione e dal diritto processuale oppure dagli orientamenti e dalle politiche del Dipartimento della Giustizia. Tuttavia l'allegato VII non richiama specificamente tutte le leggi che contemplano tali procedure, bensì si concentra su una breve descrizione delle procedure stesse. L'allegato VII indica inoltre che "[s]econdo il settore specifico in cui opera e la tipologia di dati che detiene, l'impresa può addurre altre basi giuridiche per contestare la richiesta di dati presentata dall'ente amministrativo" e offre vari esempi non esaustivi quali la legge sul segreto bancario, la legge sull'informativa corretta nel credito e la legge sul diritto alla privacy finanziaria.

Il Gruppo di lavoro rileva che il quadro delle leggi, procedure e politiche è frammentato e che la base giuridica applicabile a una determinata domanda di accesso dipenderà dalla natura dei dati richiesti, dal tipo di impresa, dalla natura delle procedure giuridiche (penale, amministrativa, relativa ad altro interesse pubblico) e dal tipo di ente che chiede l'accesso.

Poiché tutte le norme applicabili che limitano l'accesso delle autorità di contrasto ai dati trasferiti nell'ambito dello scudo si basano sulla Costituzione, sulla legge e su politiche trasparenti del Dipartimento della Giustizia, il Gruppo di lavoro tiene conto di una

presunzione di accessibilità di tali norme. Tuttavia la chiarezza e la precisione delle norme possono essere valutate soltanto in ogni singolo tipo di procedura e di richiesta di accesso. Pertanto il Gruppo di lavoro constata con rammarico che, in base alle indicazioni fornite nell'allegato VII dello scudo e alle constatazioni contenute nel progetto di decisione, questo tipo di valutazione non è al momento fattibile.

4.2.2 Occorre dimostrare la necessità e la proporzionalità rispetto agli obiettivi legittimi perseguiti

Il Gruppo di lavoro rileva che la richiesta di accesso ai dati per finalità di contrasto può essere considerata una richiesta che persegue un obiettivo legittimo. Ad esempio l'articolo 8, paragrafo 2, della CEDU ammette l'ingerenza di un'autorità pubblica nel diritto alla protezione della vita privata se "necessaria […] alla pubblica sicurezza, […] alla difesa dell'ordine e alla prevenzione dei reati". Tuttavia tali ingerenze sono accettabili solo se necessarie e proporzionate[83].

Secondo una costante giurisprudenza della Corte di giustizia, il principio di proporzionalità esige che le misure legislative che propongono ingerenze nei diritti al rispetto della vita privata e alla protezione dei dati personali siano idonee "a realizzare gli obiettivi legittimi perseguiti *dalla normativa di cui trattasi* e non superino i limiti di ciò che è idoneo e necessario al conseguimento degli obiettivi stessi"[84] (corsivo nostro). Pertanto la valutazione della necessità e proporzionalità è sempre effettuata in relazione a una misura specifica contemplata dalla legislazione.

Nell'allegato VII le autorità statunitensi precisano che i procuratori federali e gli inquirenti federali hanno facoltà di accesso ai documenti e ad altre informazioni detenute dalle organizzazioni attivando "varie procedure giuridiche obbligatorie, tra cui citazioni dinanzi al *grand jury*, citazioni amministrative e mandati di perquisizione" e possono acquisire altre comunicazioni "in virtù dei poteri di intercettazione delle comunicazioni e dei dati informativi conferiti per le indagini penali federali"[85]. Inoltre gli enti che hanno competenze civili o di regolamentazione possono citare le organizzazioni ingiungendo loro di trasmettere "documenti aziendali, informazioni conservate su supporto elettronico o altri beni materiali"[86]. L'allegato VII precisa inoltre che tali procedure giuridiche sono seguite in generale per ottenere informazioni dalle "imprese" presenti negli USA, indipendentemente dal fatto che siano certificate o meno nell'ambito dello scudo, e "a prescindere dalla cittadinanza dell'interessato". In altri termini, sembra che a beneficiare di tali tutele siano le organizzazioni e non le persone stesse.

