I

(Risoluzioni, raccomandazioni e pareri)

PARERI

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Parere del garante europeo della protezione dei dati sulla relazione finale del Gruppo di contatto ad alto livello UE-USA sulla condivisione delle informazioni e sulla tutela della vita privata e la protezione dei dati di carattere personale

(2009/C 128/01)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 286,

vista la carta dei diritti fondamentali dell'Unione europea, in particolare l'articolo 8,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati,

visto il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, in particolare l'articolo 41,

HA ADOTTATO IL SEGUENTE PARERE:

I. INTRODUZIONE — CONTESTO DEL PARERE

1. In data 28 maggio 2008 la presidenza del Consiglio dell'Unione europea ha annunciato al COREPER, in vista del vertice UE del 12 giugno 2008, che il Gruppo di contatto ad alto livello UE-USA (in appresso «GCAL») sulla condivisione delle informazioni e sulla tutela della vita privata e la protezione dei dati di carattere personale aveva messo a punto la propria relazione. La relazione è stata resa pubblica il 26 giugno 2008 ([1]).

2. La relazione individua principi comuni relativi alla tutela della vita privata e alla protezione dei dati come primo passo verso uno scambio di informazioni con gli Stati Uniti ai fini della lotta al terrorismo ed alle forme gravi di criminalità transnazionale grave.

3. Nel suo annuncio, la presidenza del Consiglio dichiara di accogliere con favore qualsiasi suggerimento sul seguito da riservare alla relazione ed in particolare qualsiasi reazione alle raccomandazioni sui modi di procedere in essa individuati. Il GEPD risponde a tale invito pubblicando il presente parere, fondato sullo stato dei fatti quali resi pubblici e riservandosi la facoltà di modificare la propria posizione alla luce degli ulteriori sviluppi.

4. Il GEPD prende atto che i lavori del GCAL si sono svolti in un contesto caratterizzato, in particolare dopo l'11 settembre 2001, dallo sviluppo dello scambio di dati tra gli USA e l'UE mediante accordi internazionali o altri tipi di strumenti. Tra questi vi sono gli accordi di Europol e Eurojust con gli Stati Uniti, nonché gli accordi PNR ed il caso Swift, che ha condotto ad uno scambio di lettere tra funzionari UE e USA al fine di stabilire garanzie minime di protezione dei dati ([2]).

([1]) Documento del Consiglio n. 9831/08, disponibile su: http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

([2]) — Accordo tra gli Stati Uniti d'America e l'Ufficio europeo di Polizia del 6 dicembre 2001 e accordo supplementare tra gli Stati Uniti d'America e l'Europol sullo scambio di dati personali e di informazioni connesse, pubblicato (in lingua inglese) sul sito web di Europol;
— accordo tra gli Stati Uniti d'America e Eurojust sulla cooperazione giudiziaria, del 6 novembre 2006, pubblicato sul sito web di Eurojust;
— accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) da parte dei vettori aerei al dipartimento per la sicurezza interna degli Stati Uniti (DHS) (Accordo PNR del 2007), firmato a Bruxelles il 23 luglio 2007 e a Washington il 26 luglio 2007, GU L 204 del 4.8.2007, pag. 18;
— scambio di lettere tra le autorità USA e UE sul programma di controllo delle transazioni finanziarie dei terroristi, 28 giugno 2007.

5. Inoltre, l'UE intraprende inoltre negoziati e approva anche strumenti analoghi che prevedono lo scambio di dati personali con altri paesi terzi. Un esempio recente è l'accordo tra l'Unione Europea e l'Australia sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger Name Record — PNR) originari dell'Unione europea da parte dei vettori aerei all'amministrazione doganale australiana ([3]).

6. Da tale contesto emerge che la richiesta di informazioni di carattere personale da parte delle autorità di contrasto di paesi terzi è in costante aumento e si estende anche dalle banche dati governative tradizionali ad altri tipi di archivi, in particolare archivi di dati raccolti dal settore privato.

7. Il GEPD rammenta inoltre un elemento di fondo rilevante, ossia che la questione del trasferimento di dati personali verso paesi terzi nell'ambito della cooperazione di polizia e giudiziaria in materia penale è oggetto della decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale ([4]), la cui adozione è prevista entro la fine del 2008.

