COMMISSIONE
EUROPEA

Bruxelles, 27.11.2013
COM(2013) 847 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite

1. INTRODUZIONE

La direttiva 95/46/CE, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (in appresso: "direttiva sulla protezione dei dati") stabilisce le regole per il trasferimento dei dati personali dagli Stati membri dell'UE ad altri paesi al di fuori dell'UE[1], nella misura in cui tali trasferimenti rientrino nel campo d'applicazione di tale strumento[2].

Ai sensi della direttiva, la Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato in considerazione della sua legislazione nazionale o degli impegni internazionali che ha stipulato per proteggere i diritti delle persone: in questo caso non sarebbero d'applicazione le specifiche restrizioni al trasferimento di dati verso tale paese. Queste decisioni sono comunemente denominate "**decisioni sull'adeguatezza**".

Il 26 luglio 2000, la Commissione ha adottato la decisione 520/2000/CE[3] (in appresso la "**decisione Approdo sicuro**") che riconosce che i principi di Approdo sicuro e le Domande più frequenti (rispettivamente: "i principi" e "le FAQ"), pubblicate dal Dipartimento del Commercio degli Stati Uniti, offrono una protezione adeguata ai fini del trasferimento dei dati personali dall'UE. La decisione Approdo sicuro è stata adottata a seguito di un parere del Gruppo di lavoro "Articolo 29" e di un parere del Comitato "Articolo 31" formulato a maggioranza qualificata degli Stati membri. Conformemente alla decisione 1999/468 del Consiglio, la decisione Approdo sicuro è stata sottoposta all'esame preliminare del Parlamento europeo.

Il risultato è che l'attuale decisione Approdo sicuro consente il libero trasferimento[4] di informazioni personali dagli Stati membri dell'UE[5] a imprese negli Stati Uniti che abbiano aderito ai principi in casi in cui altrimenti – date le sostanziali differenze nei regimi di privacy fra le due sponde dell'Atlantico – il trasferimento non sarebbe conforme alle norme UE sull'adeguato livello di protezione dei dati.

Il funzionamento dell'attuale accordo sull'Approdo sicuro si basa sugli impegni assunti dalle imprese che vi aderiscono e sulla loro auto-certificazione. L'adesione è volontaria, ma una volta sottoscritta le norme sono vincolanti. I principi fondamentali dell'accordo sono i seguenti:

---

1 L'articolo 25 e l'articolo 26 della direttiva sulla protezione dei dati stabiliscono il quadro giuridico per il trasferimento dei dati personali dall'UE a paesi terzi al di fuori del SEE.

2 Norme supplementari figurano all'articolo 13 della decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, nella misura in cui tali trasferimenti riguardino dati personali trasmessi o resi disponibili da uno Stato membro a un altro Stato membro che successivamente intende trasferirli a un paese terzo o a un organismo internazionale ai fini della prevenzione, dell'indagine, dell'accertamento o del perseguimento dei reati o dell'esecuzione delle sanzioni penali.

3 Decisione 520/2000/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di Approdo sicuro e dalle relative "Domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal Dipartimento del Commercio degli Stati Uniti (GU L 215 del 25.8.2000, pag. 7).

4 Quanto sopra non esclude l'applicazione, al trattamento dei dati, di altre condizioni che possono esistere ai sensi della legislazione nazionale d'attuazione della direttiva UE sulla protezione dei dati.

5 I trasferimenti di dati dai tre Stati del SEE sono parimenti interessati a seguito dell'estensione della direttiva 95/46/CE all'accordo SEE, decisione 83/1999 del 25 giugno 1999 (GU L 296 del 23.11.2000, pag. 41).

a) trasparenza delle politiche di tutela della sfera privata delle imprese che aderiscono;

b) incorporazione dei principi dell'Approdo sicuro in tali politiche, e

c) applicazione, anche da parte delle pubbliche autorità.

Questi fondamenti dell'Approdo sicuro devono essere rivisti dato il **nuovo contesto** caratterizzato dagli elementi seguenti:

a) l'aumento esponenziale di flussi di dati una volta accessori, ma adesso al centro della rapida crescita dell'economia digitale e dei considerevoli sviluppi in materia di raccolta, trattamento e uso delle informazioni;

b) l'importanza fondamentale dei flussi di dati specialmente per l'economia transatlantica[6];

c) la rapida crescita del numero di imprese statunitensi aderenti al regime Approdo sicuro, che si è ottuplicato dal 2004 (da 400 imprese nel 2004 a 3 246 nel 2013);

d) le informazioni recentemente diffuse sui programmi di controllo americani, che sollevano nuove questioni sul livello di protezione che si ritiene debba offrire l'accordo sull'Approdo sicuro.

In tale contesto, la presente comunicazione fa il punto sul funzionamento del regime dell'Approdo sicuro. Essa si **basa su elementi di prova** raccolti dalla Commissione, sui lavori svolti nel 2009 dal Gruppo di contatto UE-Stati Uniti sulla vita privata, su uno studio preparato da un contraente indipendente nel 2008[7] e sulle informazioni ricevute nell'ambito del Gruppo di lavoro ad hoc UE-USA, istituito dopo le rivelazioni sui programmi di controllo americani (*si veda un documento parallelo)*. La presente comunicazione fa seguito alle due **relazioni di valutazione della Commissione**, presentate rispettivamente nel 2002[8] e nel 2004[9], nella fase iniziale dell'accordo sull'Approdo sicuro.

2. STRUTTURA E FUNZIONAMENTO DEL REGIME APPRODO SICURO

2.1. Struttura del regime Approdo sicuro

Un'impresa americana che intenda aderire al regime Approdo sicuro deve a) stipulare, nella sua politica pubblica di tutela della sfera privata, che aderisce ai principi in questione e vi si conforma effettivamente, e b) auto-certificarsi, cioè dichiarare al Dipartimento del Commercio degli Stati Uniti che osserva tali principi. L'auto-certificazione deve essere ripresentata ogni anno. I principi di Approdo sicuro in materia di riservatezza, figuranti all'allegato I della decisione Approdo sicuro, includono condizioni sia sulla protezione materiale dei dati personali (principi riguardanti l'integrità dei dati, la sicurezza, la scelta e i trasferimenti successivi) che sui diritti procedurali degli interessati (principi riguardanti la notifica, l'accesso e le garanzie d'applicazione).

---

6 Secondo certi studi, se i servizi e i flussi di dati transfrontalieri dovessero subire perturbazioni a seguito delle soppressione di norme vincolanti d'impresa, di clausole contrattuali tipo e del regime di Approdo sicuro, l'impatto negativo sul PIL dell'UE potrebbe essere compreso fra -0,8% e -1,3%, e le esportazioni di servizi dall'UE agli USA calerebbero al -6,7% a causa della perdita di competitività. Si veda: "The Economic Importance of Getting Data Protection Right", studio del Centro europeo per la politica economica internazionale per la Camera di Commercio statunitense, marzo 2013.

7 Studio di valutazione d'impatto preparato nel 2008 per la Commissione europea dal *Centre de Recherche Informatique et Droit* ("CRID") dell'Università di Namur.

8 Documento di lavoro dei servizi della Commissione sull'applicazione della decisione 520/2000/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal Dipartimento del Commercio degli Stati Uniti (SEC (2002) 196, 13.12.2002).

9 Documento di lavoro dei servizi della Commissione sull'attuazione della decisione 520/2000/CE della Commissione sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal Dipartimento del Commercio degli Stati Uniti (SEC (2004) 1323, 20.10.2004).

Per quanto attiene all'applicazione del regime Approdo sicuro negli Stati Uniti, il ruolo principale spetta a due istituzioni americane: il Dipartimento del Commercio e la Commissione federale per il Commercio.

Il **Dipartimento del Commercio** esamina tutte le auto-certificazioni Approdo sicuro e tutti i relativi rinnovi annuali presentati dalle imprese per verificare che contengano tutti gli elementi richiesti per essere membro[10]. Aggiorna l'elenco delle imprese che hanno presentato una lettera di auto-certificazione e pubblica l'elenco e le lettere sul suo sito web. Controlla inoltre il funzionamento del regime Approdo sicuro ed elimina dall'elenco le imprese che non ne rispettano i principi.

La **Commissione federale per il Commercio (FTC)**, nell'ambito delle sue competenze in materia di protezione dei consumatori, interviene contro le pratiche sleali o ingannevoli ai sensi della sezione 5 del Free Trade Commission Act. Nell'ambito dei suoi interventi d'applicazione, la Commissione federale per il Commercio indaga sulle false dichiarazioni di adesione ad Approdo sicuro e sulla non osservanza dei principi da parte di imprese che ne sono membri. Negli specifici casi di applicazione dei principi di Approdo sicuro nei confronti di vettori aerei, l'organismo competente è il Dipartimento USA dei Trasporti[11].

L'attuale decisione Approdo sicuro fa parte del diritto dell'UE che deve essere applicato dalle autorità degli Stati membri. Ai sensi della decisione, le **autorità per la protezione dei dati** (APT) degli Stati membri dell'UE hanno la facoltà, in specifici casi, di sospendere i trasferimenti di dati verso imprese certificate nell'ambito di Approdo sicuro[12]. La Commissione non è a conoscenza di casi di sospensione disposti da un'autorità nazionale per la protezione dei dati da quando è stato istituito, nel 2000, il regime Approdo sicuro. Indipendentemente dai poteri loro conferiti dalla decisione Approdo sicuro, le autorità di protezione dei dati degli Stati membri dell'UE sono competenti a intervenire, anche in caso di trasferimenti internazionali, per garantire l'osservanza dei principi generali di tutela dei dati sanciti dalla direttiva del 1995 sulla protezione dei dati.