Oltre all'allegato VII, il progetto di decisione, che si basa sui principi dello scudo, contiene alcune constatazioni della Commissione relative all'esistenza, negli Stati Uniti, di norme volte

[83] Cfr. il documento di lavoro relativo alle garanzie essenziali europee, pagg. da 7 a 9. Per la valutazione generale dei concetti di necessità e proporzionalità, cfr. il "Parere 01/2014 sull'applicazione dei principi di necessità e proporzionalità nell'azione di contrasto" del 27 febbraio 2014.
[84] Digital Rights Ireland, punto 46 e la giurisprudenza citata in tale sentenza.
[85] Allegato VII, pag. 2.
[86] Allegato VII, pag. 4.

a limitare le ingerenze nei diritti fondamentali delle persone i cui dati sono trasferiti dall'Unione verso gli Stati Uniti nell'ambito dello scudo.

In particolare le constatazioni del progetto di decisione riguardano le limitazioni e garanzie applicabili a titolo del quarto emendamento della Costituzione degli Stati Uniti, il quale dispone che le autorità di contrasto possano, in via di principio, procedere a perquisizioni e sequestri soltanto con un mandato del giudice ottenuto dimostrando una fondata supposizione[87]. Le constatazioni si riferiscono inoltre al fatto che nei casi eccezionali in cui il mandato non è necessario, l'applicazione della legge è subordinata a una prova di ragionevolezza[88].

Le constatazioni, tuttavia, non chiariscono in che modo tali garanzie si applichino ai cittadini stranieri. In effetti in un considerando del progetto di decisione si riconosce che la tutela contemplata dal quarto emendamento non è estesa ai "cittadini stranieri che non sono residenti negli Stati Uniti"[89]. Negli stessi paragrafi del progetto di decisione è inoltre stabilito che i cittadini stranieri godono indirettamente delle tutele garantite alle imprese statunitensi che detengono i dati personali e che sono destinatarie delle domande delle autorità di contrasto. Il Gruppo di lavoro, tuttavia, constata con rammarico che tale conclusione non fa riferimento ad una fonte di diritto (giurisprudenza o diritto positivo).

Complessivamente il Gruppo di lavoro rileva che il sistema di strumenti investigativi usati per ottenere dati commerciali e altre informazioni dalle imprese presenti negli Stati Uniti a fini di applicazione della normativa penale o per scopi d'interesse pubblico, comprese le limitazioni e le garanzie relative all'accesso, rappresenta un insieme di misure complesso. Sulla base delle informazioni disponibili, al momento non è possibile valutare tale sistema in generale. Per poter valutare realmente la necessità e proporzionalità delle misure d'indagine a fini di contrasto in rapporto ai diritti fondamentali al rispetto della vita privata e alla protezione dei dati è necessaria una valutazione specifica dei singoli casi.

4.2.3 Dovrebbe esistere un meccanismo di vigilanza indipendente

Il Gruppo di lavoro prende debita nota del fatto che la maggioranza delle procedure descritte nell'allegato VII presuppone che un giudice emetta una decisione prima che le autorità siano autorizzate ad accedere ai dati (ad esempio provvedimenti giudiziari relativi ai dispositivi d'intercettazione dei dati informativi della comunicazione in entrata e in uscita, ordini giudiziari che dispongono la sorveglianza a norma della legge federale sulle intercettazioni, mandati di perquisizione — articolo 41). Tuttavia sembra che non tutte le procedure richiedano il previo intervento di un giudice. Ad esempio gli enti che hanno competenze civili o di regolamentazione "possono citare"[90] le imprese. In questi casi esiste la possibilità di un

[87] Progetto di decisione sull'adeguatezza, considerando 107.
[88] Scudo, considerando 107.
[89] Progetto di decisione sull'adeguatezza, considerando 108.
[90] Allegato VII, pag. 4.

controllo giurisdizionale ex post sulla ragionevolezza della citazione, giacché "[i]l destinatario della citazione amministrativa può contestarne l'esecuzione in sede giudiziaria"[91].