8. Si può solo prevedere che tale scambio d'informazioni transatlantico aumenti arrivando ad interessare nuovi settori in cui vengono trattati dati di carattere personale. In tale contesto, un dialogo in materia di «attività di contrasto a livello transatlantico» è al tempo stesso gradito e sensibile: gradito nel senso che potrebbe fornire un quadro più chiaro per gli scambi di dati in corso o previsti, ma anche sensibile poiché tale quadro potrebbe legittimare massicci trasferimenti di dati in un settore, quello delle attività di contrasto, il cui impatto sulle persone fisiche è particolarmente grave e per il quale sono più che mai necessarie garanzie rigorose e affidabili ([5]).

9. Il presente parere intende affrontare nella sezione seguente lo stato attuale dei fatti e i possibili modi di procedere. La sezione III è incentrata sulla portata e la natura di uno strumento che consentirebbe la condivisione delle informazioni. Nella sezione IV il parere analizza, su un piano generale, le questioni giuridiche inerenti al contenuto di un eventuale accordo. Essa affronta altresì questioni quali le condizioni di valutazione del livello di protezione fornito negli Stati Uniti nonché la questione dell'uso del quadro normativo dell'UE come parametro di valutazione di detto livello di protezione. Vi figura inoltre un elenco dei requisiti di base da includere in un tale accordo. Infine, la sezione V presenta un'analisi dei principi in materia di tutela della vita privata allegati alla relazione.

([3]) GU L 213 dell'8.8.2008, pag. 49.

([4]) Decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, versione del 24 giugno 2008 disponibile su http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=it&DosId=193371

([5]) Riguardo alla necessità di un quadro giuridico chiaro, si rimanda alle sezioni III e IV del presente parere.

II. STATO ATTUALE DEI FATTI E POSSIBILI MODI DI PROCEDERE

10. Secondo la valutazione dello stato attuale dei fatti effettuata dal GEPD si sono compiuti progressi verso la definizione di norme comuni in materia di condivisione delle informazioni e di tutela della vita privata e protezione dei dati personali.

11. I lavori preparatori per un qualsiasi tipo di accordo tra l'UE e gli USA non sono tuttavia ancora stati conclusi ed occorre proseguirli. La relazione stessa del GCAL segnala una serie di questioni in sospeso, tra cui quella del «ricorso» è la più rilevante. Permangono disaccordi sulla portata necessaria del ricorso giurisdizionale ([6]). Altre cinque questioni in sospeso sono presentate nel capitolo 3 della relazione. Si deduce inoltre dal presente parere che molte altre questioni restano insolute, come ad esempio la portata e la natura di uno strumento sulla condivisione delle informazioni.

12. Poiché l'opzione auspicata nella relazione è quella di un accordo vincolante — preferenza condivisa dal GEPD — è più che mai necessario procedere con cautela. Occorrono ulteriori preparativi, accurati e approfonditi, prima di poter giungere ad un accordo.

13. Infine, secondo il GEPD la soluzione migliore sarebbe concludere un accordo nel quadro del trattato di Lisbona, ovviamente in funzione della sua entrata in vigore. Esso consentirebbe, in effetti, di scongiurare qualsiasi incertezza giuridica riguardo alla linea di demarcazione tra i pilastri dell'UE. Sarebbero inoltre garantiti il pieno coinvolgimento del Parlamento europeo e il controllo giurisdizionale da parte della Corte di giustizia.

14. In tale contesto, il modo migliore di procedere sarebbe la messa a punto di una tabella di marcia verso un eventuale accordo in una fase successiva. Tale tabella di marcia potrebbe contenere i seguenti elementi:

— orientamenti per il proseguimento dei lavori del gruppo di contatto (o di qualsiasi altro gruppo) e relativo calendario;

— in una fase iniziale, discussione e possibilmente accordo su questioni fondamentali quali la portata e la natura dell'accordo;

— sulla base di un'intesa comune su tali questioni fondamentali, ulteriore elaborazione dei principi di protezione dei dati;

— coinvolgimento dei soggetti interessati in diverse fasi della procedura;

— da parte europea, esame dei vincoli istituzionali.