Come ricorda l'attuale decisione Approdo sicuro, **spetta alla Commissione** – agendo secondo la procedura d'esame di cui al regolamento n. 182/2011 – adattare la decisione stessa, sospenderla o limitarne il campo d'applicazione in qualsiasi momento, alla luce dell'esperienza acquisita nella sua attuazione. Ciò è previsto in particolare in caso di sistematica inosservanza da parte americana, ad esempio se un organismo incaricato di garantire il rispetto dei principi Approdo sicuro negli Stati Uniti non svolge efficacemente il suo ruolo, o se le condizioni imposte dalla legislazione americana prevalgono su tali principi e sul livello di protezione da essi offerto. Come avviene per ogni altra decisione della Commissione, la decisione in oggetto può essere modificata pure per altri motivi o addirittura annullata.

---

[10] Se la certificazione di un'impresa, o il rinnovo, non soddisfano le condizioni dell'Approdo sicuro, il Dipartimento del Commercio lo notifica all'impresa interessata indicando i provvedimenti da prendere (ad es. chiarimenti o modifiche nella descrizione della politica) per poter ultimare la procedura.

[11] Ai sensi del Titolo 49 dell' US Code, sezione 41712.

[12] Più precisamente, la sospensione dei trasferimenti può essere disposta in due situazioni, cioè quando:
a) gli enti governativi negli USA abbiano accertato che l'impresa viola i principi dell'Approdo sicuro in materia di riservatezza, oppure
b) sia molto probabile che i principi dell'Approdo sicuro in materia di riservatezza vengano violati; vi siano ragionevoli motivi per ritenere che l'organismo di esecuzione competente non stia adottando o non adotterà misure adeguate e tempestive per risolvere un caso concreto, la continuazione del trasferimento dei dati potrebbe determinare un rischio imminente di gravi danni per gli interessati e le autorità competenti dello Stato membro abbiano fatto il possibile, date le circostanze, per informare l'impresa dandole l'opportunità di replicare.

2.2. Funzionamento del regime Approdo sicuro

Le **3 246**[13] **società certificate** includono imprese sia di piccole che di grosse dimensioni[14]. I settori dei servizi finanziari e delle telecomunicazioni non rientrano nei poteri d'applicazione della Commissione federale per il Commercio e sono quindi esclusi dal regime Approdo sicuro, ma molti altri settori dell'industria e dei servizi sono invece rappresentati dalle imprese certificate – che contano note imprese del settore di Internet, settori che vanno dai servizi di informazione ed informatici ai prodotti farmaceutici, ai servizi di viaggio e turistici e a quelli sanitari o delle carte di credito[15]. Si tratta principalmente di imprese statunitensi che forniscono servizi sul mercato interno dell'UE, ma vi sono anche controllate di alcune società dell'UE come Nokia o Bayer. Per il 51% sono società che trattano dati relativi ai dipendenti in Europa e li inviano negli Stati Uniti a fini di gestione delle risorse umane[16].

Alcune APT dell'UE hanno espresso **crescente preoccupazione** in merito ai trasferimenti di dati effettuati nell'ambito dell'attuale regime di Approdo sicuro. Alcune APT degli Stati membri hanno criticato la formulazione molto generale dei principi e il fatto che l'attuale regime si basa in modo considerevole sull'auto-certificazione e sull'auto-regolamentazione. Preoccupazioni analoghe sono state sollevate dall'industria, che ha evidenziato distorsioni della concorrenza causate da carenze a livello d'applicazione.

L'attuale accordo Approdo sicuro si basa sull'adesione volontaria delle imprese, sulla loro auto-certificazione e sul controllo, da parte delle autorità pubbliche, dell'attuazione degli impegni assunti con l'auto-certificazione. In tale contesto, la minima mancanza di trasparenza e qualsiasi carenza a livello di applicazione minano le fondamenta su cui è costruito questo meccanismo.

Ogni insufficienza a livello di trasparenza o di applicazione da parte americana ha l'effetto di far ricadere la responsabilità sulle autorità per la protezione dei dati europee e sulle imprese che si avvalgono del regime in oggetto. Il 29 aprile 2010 l'APT tedesca ha emanato una decisione con cui hanno chiesto alle imprese che trasferiscono dati dall'Europa agli USA di controllare attivamente che le imprese importatrici dei dati osservino effettivamente i principi d'Approdo sicuro in materia di riservatezza, e in cui raccomandano che "almeno l'impresa esportatrice debba determinare se la certificazione Approdo sicuro dell'importatore è sempre valida"[17].

Il 24 luglio 2013, a seguito delle rivelazioni sui programmi di controllo americani, l'APT tedesca si è spinta ancora più in là esprimendo la preoccupazione che "sia molto probabile che i principi enunciati nelle decisioni della Commissione vengano violati"[18]. Alcune APT (ad es. quella di Brema) hanno chiesto a un'impresa che trasferisce dati personali a provider

---

13 Al 26 settembre 2013, il numero di organizzazioni indicate nell'elenco Approdo sicuro come **"Attuali"** era **3 246**, il numero di organizzazioni indicate come **"Non attuali"** era **935.**

14 Le organizzazioni Approdo sicuro che contano fino a 250 dipendenti sono il 60**%** (1 925 su 3 246). Le organizzazioni Approdo sicuro dai 251 dipendenti in su sono il **40%** (1 295 su 3 246).

15 MasterCard, ad esempio, lavora con migliaia di banche, ed è un chiaro esempio di un caso in cui, ai fini del trasferimento dei dati personali, l'Approdo sicuro non può essere sostituito da altri strumenti giuridici come norme vincolanti di impresa o disposizioni contrattuali.

16 Organizzazioni Approdo sicuro che trattano dati relativi alle risorse umane in virtù della loro certificazione (e che hanno quindi stipulato di conformarsi alle norme e di cooperare con le APT europee): **51%** (1 671 su 3 246).

17 Si veda la decisione del Düsseldorfer Kreis del 28/29 aprile 2010. Cfr. Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile. Tuttavia, il 7 ottobre 2013, in occasione dell'indagine della commissione LIBE del Parlamento europeo, il garante europeo della protezione dei dati (GEPD) Peter Hustinx ha dichiarato, in merito al regime Approdo sicuro, che: "sono stati compiuti sostanziali miglioramenti e che le maggior parte delle questioni sono state risolte": https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf.

18 Si veda la risoluzione della conferenza tedesca dei Commissari per la protezione dei dati, che suggerisce che i servizi di intelligence costituiscano una grossa minaccia per il traffico di dati fra la Germania e i paesi al di fuori dell'Europa: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870.

statunitensi di comunicare loro se e come tali provider impediscono l'accesso ai dati all'Agenzia nazionale per la sicurezza. La APT irlandese ha riferito di aver recentemente ricevuto due denunce riguardanti il regime Approdo sicuro a seguito della divulgazione di notizie sui programmi delle agenzie di intelligence americane, ma che si è rifiutata di indagare per il fatto che il trasferimento di dati personali verso il paese terzo rispettava le condizioni della legislazione irlandese sulla protezione dei dati. A seguito di una denuncia analoga, l'APT lussemburghese ha accertato che il trasferimento di dati da parte di Microsoft e Skype verso gli USA è stato conforme alla legge lussemburghese sulla protezione dei dati[19]. L'Alta Corte irlandese, invece, ha in seguito accolto un'istanza di controllo giurisdizionale in virtù della quale esaminerà l'inazione del Commissario irlandese per la protezione dei dati in relazione ai programmi americani di controllo. Una delle due denunce era stata presentata dal gruppo di studenti "Europe versus Facebook" (EvF), che ha anche depositato un reclamo analogo contro Yahoo in Germania, attualmente esaminato dalle competenti autorità per la protezione dei dati.

Queste reazioni divergenti alle rivelazioni sui programmi americani di controllo da parte delle autorità per la protezione dei dati mostrano il reale rischio di frammentazione del regime di Approdo sicuro, e sollevano questioni sulla portata della sua applicazione

3. TRASPARENZA DELLE POLITICHE DI TUTELA DELLA SFERA PRIVATA DELLE IMPRESE CHE ADERISCONO AD APPRODO SICURO

Secondo la FAQ 6 dell'allegato II della decisione Approdo sicuro, le imprese interessate alla certificazione devono fornire al Dipartimento del Commercio, e devono rendere pubblica, la politica da esse perseguita in tema di tutela della sfera privata. Essa deve includere l'impegno ad attenersi ai principi di riservatezza. La condizione di **rendere pubbliche le politiche di tutela della sfera privata** delle imprese auto-certificate, e la dichiarazione di aderire ai principi di riservatezza, sono elementi fondamentali per il funzionamento del regime.

Un'accessibilità insufficiente alle politiche di tutela della sfera privata delle imprese nuoce alle persone in cui dati personali vengono raccolti e trattati, e può costituire una **violazione del principio di notifica**. In tali casi, può accadere che le persone i cui dati sono trasferiti dall'UE ignorino i loro diritti e gli obblighi cui è tenuta un'impresa auto-certificata.

Inoltre, l'impegno stipulato dalle imprese di rispettare i principi di riservatezza **autorizza la Commissione federale per il Commercio ad avvalersi della facoltà di fare applicare tali principi** in caso di inosservanza, come se si trattasse di una pratica sleale o ingannevole. La mancanza di trasparenza delle imprese statunitensi rende la supervisione da parte della Commissione federale per il Commercio più difficile e mina l'efficacia del controllo dell'applicazione dei principi.

Nel corso degli anni, è successo che un numero considerevole di imprese auto-certificate non abbia reso pubblica la propria politica di tutela della sfera privata e/o non abbia dichiarato pubblicamente l'adesione ai principi in materia di riservatezza. La relazione del 2004 sul regime Approdo sicuro ha evidenziato la necessità che il Dipartimento del Commercio **adotti un atteggiamento più attivo nell'esaminare l'osservanza** di questa condizione.

Dal 2004, il Dipartimento del Commercio ha sviluppato **nuovi strumenti di informazione** per aiutare le imprese ad adempiere ai loro obblighi in materia di trasparenza. Le informazioni rilevanti sul regime sono consultabili sul sito web del Dipartimento del Commercio dedicato ad Approdo sicuro[20], che consente anche alle imprese di caricare le loro politiche di tutela

[19] Si veda il comunicato stampa del 18 novembre 2013 dell'APT lussemburghese.