Sulla base delle informazioni disponibili, il Gruppo di lavoro rileva che, riguardo all'accesso delle autorità di contrasto ai dati detenuti da imprese presenti negli Stati Uniti, sembra esistere un meccanismo di vigilanza indipendente piuttosto solido.

4.2.4 La persona deve poter disporre di mezzi di ricorso efficaci

Come ricordato sopra, la protezione offerta dal quarto emendamento non contempla "i cittadini stranieri che non sono residenti negli Stati Uniti"[92]. Ciò significa che un cittadino straniero non avrebbe facoltà di contestare un mandato o una citazione dinanzi a un giudice invocando il quarto emendamento. Il progetto di decisione sull'adeguatezza precisa che i cittadini stranieri godono indirettamente delle tutele garantite alle imprese statunitensi che detengono i dati personali e che sono destinatarie di domande di accesso a fini di contrasto. Il Gruppo di lavoro constata tuttavia che, anche qualora tale protezione fosse effettiva, essa non significa che i cittadini dispongano di mezzi di ricorso efficaci, giacché in questo scenario il titolare del diritto a un ricorso effettivo sembra essere l'impresa che riceve la richiesta di accesso ai dati e non la persona i cui dati formano oggetto della domanda.

L'allegato VII non fornisce ulteriori indicazioni riguardo alle possibilità di ricorso offerte dal diritto positivo ai cittadini stranieri quando le autorità o le imprese forniscono ovvero ottengono illecitamente l'accesso al contenuto dei dati che li riguardano.

Il Gruppo di lavoro si compiace del fatto che la legge sul ricorso giurisdizionale (Judicial Redress Act)[93] di recente adozione conferisca ai cittadini stranieri il diritto di ricorso giudiziario. Tuttavia tale diritto può essere esercitato soltanto se esistono precisi motivi per adire le vie legali, ovvero per ottenere la rettifica dei dati e l'accesso agli stessi nonché il rimborso delle spese legali qualora un ente o servizio federale rifiuti di modificare i dati o neghi l'accesso agli stessi e per ottenere riparazioni in sede civile in caso di divulgazione intenzionale o volontaria dei dati.

Inoltre la giurisprudenza statunitense citata nelle note in calce dei considerando pertinenti del progetto di decisione, in particolare le sentenze nelle cause City of Ontario contro Quon[94], Maryland contro King[95] e Samson contro California[96], non è pertinente per valutare se un cittadino straniero possa promuovere un'azione in giudizio al fine di contestare la liceità di un'ingerenza nella propria sfera privata[97]. Tutte queste cause si riferiscono al diritto al rispetto

[91] Allegato VII, pag. 4.
[92] Progetto di decisione sull'adeguatezza, considerando 108.
[93] Judicial Redress Act del 2015, H.R. 1428.
[94] *City of Ontario, Cal./Quon*, 130 S. Ct. 2619, 2630 (2010).
[95] *Maryland/ King*, 133 S. Ct. 1958, 1970 (2013).
[96] *Samson/California*, 547 U.S. 843, 848 (2006).
[97] Nella causa *Ontario/Quon*, il giudice ha statuito che la Città di Ontario non aveva violato i diritti dei suoi dipendenti, quali garantiti dal quarto emendamento, perché l'accesso dell'amministrazione pubblica al contenuto dei messaggi privati del dipendente in questione era ragionevole, in quanto motivato da una finalità occupazionale legittima e non era di portata eccessiva. Nella causa *Samson/California*, il giudice ha concluso che il quarto emendamento non osta a che un funzionario di polizia conduca una perquisizione senza sospetto ("suspicionless search") su una persona rilasciata sulla parola. Nella causa

della vita privata di cittadini statunitensi e tutte le relative decisioni della Corte suprema degli Stati Uniti limitano, di fatto, l'applicazione del quarto emendamento.