([6]) Vedasi pagina 5 della relazione, parte C.

III. **PORTATA E NATURA DI UNO STRUMENTO DI CONDIVISIONE DELLE INFORMAZIONI**

15. Secondo il GEPD è fondamentale definire chiaramente la portata e la natura di un eventuale strumento che includa principi di protezione dei dati, in quanto primo passo verso il suo successivo sviluppo.

16. Riguardo alla portata, occorre trovare una risposta ad alcuni importanti quesiti:

— chi sono i soggetti coinvolti all'interno e all'esterno del settore delle attività di contrasto;

— cosa si intende con l'espressione «finalità di contrasto» e qual è il rapporto con altre finalità quali la sicurezza nazionale e più specificamente il controllo delle frontiere e la sanità pubblica;

— come lo strumento si inserirebbe nella prospettiva di uno spazio di sicurezza transatlantico globale.

17. La definizione della natura dello strumento dovrebbe chiarire i seguenti punti:

— se del caso, nell'ambito di quale pilastro lo strumento sarà negoziato;

— se lo strumento avrà carattere vincolante per l'UE e gli USA;

— se avrà efficacia diretta, nel senso che conterrà diritti ed obblighi per le persone fisiche che un'autorità giudiziaria potrà far rispettare;

— se lo strumento stesso consentirà lo scambio di informazioni o stabilirà norme minime per lo scambio di informazioni da integrare con accordi specifici;

— quale sarà il rapporto con gli strumenti esistenti: li rispetterà, li sostituirà o li integrerà?

III. 1. **Portata dello strumento**

Soggetti coinvolti

18. Sebbene la relazione del GCAL non indichi chiaramente la portata precisa del futuro strumento, dai principi in essa menzionati si può evincere che prevede di contemplare sia i trasferimenti tra attori pubblici e privati ([7]) sia quelli tra autorità pubbliche.

([7]) Vedasi in particolare il capitolo 3 della relazione «Questioni in sospeso riguardanti le relazioni transatlantiche», punto 1: «Coerenza degli obblighi di organismi privati durante i trasferimenti di dati».

— Tra attori pubblici e privati

19. Il GEPD ritiene ragionevole applicare un futuro strumento ai trasferimenti tra attori pubblici e privati. Tale strumento si è sviluppato negli ultimi anni in seguito alle richieste di informazioni rivolte dagli USA a soggetti privati. Il GEPD prende atto in effetti che gli attori privati stanno diventando una fonte sistematica di informazioni in una prospettiva di contrasto, sia a livello dell'UE sia a livello internazionale ([8]). Il caso SWIFT ha costituito un precedente importante in cui ad una società privata era stato richiesto di trasmettere sistematicamente blocchi di dati ad autorità di contrasto di uno Stato terzo ([9]). La raccolta di dati PNR provenienti da compagnie aeree segue la medesima logica. Nel suo parere su un progetto di decisione quadro per la creazione di un sistema PNR europeo il GEPD ha già messo in discussione la legittimità di tale tendenza ([10]).

20. Vi sono altri due motivi per considerare con riluttanza l'eventualità di includere trasferimenti tra attori pubblici e privati nell'ambito di un futuro strumento.

21. In primo luogo, tale inclusione potrebbe comportare conseguenze indesiderate all'interno del territorio stesso dell'UE. Il GEPD è gravemente preoccupato per il fatto che, se in linea di principio i dati di società private (quali le istituzioni finanziarie) possono essere trasmessi a paesi terzi, ciò potrebbe provocare forti pressioni al fine di rendere lo stesso tipo di dati ugualmente disponibili alle autorità di contrasto all'interno dell'UE. Il sistema PNR è un esempio di tale sviluppo non gradito, avviato con una raccolta in blocco di dati relativi ai passeggeri da parte degli USA, successivamente applicato anche in ambito interno europeo ([11]), senza che la necessità e la proporzionalità del sistema siano state chiaramente dimostrate.