[20] http://www.export.gov/SafeHarbour/

della sfera privata. Il Dipartimento del Commercio ha riferito che le imprese hanno utilizzato questa funzionalità, e contestualmente alla domanda di adesione ad Approdo sicuro hanno pubblicato le loro politiche in materia[21]. Il Dipartimento del Commercio ha inoltre pubblicato fra il 2009 e il 2013 una serie di orientamenti per le imprese che intendono aderire al regime, come una "Guida all'auto-certificazione" ("*Guide to Self-Certification*") e "Consigli utili per un'auto-certificazione conforme" ("*Helpful Hints on Self-Certifying Compliance*")[22].

Il grado di osservanza degli obblighi in materia di trasparenza varia da impresa a impresa. Se alcune società si limitano a comunicare al Dipartimento del Commercio una descrizione della loro politica di tutela della sfera privata come parte della procedura di auto-certificazione, la maggior parte pubblicano queste politiche sui loro siti web oltre a caricarle su quello del Dipartimento del Commercio. Tuttavia, queste **politiche non sono sempre presentate in una forma adatta ai consumatori e facilmente leggibile**. Gli hyperlink alle politiche non sempre funzionano correttamente e non sempre rimandano alle pagine giuste.

Dalla decisione e dai relativi allegati consegue che la condizione che le imprese rendano pubbliche le loro politiche di tutela della sfera privata **va al di là della mera comunicazione** dell'autocertificazione al Dipartimento del Commercio. Le condizioni da rispettare per la certificazione, quali enunciate nelle FAQ, includono una descrizione della politica di tutela della sfera privata e informazioni trasparenti sulla sede in cui essa è pubblicamente consultabile[23]. Le dichiarazioni relative alla politica di tutela della sfera privata devono essere chiare e facilmente accessibili al pubblico. Devono includere un hyperlink verso il sito web sull'Approdo sicuro del Dipartimento del Commercio, che elenca tutti i membri "attuali" del regime, e un link che rinvii a un prestatore incaricato della risoluzione alternativa delle controversie. Tuttavia, un certo numero di imprese iscritte ad Approdo sicuro fra il 2000 e il 2013 non ha adempiuto a queste condizioni. In occasione di contatti di lavoro con la Commissione nel febbraio 2013, il Dipartimento del Commercio ha riconosciuto che esiste una proporzione del 10% di imprese certificate che possono effettivamente non aver pubblicato sul loro sito la loro politica di tutela della privacy con la dichiarazione di adesione ai principi di Approdo sicuro.

Recenti statistiche evidenziano inoltre un persistente problema di **false dichiarazioni di adesione al regime Approdo sicuro**. Circa il 10% delle imprese che dichiarano di avervi aderito non figurano nell'elenco del Dipartimento del Commercio come membri attuali[24]: si tratta sia di società che non hanno mai partecipato all'accordo che di imprese un tempo iscritte ma che non hanno poi rinnovato l'auto-certificazione presso il Dipartimento del Commercio alle scadenze annuali. In quest'ultimo caso esse continuano a figurare sul sito web del Dipartimento dedicato ad Approdo sicuro ma lo status della loro certificazione è "non attuale", il che significa che l'impresa ha partecipato all'accordo e ha pertanto l'obbligo di continuare a tutelare i dati già trattati. La Commissione federale per il Commercio è competente a intervenire in casi di pratiche ingannevoli e di inosservanza dei principi di Approdo sicuro (vedi punto 5.1). La mancanza di chiarezza in merito alle "false dichiarazioni" nuoce alla credibilità del regime.

---

21 https://SafeHarbour.export.gov/list.aspx

22 La Guida è disponibile sul sito web del programma, all'indirizzo: http://export.gov/SafeHarbour/ *Helpful Hints*: http://export.gov/SafeHarbour/eu/eg_main_018495.asp.

23 Il 12 novembre 2013 il Dipartimento del Commercio ha confermato: "Oggi, le imprese che dispongono di siti web pubblici, e che trattano dati di consumatori/clienti/visitatori, devono pubblicare sul loro sito una politica di tutela della sfera privata che sia conforme ai principi dell'Approdo sicuro" ("U.S.-EU Cooperation to Implement the Safe Harbor Framework" del 12 novembre 2013).

24 Nel settembre 2013 uno studio di consulenza australiano, Galexia, ha raffrontato le "false dichiarazioni" d'adesione ad Approdo sicuro nel 2008 e nel 2013. La principale conclusione è che, parallelamente all'aumento delle adesioni al regime fra il 2008 e il 2013 (da 1 109 a 3 246), il numero di false dichiarazioni è passato da 206 a 427. http://www.galexia.com/public/about/news/about_news-id225.html

Nel 2012 e nel 2013, con regolari contatti, la Commissione europea ha avvertito il Dipartimento del Commercio che, per soddisfare gli obblighi in materia di trasparenza, non basta che le imprese gli forniscano semplicemente una descrizione della loro politica di tutela della sfera privata, e che le dichiarazioni relative a tale politica devono essere rese pubbliche. Il Dipartimento del Commercio è inoltre stato invitato a **intensificare i controlli periodici dei siti web delle imprese** dopo la procedura di verifica svolta nel contesto della prima procedura di auto-certificazione o del rinnovo annuale, e di adottare provvedimenti nei riguardi delle imprese che non adempiono alle condizioni in materia di trasparenza

Come prima risposta alle preoccupazioni dell'UE, **da marzo 2013 il Dipartimento del Commercio ha imposto** alle imprese Approdo sicuro che dispongono di un sito web pubblico di presentarvi prontamente la loro politica in materia di riservatezza relativa ai clienti/utenti. Al tempo stesso ha cominciato a sollecitare tutte le imprese che non avevano ancora inserito nella loro politica di tutela della privacy il link al sito web Approdo sicuro del Dipartimento, per poter così rendere l'elenco ufficiale Approdo sicuro e il sito web direttamente accessibili ai consumatori che consultano il sito di un'impresa. Questo consentirà agli interessati europei di verificare immediatamente, senza ricerche supplementari sul web, gli impegni che una data impresa ha presentato al Dipartimento del Commercio. Il Dipartimento del Commercio ha altresì cominciato a comunicare alle imprese l'esigenza di inserire, nella loro politica di tutela della sfera privata, anche le coordinate del loro prestatore indipendente incaricato della risoluzione delle controversie[25].

Questo processo deve essere accelerato per garantire che tutte le imprese certificate si conformino pienamente alle condizioni di Approdo sicuro entro marzo 2014 (cioè alla scadenza del rinnovo annuale dell'auto-certificazione a decorrere dall'introduzione delle nuove condizioni nel marzo 2013).

Permangono comunque preoccupazioni in merito alla piena osservanza, da parte delle imprese certificate, degli obblighi in materia di trasparenza. È opportuno che il Dipartimento del Commercio proceda a controlli e a indagini più rigorosi per verificare il rispetto degli obblighi assunti al momento della prima auto-certificazione e del rinnovo annuale.

4. INTEGRAZIONE DEI PRINCIPI DI APPRODO SICURO IN MATERIA DI RISERVATEZZA NELLE POLITICHE DI TUTELA DELLA SFERA PRIVATA ADOTTATE DALLE IMPRESE

Per ottenere e conservare i vantaggi del regime Approdo sicuro le imprese auto-certificate devono rispettare i principi in materia di riservatezza di cui all'allegato I della relativa decisione.

Nella relazione del 2004, la Commissione ha concluso che un numero considerevole di imprese **non aveva correttamente integrato i principi di Approdo sicuro in materia di riservatezza** nelle politiche di trattamento dei dati. Ad esempio, gli interessati non ricevevano sempre informazioni chiare e trasparenti sulle finalità del trattamento dei loro dati, o non avevano facoltà di rifiuto nel caso in cui tali dati dovessero essere divulgati a terzi o usati per fini incompatibili con quelli per cui erano stati originariamente raccolti. In tale relazione, la Commissione ha ritenuto che il Dipartimento del Commercio "*dovrebbe essere più proattivo per quanto riguarda l'accesso ad Approdo sicuro e la sensibilizzazione ai suoi principi*"[26].

[25] Fra marzo e settembre 2013 il Dipartimento del Commercio ha:
- comunicato alle 101 imprese che avevano già caricato sul sito Approdo sicuro del Dipartimento la loro politica di tutela della sfera privata conforme ai principi del regime, che esse devono pubblicare tale politica anche sul loro proprio sito web;
- sollecitato 154 imprese a inserire nella loro politica di tutela della sfera privata un link al sito Approdo sicuro;
- comunicato a più di 600 imprese l'esigenza di inserire, nella loro politica di tutela della sfera privata, le coordinate del loro prestatore indipendente incaricato della risoluzione delle controversie.

[26] Si veda pag. 8 della relazione del 2004, SEC (2004) 1323.

Sotto tale aspetto i progressi compiuti sono pochi. Dal 1° gennaio 2009, ogni impresa che alla scadenza annuale intenda rinnovare lo status della certificazione per Approdo sicuro deve sottoporre preliminarmente la propria politica di tutela della sfera privata al Dipartimento del Commercio. Tale valutazione ha tuttavia una portata limitata. Non esiste **alcuna valutazione completa delle pratiche effettive delle imprese auto-certificate**, che aumenterebbe invece significativamente la credibilità della procedura di auto-certificazione.