Nel complesso il Gruppo di lavoro riconosce e accoglie con favore l'adozione del Judicial Redress Act, ma continua a nutrire dubbi circa l'effettiva esistenza di mezzi di ricorso efficaci di cui il singolo interessato possa avvalersi.

4.3 Osservazioni conclusive

Il Gruppo di lavoro riconosce e apprezza gli sforzi profusi dall'amministrazione statunitense per fornire maggiori indicazioni sul quadro giuridico in relazione all'ingerenza nei dati personali trasferiti nell'ambito dello scudo UE-USA per la privacy a fini di contrasto, comprese le limitazioni e garanzie applicabili.

Il Gruppo di lavoro rileva che il sistema di strumenti investigativi a disposizione delle autorità di contrasto, comprese le limitazioni e garanzie applicabili, è vasto e complesso e che le informazioni fornite nei documenti dello scudo sono succinte. Il Gruppo di lavoro, pertanto, si rammarica di non potere fornire in questo momento, sulla base delle informazioni limitate (ovvero l'allegato VII dello scudo e le constatazioni contenute nel progetto di decisione), una valutazione globale per quanto riguarda l'accessibilità, prevedibilità, necessità e proporzionalità delle norme applicabili. Ferme restando le altre constatazioni formulate dal Gruppo di lavoro in relazione allo scudo nel presente parere, una siffatta valutazione potrebbe essere ricompresa nel riesame annuale dello scudo.

Quanto all'accesso da parte delle autorità di contrasto, il Gruppo di lavoro rileva che il meccanismo di vigilanza indipendente posto in essere sembra piuttosto solido. Inoltre il Gruppo di lavoro plaude all'adozione del Judicial Redress Act, che conferisce diritti di ricorso per via giudiziaria ai cittadini stranieri ma rileva che tali diritti sono di natura limitata. Oltre a constatare che un cittadino straniero non sarebbe in grado di contestare dinanzi a un giudice mandati o citazioni invocando il quarto emendamento, il Gruppo di lavoro continua a nutrire dubbi circa l'effettiva esistenza di mezzi di ricorso efficaci di cui il singolo interessato possa avvalersi nel settore delle attività di contrasto.

5. CONCLUSIONI E RACCOMANDAZIONI

In primo luogo il Gruppo di lavoro constata con soddisfazione che a cinque mesi di distanza dall'invalidazione della decisione sull'approdo sicuro sia stato presentato un nuovo progetto di decisione sull'adeguatezza che introduce molti miglioramenti rispetto al meccanismo precedente. Il Gruppo di lavoro apprezza in particolare la maggiore trasparenza offerta con l'inserimento di due elenchi sul sito web del Dipartimento del Commercio, che contengono rispettivamente i dati delle organizzazioni aderenti allo scudo e i dati delle organizzazioni che non aderiscono più allo scudo. Si apprezza altresì la maggiore trasparenza in relazione

---

Maryland/King il giudice ha ritenuto che quando le autorità procedono a un arresto sulla base di un motivo plausibile per trattenere la persona sospettata di un reato grave e conducono la stessa alla stazione di polizia affinché sia posta in stato di custodia, il prelievo e l'analisi di un campione di DNA salivare della persona in stato di arresto costituisce, al pari dei rilievi fotografici e dattiloscopici, una procedura di schedatura legittima che è ragionevole ai sensi del quarto emendamento.

all'accesso delle autorità pubbliche ai dati trasferiti nell'ambito dello scudo per fini di sicurezza nazionale o di contrasto. Infine il Gruppo di lavoro apprende con viva soddisfazione che tutti i trasferimenti di dati verso gli Stati Uniti beneficeranno d'ora in poi della medesima tutela: non vi sono norme specifiche che privilegino uno strumento piuttosto che un altro.