22. In secondo luogo, nel suo parere relativo alla proposta della Commissione su un sistema PNR europeo, il GEPD ha inoltre sollevato la questione del quadro per la protezione dei dati (primo o terzo pilastro) applicabile alle condizioni della cooperazione tra attori pubblici e privati:

([8]) Vedasi in proposito il parere del GEPD del 20 dicembre 2007 relativo al progetto di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione (Passenger Name Record, PNR) nelle attività di contrasto, GU C 110 dell'1.5.2008, pag. 1. «Tradizionalmente esiste una netta separazione tra attività di contrasto e attività del settore privato, dove i compiti di contrasto sono eseguiti da autorità specificamente preposte, in particolare le forze di polizia, e gli attori privati sono sollecitati caso per caso a comunicare dati personali alle autorità di contrasto. Si registra attualmente una tendenza ad imporre ad attori privati di cooperare sistematicamente per finalità di contrasto».

([9]) Vedasi il parere 10/2006 del Gruppo dell'articolo 29, del 22 novembre 2006, sul trattamento di dati personali da parte della «Society for Worldwide Interbank Financial Telecommunication» (SWIFT), WP 128.

([10]) Parere del 20 dicembre 2007, op. cit.

([11]) Vedasi il progetto di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione (Passenger Name Record, PNR) nelle attività di contrasto, menzionato alla nota in calce 8, attualmente in discussione in sede di Consiglio.

le norme dovrebbero basarsi sulla qualità del responsabile del trattamento dei dati (settore privato) o sulla finalità perseguita (attività di contrasto)? La linea di demarcazione tra il primo ed il terzo pilastro è tutt'altro che chiara in situazioni in cui agli attori privati sono imposti obblighi di trattamento di dati personali a fini di contrasto. In tale contesto, è significativo che nel suo recente parere in merito alla causa sulla conservazione dei dati ([12]) l'avvocato generale Bot abbia proposto una linea di demarcazione per tali situazioni, aggiungendo però: «Tale linea di demarcazione non è sicuramente esente da critiche e può sembrare artificiosa sotto alcuni aspetti.» Il GEPD rileva inoltre che la sentenza della Corte sul PNR ([13]) non fornisce una risposta soddisfacente alla questione del quadro giuridico applicabile. Ad esempio, il fatto che talune attività non siano contemplate dalla direttiva 95/46/CE non implica automaticamente che tali attività possono essere disciplinate nell'ambito del terzo pilastro. Permane di conseguenza un vuoto giuridico riguardo alla legislazione applicabile ed in ogni caso si produce un'incertezza giuridica per quanto riguarda le garanzie legali a disposizione degli interessati.

23. In questa prospettiva il GEPD sottolinea che occorre garantire che un futuro strumento contenente principi generali di protezione dei dati non possa legittimare in quanto tale il trasferimento transatlantico di dati personali tra attori pubblici e privati. Tale trasferimento può essere incluso in un futuro strumento a condizione che:

— lo strumento futuro sancisca che il trasferimento è autorizzato soltanto se ne è comprovata l'assoluta necessità per uno scopo specifico, da decidere caso per caso;

— il trasferimento stesso avvenga in condizioni di elevata garanzia di protezione dei dati (come descritto nel presente parere).

Il GEPD prende atto inoltre dell'incertezza riguardante il quadro applicabile in materia di protezione dei dati ed esorta pertanto, in ogni caso, a non introdurre il trasferimento di dati personali tra attori pubblici e privati nella legislazione UE allo stato attuale.

— Tra autorità pubbliche:

24. L'esatta portata dello scambio di informazioni non è chiara. Come primo passo nella prospettiva dei futuri lavori volti a definire uno strumento comune, occorre chiarire la portata prevista di detto strumento. Restano aperte in particolare le seguenti questioni:

— per quanto riguarda le banche dati situate nell'UE, se lo strumento sia inteso per le banche dati centralizzate (parzialmente) gestite dall'UE, quali le banche dati di Europol e Eurojust, o per le banche dati decentrate gestite dagli Stati membri, o per entrambe;

— se la portata dello strumento si estenda alle reti interconnesse, ossia se le garanzie previste debbano riguardare i dati scambiati tra Stati membri o agenzie sia nell'UE che negli USA;