A seguito della richiesta, avanzata dalla Commissione, di una supervisione più rigorosa e sistematica delle imprese auto-certificate da parte del Dipartimento del Commercio, **le nuove domande di adesione sono ora oggetto di una maggiore attenzione**. Fra il 2010 e il 2013 il numero di domande non accettate e rinviate alle imprese affinché apportassero miglioramenti alle loro politiche in materia di privacy è considerevolmente aumentato: è raddoppiato per quanto riguarda le richieste di rinnovo ed è triplicato per quanto riguarda le nuove adesioni[27]. Il Dipartimento del Commercio ha assicurato alla Commissione che le nuove certificazioni e i rinnovi possono essere ultimati solo se le politiche di tutela della sfera privata adottate dall'impresa soddisfano tutte le condizioni e, specialmente, comportano l'impegno di adesione all'insieme dei principi rilevanti di Approdo sicuro e sono pubbliche. Le imprese sono tenute a precisare, nelle menzioni figuranti nell'elenco di Approdo sicuro, la sede in cui è consultabile la loro politica. Devono anche indicare chiaramente sul loro sito web un prestatore indipendente incaricato della risoluzione delle controversie, e devono inserire un link che rinvii alla rubrica dell'auto-certificazione Approdo sicuro sul sito del Dipartimento del Commercio. È stato tuttavia stimato che più del 30% dei membri di Approdo sicuro non hanno inserito alcuna informazione sulla risoluzione delle controversie nelle politiche sulla privacy pubblicate sui loro siti[28].

In caso di eliminazione di società dall'elenco di Approdo sicuro da parte del Dipartimento del Commercio, ciò è avvenuto la maggior parte delle volte su esplicita richiesta delle imprese interessate (ad es. imprese che erano state oggetto di una fusione o di un'acquisizione, che avevano cambiato ramo di attività o avevano cessato di operare). Un più piccolo numero di imprese inattive è stato eliminato quando è stato constatato che i siti web indicati nell'elenco non risultavano più operativi e che lo status della certificazione di queste imprese era stato "Non attuale" per parecchi anni[29]. È importante osservare che nessuna di queste rimozioni sembra essere avvenuta a causa dell'individuazione di problemi di conformità a seguito della verifica del Dipartimento del Commercio.

L'elenco di Approdo sicuro funge da avviso pubblico e da registrazione degli impegni assunti dai membri. **L'adesione ai principi di Approdo sicuro non viene meno col tempo** per quanto riguarda i dati ricevuti nel corso del periodo durante il quale l'impresa gode dei vantaggi del regime: l'impresa deve continuare ad applicarne i principi ai dati in questione sino a quando essa continuerà a detenerli, utilizzarli o rivelarli, anche se dovesse per qualsiasi motivo abbandonare l'Approdo sicuro.

Il numero di **richiedenti l'adesione** al regime e che non sono mai stati inseriti nell'elenco Approdo sicuro poiché **non hanno superato il controllo amministrativo** svolto dal

[27] Secondo le statistiche da esso fornite nel settembre 2013, il Dipartimento del Commercio ha contattato nel 2010 il 18% (93) delle 512 nuove imprese aderenti e il 16% (231) delle 1 417 imprese in fase di rinnovo affinché apportassero miglioramenti alle loro politiche in materia di privacy e/o alle domande di adesione. A seguito della richiesta, avanzata dalla Commissione, di sottoporre a un esame rigoroso, accurato e sistematico tutte le domande, a metà settembre 2013 il DdC aveva contattato il 56% (340) delle 602 nuove imprese aderenti e il 27% (493) delle 1 809 imprese in fase di rinnovo invitandole ad apportare miglioramenti alle loro politiche in materia di privacy.

[28] Intervento di Chris Connolly (Galexia) in occasione dell'indagine della commissione LIBE del Parlamento europeo il 7 ottobre 2013.

[29] A dicembre 2011, il Dipartimento del Commercio statunitense aveva tolto dall'elenco di Approdo sicuro 323 imprese: 94 erano state eliminate perché non più in attività, 88 a seguito di acquisizioni o fusioni; 95 su richiesta della società madre; 41 per ripetuto mancato rinnovo della certificazione e 5 per ragioni varie.

Dipartimento del Commercio è il seguente: **nel 2010**, solo il **6%** (33) delle 513 nuove imprese aderenti non sono state inserite nell'elenco Approdo sicuro poiché non soddisfacevano le regole di auto-certificazione del Dipartimento del Commercio; nel **2013**, la percentuale di nuove imprese aderenti non inserite nell'elenco Approdo sicuro poiché non soddisfacevano le regole di auto-certificazione del Dipartimento del Commercio è stata del **12%** (75 su 605).

Come condizione minima per accrescere la trasparenza della supervisione esercitata, il Dipartimento del Commercio dovrebbe elencare sul suo sito web tutte le imprese eliminate dal regime Approdo sicuro e dovrebbe indicare le ragioni del non avvenuto rinnovo. La dicitura "Non attuale" figurante nell'elenco dei membri di Approdo sicuro del Dipartimento del Commercio non dovrebbe essere considerata una semplice informazione, ma dovrebbe essere accompagnata da **un chiaro avvertimento** – sia scritto che grafico – del fatto che attualmente l'impresa in questione non soddisfa le condizioni del regime.

Inoltre, alcune imprese non hanno ancora pienamente integrato tutti i principi di Approdo sicuro. Oltre al problema della trasparenza di cui sopra, al punto 3, le politiche di tutela della sfera privata delle imprese auto-certificate spesso sono opache per quanto riguarda le finalità di raccolta dei dati e il diritto di accettare o meno la loro divulgazione a terzi e sollevano di conseguenza problemi di conformità con i principi della "Notifica" e della "Scelta" – che sono principi fondamentali per garantire il controllo, da parte degli interessati, su quanto accade alle informazioni personali che li riguardano.

Il primo passo decisivo del processo di messa in conformità – cioè l'integrazione dei principi d'Approdo sicuro in materia di riservatezza nelle politiche di tutela della sfera privata adottate dalle imprese – non è sufficientemente garantito. Il Dipartimento del Commercio dovrebbe affrontare tale questione in maniera prioritaria, elaborando una metodologia di messa in conformità rivolta alle imprese, sia nella loro pratica operativa che nelle interazioni con i clienti. **Occorre che il Dipartimento del Commercio segua attivamente la questione dell'effettiva integrazione dei principi d'Approdo sicuro in materia di riservatezza nelle politiche di tutela della sfera privata delle imprese**, senza lasciare che le azioni per garantire l'applicazione dei principi intervengano solo in caso di denunce dei cittadini.

5. APPLICAZIONE DA PARTE DELLE PUBBLICHE AUTORITÀ

Esiste una serie di meccanismi per garantire l'effettiva applicazione del regime Approdo sicuro e la possibilità di ricorso per le persone nel caso in cui la protezione delle loro informazioni personali sia venuta meno a causa dell'inosservanza dei principi in materia di riservatezza.

Secondo il principio "Garanzie d'applicazione", le politiche di tutela della sfera privata applicate dalle organizzazioni auto-certificate devono comportare efficaci meccanismi volti ad assicurare il rispetto delle regole. Il principio "Garanzie d'applicazione", quale chiarito dalle FAQ 11, 5 e 6, prevede che tale condizione possa essere soddisfatta aderendo a **dispositivi indipendenti di ricorso** di organi che hanno dichiarato pubblicamente la loro competenza a trattare reclami individuali per inosservanza dei principi. Alternativamente, l'organizzazione può adempiere a tale obbligo impegnandosi a cooperare con il **Comitato UE per la tutela dei dati**[30]. Inoltre, le imprese auto-certificate sono sottoposte all'autorità della Commissione

[30] Il Comitato UE per la tutela dei dati è un organo competente a esaminare e a provvedere in merito alle denunce presentate dai cittadini per presunta violazione dei principi di Approdo sicuro da parte di imprese statunitensi membri dell'accordo. Le imprese che sottoscrivono i principi di Approdo sicuro devono scegliere di aderire a meccanismi di ricorso indipendenti o di cooperare con il Comitato UE per la tutela dei dati per rimediare ad eventuali problemi insorti in seguito al mancato rispetto dei principi Approdo sicuro. La cooperazione con il Comitato UE per la tutela dei dati è tuttavia obbligatoria quando l'impresa USA tratta dati personali trasferiti dall'UE e riguardanti le risorse umane nel contesto di un rapporto di lavoro. Se l'impresa si impegna a cooperare con il Comitato, deve anche impegnarsi ad adeguarsi a qualsiasi parere da esso formulato qualora questo

federale per il Commercio ai sensi della sezione 5 del Federal Trade Commission Act, che vieta attività o pratiche sleali o ingannevoli in materia commerciale o collegata al commercio[31].

La relazione del 2004 ha espresso preoccupazioni quanto all'applicazione del regime Approdo sicuro, indicando nello specifico che la Commissione federale per il Commercio dovrebbe essere più proattiva nell'avviare indagini e nel sensibilizzare i cittadini sui propri diritti. Un altro motivo di preoccupazione era la mancanza di chiarezza per quanto riguarda la competenza della Commissione federale per il Commercio ad applicare i principi riguardanti i dati sulle risorse umane.

L'organo di ricorso per i dati sulle risorse umane – il Comitato UE per la tutela dei dati – ha ricevuto una sola denuncia in materia[32]. L'assenza di denunce non consente tuttavia di concludere che il regime funzioni pienamente. Sarebbe opportuno introdurre controlli d'ufficio sulla conformità delle imprese per verificare l'attuazione effettiva degli impegni assunti in materia di protezione dei dati. Le autorità europee per la protezione dei dati dovrebbero a loro volta intraprendere azioni di sensibilizzazione sull'esistenza del Comitato.

Sono stati evidenziati problemi in relazione al funzionamento degli organi di ricorso alternativi come organi di controllo dell'applicazione. Alcuni di questi organi non dispongono di mezzi adeguati per rimediare ai casi di inosservanza dei principi. Queste lacune devono essere affrontate.