5.1 Tre motivi di preoccupazione

Permangono tuttavia tre motivi di preoccupazione principali che il Gruppo di lavoro ritiene debbano essere affrontati.

In primo luogo il testo del progetto di decisione sull'adeguatezza, così come formulato, non obbliga le organizzazioni a cancellare i dati che non sono più necessari. Un elemento essenziale della normativa dell'Unione sulla protezione dei dati è garantire che i dati siano conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono stati raccolti. In secondo luogo il Gruppo di lavoro desume dall'allegato VI che l'amministrazione statunitense non escluda completamente di proseguire le attività di raccolta indiscriminata e in massa di dati. Il Gruppo di lavoro ha costantemente sostenuto che una siffatta raccolta di dati costituisce un'ingerenza ingiustificata nei diritti fondamentali della persona. Il terzo motivo di preoccupazione riguarda l'introduzione della figura del mediatore. Sebbene il Gruppo di lavoro apprezzi questa iniziativa senza precedenti che mette a disposizione dei cittadini un ulteriore meccanismo di ricorso e di vigilanza, non è certo che il mediatore disponga di poteri sufficienti a garantire l'espletamento efficace delle funzioni attribuitegli. Perlomeno è necessario chiarire quali siano i poteri e la posizione del mediatore, al fine di dimostrare che tale figura è realmente indipendente e può offrire un mezzo di ricorso effettivo in caso di non conformità del trattamento dei dati.

5.2 Chiarimenti raccomandati

Oltre agli aspetti sopra ricordati, il Gruppo di lavoro ha indicato, nel presente parere, vari elementi che sarebbe opportuno fossero chiariti nella decisione sull'adeguatezza. In particolare è necessario garantire una definizione e applicazione coerenti dei principali concetti dello scudo che attengono alla protezione dei dati. Attualmente ciò non avviene. Sarebbe auspicabile l'introduzione di un glossario di termini nelle F.A.Q. dello scudo, contenente definizioni idealmente concordate tra l'Unione e gli Stati Uniti. Il Gruppo di lavoro conclude inoltre che l'ulteriore trasferimento di dati personali dall'UE è definito in maniera insufficiente, soprattutto per quanto riguarda il suo ambito di applicazione, la limitazione della sua finalità e le tutele applicabili ai trasferimenti verso i procuratori. Quanto all'accesso ai dati nell'ambito dello scudo da parte delle autorità di contrasto, desta preoccupazione soprattutto l'aspetto della prevedibilità del diritto, data la natura vasta e complessa del sistema repressivo statunitense sia livello federale sia a livello statale e date le scarse indicazioni fornite nella decisione sull'adeguatezza.

La decisione sullo scudo è la prima decisione sull'adeguatezza elaborata dopo che è stato raggiunto un accordo di massima sul testo del regolamento generale sulla protezione dei dati. Tuttavia molti dei miglioramenti riguardanti il livello di protezione dei dati offerto alle

persone non si riflettono nello scudo. Il Gruppo di lavoro raccomanda pertanto che la decisione sull'adeguatezza e le decisioni sull'adeguatezza adottate per altri paesi terzi siano sottoposte a riesame subito dopo l'entrata in applicazione del regolamento generale sulla protezione dei dati.

Il Gruppo di lavoro richiama infine l'attenzione su un'ultima raccomandazione che riguarda il riesame comune. Il Gruppo di lavoro constata con soddisfazione che la decisione sull'adeguatezza dello scudo sarà effettivamente riesaminata a cadenza annuale, con un ampio coinvolgimento delle autorità di protezione dei dati e di altre parti interessate. Il Gruppo di lavoro auspica che tutte le parti raggiungano un'intesa sugli elementi di tale riesame comune, comprese la stesura e la presentazione della relazione sulle risultanze, con largo anticipo rispetto alla data del primo riesame.