— se lo strumento riguardi unicamente gli scambi tra banche dati nel settore delle attività di contrasto (polizia, giustizia, eventualmente dogane) o anche altre banche dati, ad esempio quelle fiscali;

— se lo strumento sia collegato anche alle banche dati delle agenzie di sicurezza nazionale o se consenta a tali agenzie l'accesso alle banche dati delle forze di polizia nel territorio dell'altra parte contraente (l'UE per gli USA e viceversa);

— se lo strumento riguardi trasferimenti di informazioni caso per caso o un accesso permanente alle banche dati esistenti. Quest'ultima ipotesi solleverebbe sicuramente questioni di proporzionalità, come illustrato nella sezione V, punto 3.

Finalità di contrasto

25. Anche la definizione delle finalità di un eventuale accordo fa emergere elementi di incertezza. Le finalità di contrasto sono chiaramente indicate nell'introduzione nonché nel primo principio allegato alla relazione e saranno ulteriormente analizzate nella sezione IV del presente parere. Il GEPD rileva già che da tali dichiarazioni risulta che lo scambio di dati riguarderebbe principalmente questioni relative al terzo pilastro, ma ci si potrebbe domandare se questo è solo un primo passo verso un più ampio scambio di informazioni. Sembra chiaro che le finalità di «sicurezza pubblica» dichiarate nella relazione includono la lotta al terrorismo, alla criminalità organizzata e ad altri reati. È però inteso anche a permettere lo scambio di dati per altri interessi pubblici quali eventualmente i rischi per la salute pubblica?

26. Il GEPD raccomanda di restringere le finalità al trattamento di dati identificati con precisione e di giustificare le scelte di politica che conducono a tale definizione.

([12]) Parere dell'avvocato generale Bot del 14 ottobre 2008, Irlanda c/ Parlamento europeo e Consiglio (Causa C301/06), punto 108.

([13]) Sentenza della Corte del 30 maggio 2006, Parlamento europeo c/ Consiglio dell'Unione europea (C-317/04) e Commissione delle Comunità europee (C-318/04), cause riunite C-317/04 e C-318/04, Racc. [2006], pagina I-4721.

Uno spazio di sicurezza transatlantico globale

27. Le grandi linee della suddetta relazione dovrebbero essere inserite nella prospettiva dello spazio di sicurezza transatlantico globale discusso nell'ambito del cosiddetto «Gruppo del futuro» ([14]). La sua relazione, pubblicata nel giugno 2008, pone l'accento sulla dimensione esterna della politica in materia di affari interni. Essa sostiene che *entro il 2014 l'Unione europea dovrebbe prendere una decisione sull'obiettivo politico di realizzare un'area di cooperazione euro-atlantica con gli Stati Uniti nel settore della libertà, della sicurezza e della giustizia.* Tale cooperazione andrebbe al di là della sicurezza in senso stretto e includerebbe almeno le tematiche trattate nell'attuale titolo IV del trattato CE quali immigrazione, visti, asilo e cooperazione in materia di diritto civile. Ci si deve domandare fino a che punto un accordo sui principi di base in materia di protezione dei dati, come quelli menzionati nella relazione del GCAL, possa e debba essere la base per uno scambio di informazioni in un settore così ampio.

28. Normalmente, entro il 2014 la struttura a pilastri non esisterà più e ci sarà una sola base giuridica per la protezione dei dati all'interno dell'UE (ai sensi del trattato di Lisbona, l'articolo 16 del trattato sul funzionamento dell'Unione europea). Tuttavia, il fatto che la *regolamentazione* della protezione dei dati sia armonizzata a livello dell'UE non implica che eventuali accordi con paesi terzi possano permettere il *trasferimento* di qualsiasi dato personale, a prescindere dalle finalità. A seconda del contesto e delle condizioni del trattamento potrebbe essere necessario adattare le garanzie di protezione dei dati per settori specifici quali le attività di contrasto. Il GEPD raccomanda che si tengano in considerazione le conseguenze delle diverse prospettive nella preparazione di un futuro accordo.