5.1. Commissione federale per il Commercio

La Commissione federale per il Commercio può prendere misure d'applicazione in caso di violazione degli impegni Approdo sicuro assunti dalle imprese. Quando è stato istituito il regime Approdo sicuro, la Commissione federale per il Commercio si è impegnata ad esaminare in via prioritaria tutti i casi trasmessi dalle autorità degli Stati membri dell'UE[33]. Non avendo ricevuto denunce durante i primi dieci anni dell'accordo, la Commissione federale per il Commercio ha deciso di cercare di individuare eventuali violazioni di Approdo sicuro nelle indagini da essa svolte in materia di vita privata e sicurezza dei dati. Dal 2009 ha avviato 10 azioni nei riguardi di imprese che hanno violato i principi di Approdo sicuro: tali azioni sono sfociate nelle decisioni (soggette a considerevoli sanzioni) di proibire le presentazioni ingannevoli legate alla privacy, anche relative al rispetto dei principi di Approdo sicuro, e di imporre alle imprese ampi programmi di protezione della privacy e auditing per 20 anni. Su richiesta della Commissione federale per il Commercio, le imprese devono accettare valutazioni indipendenti dei loro programmi di tutela della riservatezza, che le sono periodicamente riferite. Le decisioni della Commissione federale per il Commercio vietano inoltre alle imprese le presentazioni ingannevoli quanto alle loro prassi in materia di privacy e alla partecipazione all'Approdo sicuro o ad analoghi regimi di tutela della vita privata. Ciò è avvenuto ad esempio nel caso delle indagini su Google, Facebook and Myspace[34]. Nel 2012 Google ha accettato di pagare un'ammenda di 22,5 milioni di dollari per

---

ritenga che l'impresa debba attuare specifici interventi per uniformarsi ai principi dell'Approdo sicuro, anche laddove tra questi rientrino provvedimenti di riparazione o risarcimento.

31 Il Dipartimento dei Trasporti esercita un'autorità analoga nei confronti dei vettori aerei in virtù del Titolo 49 della sezione 41712 dell'United States Code.

32 La denuncia è stata presentata da un cittadino svizzero. Il Comitato UE per la tutela dei dati l'ha quindi deferita all'autorità svizzera per la protezione dei dati (con la Svizzera gli USA hanno in effetti stipulato un regime di Approdo sicuro distinto).

33 Si veda l'allegato V della decisione 2000/520/CE DELLA Commissione del 26 luglio 2000.

34 Nel periodo 2009-2012 la Commissione federale per il Commercio ha portato a termine 10 azioni a seguito di violazioni degli impegni Approdo sicuro: FTC v. Javian Karnani, and Balls of Kryptonite, LLC (2009), World Innovators, Inc. (2009), Expat Edge Partners, LLC (2009), Onyx Graphics, Inc. (2009), Directors Desk LLC (2009), Progressive Gaitways LLC (2009), Collectify LLC (2009), Google Inc. (2011), Facebook, Inc. (2011), Myspace LLC (2012). Si veda: "Federal Trade Commission of Safe Harbour Commitments":

comporre le accuse di aver violato un'ordinanza. In tutte le indagini relative alla privacy, la Commissione federale per il Commercio esamina d'ufficio se intervenga una violazione dei principi Approdo sicuro.

La FTC ha recentemente ribadito le proprie dichiarazioni e il proprio impegno ad esaminare in via prioritaria qualsiasi caso trasmesso da organizzazioni di autoregolamentazione in materia di riservatezza e dagli Stati membri dell'UE per denunciare la presunta non conformità di un'impresa ai principi dell'Approdo sicuro[35]. Negli ultimi tre anni le autorità europee per la protezione dei dati hanno trasmesso alla Commissione federale per il Commercio solo pochi fascicoli.

La cooperazione transatlantica fra le autorità per la protezione dei dati ha cominciato a svilupparsi negli ultimi mesi. Il 26 giugno 2013, ad esempio, la Commissione federale per il Commercio ha firmato con l'Ufficio irlandese del Commissario per la protezione dei dati un Protocollo d'intesa sulla mutua assistenza nell'applicazione delle leggi di tutela delle informazioni personali nel settore privato. Il Protocollo stabilisce un quadro per intensificare, ottimizzare e rendere più efficace la cooperazione in materia di applicazione della tutela della privacy[36].

Nell'agosto 2013, la Commissione federale per il Commercio ha annunciato un rafforzamento delle verifiche aventi ad oggetto imprese che controllano grosse banche di dati a carattere personale. Ha inoltre creato un portale sul quale i consumatori possono presentare denunce di violazione della privacy contro imprese americane[37].

La Commissione federale per il Commercio dovrebbe altresì intensificare gli sforzi di indagine sulle false dichiarazioni di adesione ad Approdo sicuro. Un'impresa che dichiara sul proprio sito web di soddisfare le condizioni Approdo sicuro, ma che non figura nell'elenco del Dipartimento del Commercio come membro "attuale", inganna i consumatori e abusa della loro fiducia. Le false dichiarazioni indeboliscono la credibilità del sistema nel suo complesso e dovrebbero quindi essere immediatamente eliminate dai siti web delle imprese, che dovrebbero inoltre essere vincolate dall'obbligo giuridico di non ingannare i consumatori. La Commissione federale per il Commercio dovrebbe continuare a reperire le false dichiarazioni rispetto ad Approdo sicuro come è avvenuto per il caso *Karnani*, quando la FTC ha fatto chiudere un sito web in California in cui figurava una falsa registrazione Approdo sicuro, e in cui si praticavano fraudolente attività di commercio elettronico con consumatori europei[38].

Il 29 ottobre 2013 la Commissione federale per il Commercio ha annunciato di avere avviato "negli ultimi mesi numerose indagini relative all'osservanza dei principi di Approdo sicuro", e che "nei mesi a venire" erano prevedibili nuove azioni su questo fronte. La FTC ha inoltre confermato di essersi "impegnata a cercare modi per migliorare la propria efficacia" e che avrebbe "continuato ad accogliere favorevolmente ogni pista significativa, come la denuncia ricevuta nei mesi passati da un difensore dei diritti dei consumatori con sede in Europa, che ha riferito un gran numero di presunte violazioni di Approdo sicuro"[39]. La FTC si è altresì

---

http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf Si veda anche: "Case Highlights": http://business.ftc.gov/us-eu-Safe-Harbour-framework. La maggior parte di questi casi riguardavano problemi con imprese che avevano aderito ad Approdo sicuro e che continuavano a presentarsi come membri senza avere però rinnovato la certificazione annuale.

35 Questo impegno è stato ribadito a una riunione fra il Commissario della FTC Julie Brill e le autorità UE per la protezione dei dati (Gruppo di lavoro "Articolo 29") a Bruxelles il 17 aprile 2013.

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n

37 Per le loro denunce i consumatori americani possono avvalersi del sito Federal Trade Commission Complaint Assistant (https://www.ftccomplaintassistant.gov/); i consumatori stranieri possono presentare le denunce all'indirizzo http://www.econsumer.gov.

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf e http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf

impegnata a "monitorare sistematicamente l'osservanza delle decisioni relative ad Approdo sicuro, come facciamo per tutte le nostre decisioni"[40].

Il 12 novembre 2013, la Commissione federale per il Commercio ha informato la Commissione europea che: "**se la politica di tutela della sfera privata di una data imprese promette protezioni conformi ai principi Approdo sicuro, la mancata adesione al regime o il mancato rinnovo della certificazione non sono, in sé, di natura tale da sottrarre l'impresa al controllo dell'applicazione, da parte della FTC, di tali impegni Approdo sicuro**"[41].

Nel novembre 2013, il Dipartimento del Commercio ha informato la Commissione europea che "per aiutare a garantire che le imprese non facciano 'false dichiarazioni' di partecipazione ad Approdo sicuro, il Dipartimento del Commercio comincerà a contattarne i membri un mese prima della data di rinnovo della certificazione per spiegare loro la procedura da seguire qualora decidessero di non procedere a tale rinnovo". **Il Dipartimento del Commercio** "**avvertirà le imprese** di questa categoria che dovranno eliminare dalle loro politiche in materia di privacy e dai loro siti web qualsiasi riferimento all'adesione ad Approdo sicuro, compreso l'utilizzo del corrispondente marchio di certificazione, **e comunicherà loro chiaramente che, in caso di omissione, possono essere oggetto di misure d'applicazione da parte della Commissione federale per il Commercio**"[42].

Per lottare contro il fenomeno delle false dichiarazioni di adesione ad Approdo sicuro, le politiche in materia di riservatezza pubblicate sui siti web delle imprese auto-certificate dovrebbero sempre includere un link verso il sito web Approdo sicuro del Dipartimento del Commercio, dove sono elencati tutti i membri "attuali". Ciò consentirà agli interessati europei di verificare immediatamente, senza ricerche supplementari, se una società aderisce in quel momento ad Approdo sicuro. Il Dipartimento del Commercio ha cominciato a imporre questa condizione alle imprese nel marzo 2013, ma il processo dovrebbe essere intensificato.

Per garantire il corretto ed effettivo funzionamento di Approdo sicuro, la priorità fondamentale resta – oltre alle misure prese dal Dipartimento del Commercio come sopra indicato – il monitoraggio continuo da parte della Commissione federale per il Commercio e il conseguente controllo da essa svolto sull'effettiva attuazione dei principi in questione. È necessario in particolare incrementare i **controlli e le indagini d'ufficio sull'osservanza, da parte delle imprese,** dei principi di Approdo sicuro. Dovrebbe essere inoltre agevolata la presentazione delle denunce di violazione alla Commissione federale per il Commercio.

5.2. Comitato UE per la tutela dei dati

Il Comitato UE per la tutela dei dati è un organo creato nel contesto della decisione Approdo sicuro. È competente a esaminare le denunce presentate dai cittadini e riguardanti i dati personali raccolti nel contesto di un rapporto di lavoro, così come i casi delle imprese auto-certificate che hanno scelto di avvalersi di questa opzione per la risoluzione delle controversie nell'ambito di Approdo sicuro (53% di tutte le imprese). È composto da rappresentanti di varie autorità dell'UE per la protezione dei dati.

Finora il Comitato ha ricevuto 4 denunce (2 nel 2010 e 2 nel 2013). Ha deferito le due denunce del 2010 ad autorità nazionali per la protezione dei dati (Regno Unito e Svizzera), e sta attualmente esaminando la terza e la quarta denuncia. Il numero esiguo di denunce può

[40] Lettera della Presidente della Commissione federale per il Commercio Edith Ramirez alla Vicepresidente Viviane Reding.
[41] Lettera della Presidente della Commissione federale per il Commercio Edith Ramirez alla Vicepresidente Viviane Reding.
[42] "U.S.-EU Cooperation to Implement the Safe Harbor Framework", 12 novembre 2013.

spiegarsi per il fatto che i poteri del Comitato sono, come indicato sopra, limitati essenzialmente a certi tipi di dati.

Il limitato numero di casi sottoposti al Comitato potrebbe anche essere in parte spiegato dalla scarsa conoscenza della sua esistenza. Dal 2004 la Commissione ha reso più visibili sul suo sito web le informazioni relative al Comitato[43].

Affinché il Comitato sia utilizzato in modo più efficiente, le imprese negli USA che hanno scelto di cooperare con esso e di conformarsi alle sue decisioni (per alcune o per tutte le categorie di dati personali contemplati nelle loro auto-certificazioni) dovrebbero indicarlo chiaramente e visibilmente fra gli impegni assunti nelle loro politiche in materia di privacy, in modo che il Dipartimento del Commercio possa controllare questo aspetto. Sul sito web di ogni autorità europea per la protezione dei dati dovrebbe essere creata un'apposita pagina relativa ad Approdo sicuro, in modo da sensibilizzare su questo aspetto le imprese e gli interessati europei.

5.3. Miglioramento nell'applicazione

Le carenze sopra indicate in materia di trasparenza e di applicazione suscitano preoccupazione fra le imprese europee per quanto riguarda l'incidenza negativa del regime Approdo sicuro sulla loro competitività. Una società europea che compete con una società statunitense operante nell'ambito di Approdo sicuro senza applicarne i principi si trova rispetto ad essa in una situazione di svantaggio.

Inoltre, la giurisdizione della Commissione federale per il Commercio è limitata a pratiche sleali o ingannevoli "in materia commerciale o collegata al commercio". La sezione 5 del Federal Trade Commission Act ha definito eccezioni all'autorità della FTC in materia di atti o pratiche sleali o ingannevoli per quanto riguarda, fra l'altro, le **telecomunicazioni.** Non rientrando nel campo d'azione della Commissione federale per il Commercio, le società di telecomunicazione non sono autorizzate ad aderire al regime di Approdo sicuro. Tuttavia, data la crescente convergenza fra tecnologia e servizi, molti dei loro concorrenti diretti nel settore TIC negli USA ne sono invece membri. L'esclusione delle società di telecomunicazione dagli scambi di dati nell'ambito del regime Approdo sicuro preoccupa alcuni operatori di telecomunicazioni europei. Secondo l'Associazione degli operatori di reti di telecomunicazioni europei (ETNO) "vi è un chiaro conflitto con la più importante richiesta degli operatori di telecomunicazioni relativa alla necessità di eque condizioni di concorrenza"[44].

---

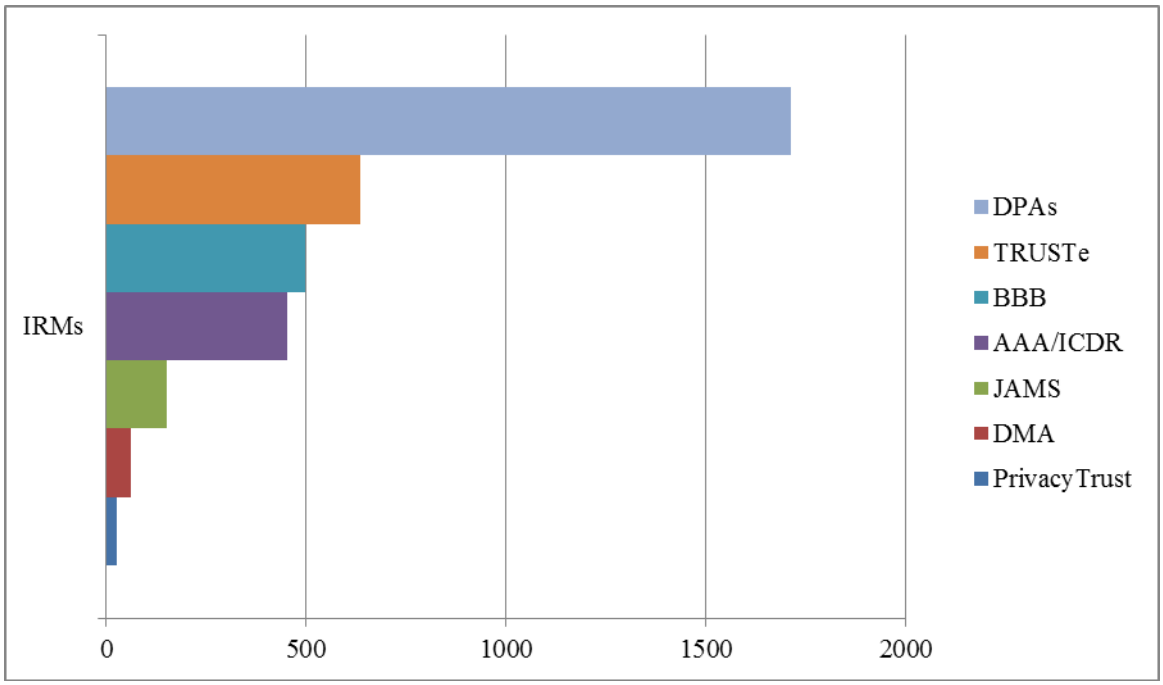
[43] A seguito della relazione del 2004, su un sito web della Commissione (DG Giustizia) è stata pubblicata una Nota informativa sul Comitato UE per la tutela dei dati in forma di Domande e Risposte, con lo scopo di sensibilizzare i cittadini e di aiutarli a presentare denuncia qualora ritengano che i loro dati personali siano stati trattati in violazione dei principi di Approdo sicuro: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf
Il modulo standard per la denuncia è disponibile al seguente indirizzo: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/ complaint_form_en.pdf

[44] Le "Considerazioni di ETNO" ricevute dai servizi della Commissione il 4 ottobre 2013 vertono anche sui punti seguenti 1) definizione di "dati personali" nell'ambito di Approdo sicuro; 2) mancanza di controllo su Approdo sicuro, e 3) il fatto che "le imprese americane possono trasferire dati con molte meno restrizioni rispetto alle loro controparti europee", cosa che "costituisce una chiara discriminazione delle imprese europee e ne sta compromettendo la competitività". Ai sensi delle norme di Approdo sicuro, le organizzazioni che comunicano informazioni a terzi devono applicare i principi di notifica e di scelta. Un'organizzazione che intende trasferire informazioni a terzi che agiscono in qualità di rappresentanti, lo può fare a condizione di accertarsi prima che questi ultimi aderiscono ai principi dell'Approdo sicuro, o rientrano nel campo d'applicazione della direttiva o di un'altra forma d'accertamento dell'idoneità, ovvero di stipulare con i terzi un accordo scritto che comporti per essi l'obbligo di offrire almeno lo stesso livello di protezione della riservatezza richiesto dai relativi principi.

6. RAFFORZAMENTO DEI PRINCIPI DI APPRODO SICURO IN MATERIA DI RISERVATEZZA

6.1. Risoluzione alternativa delle controversie

In virtù del principio "Garanzie d'applicazione", vi devono essere "**meccanismi di ricorso** [...] **di pronto impiego e di costo accessibile**, atti a consentire d'istruire [...] qualsiasi ricorso o contenzioso individuale". A tal fine il regime Approdo sicuro stabilisce un sistema di risoluzione alternativa delle controversie (ADR) da parte di un terzo indipendente[45] per offrire alle persone soluzioni rapide. I tre principali organi per i meccanismi di ricorso sono il Comitato UE per la tutela dei dati, BBB (Better Business Bureaus) e TRUSTe.



Il ricorso all'ADR è aumentato dal 2004 e il Dipartimento del Commercio ha rafforzato il controllo dei prestatori americani incaricati della risoluzione alternative delle controversie per garantire che le informazioni da essi offerte sulla procedura siano chiare, accessibili e comprensibili. Dato il limitato numero di casi trattati finora l'efficacia di questo sistema deve tuttavia essere ancora dimostrata[46].

Benché il Dipartimento del Commercio sia riuscito a ridurre gli onorari chiesti per il ricorso ad ADR, due dei sette maggiori prestatori di tali servizi continuano ad applicare onorari a chi presenta denuncia[47]. Si tratta dei prestatori di servizi ADR cui si rivolgono circa il 20% delle

45 La direttiva 2013/11/UE sull'ADR per i consumatori sottolinea l'importanza di procedure indipendenti, imparziali, trasparenti, efficaci, rapide ed eque di risoluzione alternativa delle controversie.

46 Ad esempio, un importante prestatore di servizi ("TRUSTe") ha riferito di aver ricevuto 881 domande nel 2010, ma che solo 3 sono state ritenute ammissibili e fondate, e hanno condotto alla richiesta di far modificare la politica sulla privacy e il sito web dell'impresa interessata. Nel 2011 il numero di denunce è stato 879, e in un caso è stato chiesto all'impresa di cambiare la politica sulla privacy. Secondo il Dipartimento del Commercio, l'ampia maggioranza dei ricorsi all'ADR è costituita da domande di consumatori, ad esempio utenti che hanno dimenticato la password e non sono riusciti a recuperarla dal servizio Internet. Su richiesta della Commissione, il Dipartimento del Commercio ha sviluppato nuovi criteri di comunicazione di statistiche che possono essere utilizzati da tutti i sistemi di ADR. Tali criteri fanno una distinzione fra semplici domande e denunce, e forniscono chiarimenti supplementari sul tipo di denunce ricevute. Questi nuovi criteri, tuttavia, devono essere ulteriormente discussi per garantire che le nuove statistiche nel 2014 riguardino tutti i prestatori incaricati di ADR, siano comparabili e forniscano informazioni determinanti per valutare l'efficacia del meccanismo di ricorso.

47 L'International Centre for Dispute Resolution / American Arbitration Association (ICDR/AAA) chiede 200 dollari e JAMS 250 dollari come "spese di apertura fascicolo". Il Dipartimento del Commercio ha informato la Commissione di aver lavorato con AAA, il più oneroso prestatore di servizi ADR per persone fisiche, per sviluppare uno specifico programma Approdo sicuro di riduzione dei costi per i clienti da varie migliaia di dollari a una cifra forfettaria di 200 dollari.

imprese aderenti ad Approdo sicuro. Queste società hanno selezionato un prestatore ADR che chiede un onorario ai clienti che presentano una denuncia. Tali pratiche non sono conformi al principio "Garanzie d'applicazione" di Approdo sicuro, che conferisce agli individui il diritto di accedere a "meccanismi di ricorso indipendenti, di pronto impiego e di costo accessibile". Nell'Unione europea, l'accesso a un servizio indipendente di risoluzione delle controversie fornito dal Comitato UE per la tutela dei dati è gratuito per tutti gli interessati.

Il 12 novembre 2013 il Dipartimento del Commercio ha confermato che "continuerà a difendere il diritto dei cittadini dell'UE alla protezione della vita privata e che lavorerà con i prestatori di servizi ADR per vedere se i loro onorari possano essere ulteriormente ridotti".

Per quanto riguarda le sanzioni, non tutti prestatori di servizi ADR possiedono gli strumenti necessari per rimediare a situazioni di inosservanza dei principi in materia di riservatezza. Inoltre, la pubblicazione del verdetto di non-conformità non sembra essere prevista fra la gamma di sanzioni e misure da essi applicabili.

I prestatori di servizi ADR sono inoltre tenuti a deferire alla Commissione federale per il Commercio i casi in cui un'impresa non si conformi all'esito della procedura di risoluzione alternativa della controversia, o rigetti la decisione adottata dal prestatore, in modo che la FTC possa procedere a un esame e a un'inchiesta e, se necessario, adottare misure d'applicazione. Finora, tuttavia, nessun caso di inosservanza è stato deferito dai prestatori ADR alla Commissione federale per il Commercio[48].

I prestatori ADR elencano sui loro siti web gli elenchi delle imprese che si avvalgono dei loro servizi di risoluzione alternativa delle controversie (partecipanti ADR). Questo permette ai singoli consumatori di verificare facilmente se, in caso di contenzioso con una società, possono presentare denuncia a quel dato prestatore. Ad esempio, BBB elenca tutte le imprese appartenenti al suo sistema di risoluzione delle controversie. Vi sono tuttavia numerose imprese che dichiarano di rientrare in uno specifico sistema ADR ma la cui partecipazione non è confermata dai prestatori[49].

I meccanismi ADR devono essere facilmente accessibili, indipendenti e di costo accettabile per le persone fisiche. L'interessato deve essere in grado di presentare denuncia senza eccessive costrizioni. Tutti gli organismi ADR dovrebbero pubblicare sui loro siti web statistiche sulle denunce trattate così come specifiche informazioni sul loro esito. Dovrebbero infine essere ulteriormente controllati per garantire che le informazioni fornite sulla procedura e sulle modalità di presentazione delle denunce siano chiare e comprensibili – in modo che le procedure ADR diventino un meccanismo efficace, fidato e riuscito. Occorre altresì ribadire che la pubblicazione del verdetto di non-conformità dovrebbe essere inclusa nella gamma di sanzioni obbligatorie applicabili nel contesto ADR.

6.2. Trasferimento successivo

Data la crescita esponenziale dei flussi di dati personali, sorge la necessità di garantirne la protezione continua a tutti gli stadi del trattamento, in particolare quando un'impresa aderente ad Approdo sicuro trasferisce le informazioni a un **terzo incaricato**. Pertanto, la necessità di una migliore applicazione di Approdo sicuro riguarda non solo i suoi membri ma anche gli appaltatori.

[48] Si veda la FAQ 11.

[49] Amazon ha ad esempio informato il Dipartimento del Commercio di ricorrere a BBB come prestatore ADR. BBB, tuttavia, non menziona Amazon fra i suoi partecipanti ADR. Viceversa, Arsalon Technologies (www.arsalon.net), un fornitore di servizi di cloud hosting, figura nell'elenco di BBB relativo alla risoluzione delle controversie nell'ambito di Approdo sicuro, ma l'impresa non è un membro attuale del regime (situazione al 1° ottobre 2013). BBB, TRUSTe e gli altri prestatori ADR dovrebbero eliminare o correggere le dichiarazioni di certificazione, e dovrebbero essere vincolati dall'obbligo giuridico di certificare solo le imprese che sono membri di Approdo sicuro.

Approdo sicuro consente i trasferimenti successivi a terzi che agiscono in qualità di rappresentanti a condizione che l'impresa appartenente "[accerti] che questi ultimi aderiscono ai principi dell'Approdo sicuro, o rientrano nel campo d'applicazione della direttiva o di un'altra]forma d'accertamento dell'idoneità, ovvero [stipuli] con i terzi un accordo scritto che comporti per essi l'obbligo di offrire almeno lo stesso livello di protezione della riservatezza richiesto dai relativi principi"[50]. Ad esempio, il Dipartimento del Commercio richiede che un fornitore di cloud service concluda un contratto anche se rispetta i principi Approdo sicuro e riceve i dati personali a fini di trattamento[51]. Questa disposizione, che figura all'allegato II della decisione Approdo sicuro, non è comunque chiara.

Poiché il ricorso ad appaltatori è significativamente aumentato negli ultimi anni, in particolare nel contesto del cloud-computing, un'impresa membro di Approdo sicuro, quando conclude un tale contratto, dovrebbe informare il Dipartimento del Commercio ed essere tenuta a rendere pubbliche le garanzie relative alla tutela della sfera privata[52].

I tre aspetti sopra indicati, ossia i meccanismi di risoluzione alternativa delle controversie, una supervisione rafforzata e i trasferimenti successivi di dati, dovrebbero essere ulteriormente precisati.

7. ACCESSO AI DATI TRASFERITI NEL QUADRO DEL REGIME APPRODO SICURO

Nel corso del 2013, la circolazione di informazioni relative all'ampiezza e alla portata dei programmi di controllo degli Stati Uniti ha suscitato preoccupazioni sulla continuità della protezione dei dati personali lecitamente trasferiti negli USA nell'ambito del regime Approdo sicuro. Ad esempio, tutte le imprese partecipanti al programma PRISM, e che consentono alle autorità americane di avere accesso a dati conservati e trattati negli USA, risultano certificate nel quadro di Approdo sicuro. Questo sistema è diventato così una delle piattaforme di accesso delle autorità americane di intelligence alla raccolta di dati personali inizialmente trattati nell'UE.

La decisione Approdo sicuro prevede, all'allegato I, che l'adesione ai principi in materia di riservatezza possa essere limitata se ciò è giustificato da esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia, o da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali. Per essere valide, le limitazioni e restrizioni alla fruizione dei diritti fondamentali devono essere interpretate in senso restrittivo; devono essere enunciate in una legislazione pubblicamente accessibile e devono essere necessarie e proporzionate in una società democratica. In particolare, la decisione Approdo sicuro specifica che tali limitazioni sono consentite solo "**in quanto necessario**" per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia[53]. Se il

---

50 Si veda la decisione 2000/520/CE della Commissione, pag. 7 ("Trasferimento successivo").

51 Si veda "Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud-Computing": http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf.

52 Queste osservazioni riguardano i cloud provider non aderenti ad Approdo sicuro. Secondo lo studio di consulenza Galexia, "il livello di adesione (e di conformità) ad Approdo sicuro fra i fornitori di cloud service è molto alto. I fornitori di cloud service hanno generalmente vari livelli di protezione della privacy, e combinano spesso contratti diretti con i clienti e politiche generali di protezione della vita privata. Tranne per quanto riguarda una o due grosse eccezioni, i fornitori di cloud service, nell'ambito di Approdo sicuro, rispettano le disposizioni fondamentali relative alle risoluzioni delle controversie e all'attuazione dei principi. Al momento, nell'elenco delle false dichiarazioni di adesione, non figura alcun grosso fornitore di cloud service." (intervento di Chris Connolly (Galexia) in occasione dell'indagine della commissione LIBE "Sorveglianza elettronica di massa dei cittadini dell'UE").

53 Si veda l'allegato I della decisione Approdo sicuro "L'adesione a tali 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

trattamento eccezionale di dati a fini di sicurezza nazionale, interesse pubblico o amministrazione della giustizia è previsto da Approdo sicuro, l'accesso su larga scala da parte dei servizi di intelligence ai dati trasferiti negli USA nel contesto di operazioni commerciali non era prevedibile all'epoca dell'adozione di tale regime.

Inoltre, per motivi di trasparenza e di certezza del diritto, il Dipartimento del Commercio dovrebbe informare la Commissione europea di ogni disposizione legislativa o regolamentare in grado di influire sull'adesione ai principi di Approdo sicuro in materia di riservatezza[54]. Il ricorso ad eccezioni dovrebbe essere attentamente controllato, ed esse non devono essere utilizzate in un modo che comprometta la tutela assicurata dai **principi** in questione[55]. In particolare, l'accesso massiccio da parte delle autorità americane ai dati trattati da imprese auto-certificate Approdo sicuro rischia di pregiudicare la riservatezza delle comunicazioni elettroniche.

7.1. Proporzionalità e necessità

Come risulta dalle conclusioni del Gruppo di lavoro ad hoc UE-USA sulla protezione dei dati, un certo numero di basi giuridiche previste dalla legislazione Americana consente la raccolta e il trattamento su larga scala di dati personali conservati o altrimenti trattati da società ubicate negli Stati Uniti. Fra questi possono esservi dati precedentemente trasferiti dall'UE agli USA nell'ambito di Approdo sicuro, e questo solleva la questione della continuità nell'osservanza dei principi di questo regime. A causa dell'ampia entità dei programmi, può accadere che dati trasferiti nell'ambito di Approdo sicuro siano accessibili alle autorità americane e vengano ulteriormente trattati da queste al di là di quanto è necessario e proporzionato alla protezione della sicurezza nazionale come previsto dall'eccezione di cui alla decisione Approdo sicuro.

7.2. Limitazioni e rimedi

Come risulta dalle conclusioni del Gruppo di lavoro ad hoc UE-USA sulla protezione dei dati, i principali beneficiari delle garanzie previste dal diritto americano sono i cittadini statunitensi o le persone che risiedono legalmente negli USA. Non vi è inoltre alcuna possibilità, né per gli interessati europei che per quelli americani, di ottenere l'accesso, la rettifica o la cancellazione dei dati, o rimedi amministrativi o giurisdizionali in relazione alla raccolta e all'ulteriore trattamento dei loro dati personali nell'ambito dei programmi di controllo statunitensi.

7.3. Trasparenza

Le imprese non indicano sistematicamente, nelle loro politiche in materia di tutela della sfera privata, quando applicano deroghe ai principi. I cittadini e le imprese non sanno quindi che uso viene fatto dei loro dati. Ciò è particolarmente rilevante in relazione al funzionamento dei programmi americani di sorveglianza in questione. Il risultato è che gli interessati europei, i

---

condizione che tali eccezioni o deroghe si applichino in contesti comparabili. Coerentemente con l'obiettivo di una maggiore tutela della sfera privata le organizzazioni devono fare il possibile per attuare detti principi integralmente ed in modo trasparente, specificando nelle rispettive politiche in materia di tutela della sfera privata in quali casi saranno regolarmente applicate le eccezioni ammesse dal punto b). 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."

[54] Parere 4/2000 sul livello di tutela dei dati offerto dai principi dell'"Approdo sicuro", adottato dal Gruppo di lavoro "Articolo 29" sulla protezione dei dati il 16 maggio 2000.

[55] Parere 4/2000 sul livello di tutela dei dati offerto dai principi dell'"Approdo sicuro", adottato dal Gruppo di lavoro "Articolo 29" sulla protezione dei dati il 16 maggio 2000.

cui dati vengono trasferiti a imprese negli USA nell'ambito di Approdo sicuro, possono non venire informati da tali imprese del fatto che le informazioni personali che li riguardano possono essere accessibili[56]. Ciò solleva la questione del rispetto dei principi di trasparenza di Approdo sicuro. Occorre che la trasparenza sia garantita in misura più ampia possibile senza compromettere la sicurezza nazionale. Oltre a dovere, com'è attualmente previsto, indicare nelle loro politiche sulla privacy i casi in cui i principi possono essere limitati da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali, le imprese dovrebbero anche essere incoraggiate a indicare, in dette politiche, i casi in cui applicano eccezioni ai principi per esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia.

8. CONCLUSIONI E RACCOMANDAZIONI

Dalla sua adozione, nel 2000, Approdo sicuro è diventato un veicolo per i flussi di dati personali fra l'UE e gli USA. L'importanza di una protezione efficace in caso di trasferimenti di dati personali è cresciuta dato l'aumento esponenziale dei flussi di dati, fondamentali per l'economia digitale, e gli straordinari sviluppi in materia di raccolta, trattamento e uso delle informazioni. Le imprese del web come Google, Facebook, Microsoft, Apple, Yahoo, contano milioni di clienti in Europa, e trasferiscono dati personali negli USA a fini di trattamento in quantità che nel 2000, all'epoca dell'istituzione di Approdo sicuro, erano inconcepibili.

A causa di carenze a livello di trasparenza e di applicazione dell'accordo, persistono alcune questioni che andrebbero affrontate:

a) trasparenza delle politiche in materia di privacy dei membri di Approdo sicuro;

b) applicazione effettiva dei principi in materia di riservatezza da parte delle imprese negli Stati Uniti, e

c) carattere effettivo dell'applicazione.

Inoltre, l'**accesso su larga scala, da parte dei servizi di intelligence, ai dati trasferiti negli USA da imprese certificate nell'ambito di Approdo sicuro** solleva altri gravi problemi riguardanti la continuità dei diritti dei cittadini europei in materia di protezione in caso di invio dei loro dati negli Stati Uniti.

Alla luce di quanto precede, la Commissione ha formulato le **raccomandazioni** esposte in appresso.

Trasparenza

1. *Le imprese auto-certificate dovrebbero rendere pubbliche le loro politiche di tutela della sfera privata*. Non basta che esse ne forniscano una descrizione al Dipartimento del Commercio. Tali politiche dovrebbero essere rese pubblicamente disponibili sui siti web delle imprese in maniera chiara ed intellegibile

2. *Le politiche di tutela della sfera privata pubblicate sui siti web delle imprese auto-certificate dovrebbero sempre includere un link verso il sito web del Dipartimento del Commercio dedicato ad Approdo sicuro, che elenca tutti i membri "attuali" dell'accordo*. Ciò consentirà agli interessati europei di verificare immediatamente, senza ricerche supplementari, se un'impresa partecipa in quel momento al regime Approdo sicuro. Questo contribuirebbe ad aumentare la credibilità del regime

[56] Informazioni relativamente trasparenti a questo riguardo sono fornite da alcune imprese europee aderenti ad Approdo sicuro. Ad esempio Nokia, che opera negli USA ed è membro di Approdo sicuro, fornisce la seguente nota nella sua politica sulla privacy: "Potremmo essere obbligati per legge a divulgare i Suoi dati personali a determinate autorità o ad altre parti terze, ad esempio ad organismi *di contrasto, nei paesi in cui operiamo o in cui terzi operano per nostro conto."*

riducendo le possibilità che vengano fatte false dichiarazioni di adesione. Il Dipartimento del Commercio ha cominciato a imporre questa condizione alle imprese nel marzo 2013, ma il processo andrebbe intensificato.

3. *Le imprese auto-certificate dovrebbero pubblicare le condizioni di tutela della privacy figuranti in ogni contratto concluso con appaltatori, ad esempio con servizi di cloud-computing*. Il regime Approdo sicuro consente trasferimenti successivi dalle imprese aderenti a terzi che agiscono in qualità di rappresentanti, ad esempio fornitori di cloud service. La nostra interpretazione è che, in questi casi, il Dipartimento del Commercio imponga alle imprese auto-certificate di stipulare un contratto. Tuttavia, l'impresa Approdo sicuro dovrebbe comunque informare il Dipartimento del Commercio della conclusione di tale contratto ed essere obbligata a rendere pubbliche le garanzie in materia di privacy.
4. *Tutte le imprese che non sono membri attuali di Approdo sicuro dovrebbero essere chiaramente segnalate sul sito web del Dipartimento del Commercio.* L'indicazione "Non attuale" nell'elenco dei membri di Approdo sicuro del Dipartimento del Commercio dovrebbe essere accompagnata da un chiaro avvertimento del fatto che attualmente l'impresa in questione non soddisfa le condizioni del regime. Tuttavia, nel caso dell'indicazione "Non attuale", l'impresa è obbligata a continuare ad applicare le condizioni di Approdo sicuro ai dati che ha ricevuto nel quadro del regime.

Ricorsi

5. *Le politiche di tutela della sfera private pubblicate sui siti web delle imprese dovrebbero includere un link che rimandi al prestatore incaricato della risoluzione alternativa delle controversie (ADR) e/o al Comitato UE per la tutela dei dati.* Ciò consentirà agli interessati europei di contattare immediatamente l'organismo ADR o il Comitato UE in caso di problemi. Il Dipartimento del Commercio ha cominciato a imporre questa condizione alle imprese nel marzo 2013, ma il processo andrebbe intensificato.
6. *L'ADR dovrebbe essere di pronto impiego e di costo accessibile*. Per il trattamento delle denunce delle persone fisiche alcuni organismi ADR operanti nel quadro di Approdo sicuro continuano ad applicare onorari (200-250 dollari) che possono essere molto onerosi per un singolo utente. In Europa, invece, il ricorso al Comitato per la tutela dei dati previsto per l'esame delle denunce nel quadro di Approdo sicuro è gratuito.
7. *Il Dipartimento del Commercio dovrebbe controllare più sistematicamente i prestatori di servizi ADR per quanto attiene alla trasparenza e all'accessibilità delle informazioni fornite sulla procedura seguita e sul follow-up delle denunce.* Ciò fa delle procedure ADR un meccanismo efficace, fidato e riuscito. Occorre altresì ribadire che la pubblicazione del verdetto di non-conformità dovrebbe essere inclusa nella gamma di sanzioni obbligatorie applicabili nel contesto ADR.

Applicazione

8. *A seguito della certificazione o del rinnovo Approdo sicuro, una certa percentuale di imprese dovrebbe essere oggetto di indagini d'ufficio per verificare l'effettiva*

osservanza delle loro politiche in materia di privacy (al di là del controllo del rispetto dei requisiti formali).

9. *Ogniqualvolta vi sia stato un verdetto di non-conformità, a seguito di una denuncia o di un'indagine, l'impresa interessata dovrebbe essere oggetto di una specifica inchiesta di follow-up dopo 1 anno.*

10. *In caso di dubbi quanto alla conformità di un'impresa, o in caso di denunce pendenti, il Dipartimento del Commercio dovrebbe informare la competente autorità europea per la protezione dei dati.*

11. *Occorre continuare a esaminare le false dichiarazioni di adesione ad Approdo sicuro.* Un'impresa che dichiara, sul suo sito web, di rispettare le condizioni dell'accordo, ma che non figura nell'elenco del Dipartimento del Commercio come membro "attuale", inganna i consumatori e abusa della loro fiducia. Le false dichiarazioni minano la credibilità del sistema nel suo complesso e dovrebbero quindi essere immediatamente eliminate dai siti web delle imprese.

Accesso da parte delle autorità statunitensi

12. *Nelle loro politiche sulla privacy, le imprese auto-certificate dovrebbero precisare in che misura la legislazione americana consente alle pubbliche autorità di raccogliere e trattare i dati trasferiti nel quadro del regime Approdo sicuro. In particolare, le imprese dovrebbero essere incoraggiate a indicare, in dette politiche, i casi in cui applicano eccezioni ai principi per esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia.*

13. *È importante che l'eccezione per motivi di sicurezza nazionale prevista dalla decisione Approdo sicuro sia applicata solo in misura strettamente necessaria e proporzionata.*