III.2. **Natura dell'accordo**

Il quadro istituzionale europeo

29. Nel breve termine in ogni caso è essenziale determinare nell'ambito di quale pilastro l'accordo sarà negoziato. Ciò è particolarmente necessario a causa del quadro normativo interno per la protezione dei dati che sarà influenzato da tale accordo. Sarà il primo pilastro — sostanzialmente la direttiva 95/46/CE, con il suo specifico regime per il trasferimento di dati verso paesi terzi — o sarà il terzo pilastro, con un regime meno rigido per i trasferimenti verso paesi terzi ([15])?

30. Anche se prevalgono le finalità di contrasto, come già menzionato, la relazione del GCAL cita nondimeno la raccolta di dati di soggetti privati, e le finalità possono anche essere interpretate in senso ampio, al di là della semplice sicurezza e includendo per es. le questioni in materia di immigrazione e controllo delle frontiere, ma anche eventualmente di sanità pubblica. Alla luce di queste incertezze sarebbe altamente preferibile attendere l'armonizzazione dei pilastri ai sensi della normativa UE, come previsto nel trattato di Lisbona, per stabilire chiaramente la base giuridica dei negoziati ed il ruolo preciso delle istituzioni europee, specialmente del Parlamento europeo e della Commissione.

Carattere vincolante dello strumento

31. Si dovrebbe precisare se l'esito delle discussioni condurrà ad un memorandum d'intesa o ad un altro strumento di carattere non vincolante, o se consisterà in un accordo internazionale vincolante.

32. Il GEPD sostiene la preferenza per un accordo vincolante espressa nella relazione. Un accordo ufficiale vincolante è, a suo parere, una condizione preliminare indispensabile per qualsiasi trasferimento di dati al di fuori dell'UE, indipendentemente dalla finalità del trasferimento. Nessun trasferimento di dati verso un paese terzo può avvenire senza condizioni e garanzie adeguate che rientrino in un quadro giuridico specifico (e vincolante). In altre parole, un memorandum d'intesa o un altro strumento non vincolante può essere utile per fornire orientamenti per i negoziati in vista di ulteriori accordi vincolanti, ma non può mai sostituirsi all'esigenza di un accordo vincolante.

Efficacia diretta

33. Le disposizioni dello strumento dovrebbero essere ugualmente vincolanti per gli USA e per l'UE ed i suoi Stati membri.

34. Si dovrebbe inoltre assicurare che le persone fisiche abbiano la facoltà di esercitare i loro diritti, e specialmente di essere risarcite, sulla base dei principi convenuti. Secondo il GEPD questo risultato può essere più facilmente ottenuto se le disposizioni sostanziali dello strumento sono formulate in modo tale da avere efficacia diretta rispetto ai residenti dell'Unione europea e da poter essere invocate dinanzi a un organo giurisdizionale. L'efficacia diretta delle disposizioni dell'accordo internazionale, nonché le condizioni del suo recepimento nel diritto interno, a livello europeo e nazionale, volte ad assicurare l'efficacia delle misure, devono pertanto essere espresse chiaramente nello strumento.

Relazione con altri strumenti

35. Un'altra questione fondamentale è fino a che punto l'accordo sia autonomo o debba essere completato, caso per caso, da ulteriori accordi su scambi di dati specifici. È in effetti opinabile che un solo accordo possa disciplinare in maniera adeguata, con un'unica serie di norme, le molteplici specificità del trattamento dei dati nel terzo pilastro.

([14]) Relazione del Gruppo consultivo informale ad alto livello sul futuro della politica europea in materia di affari interni, «Libertà, sicurezza, vita privata — Affari interni europei in un mondo aperto», del giugno 2008, disponibile su register.consilium.europa.eu

([15]) Cfr. gli articoli 11 e 13 della decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, citata al punto 7 del presente parere.

È ancora più dubbio che possa *permettere*, senza discussioni e garanzie aggiuntive, un'approvazione in bianco di qualsiasi trasferimento di dati personali indipendentemente dallo scopo e dalla natura dei dati in questione. Inoltre, gli accordi con paesi terzi non sono necessariamente permanenti, in quanto possono essere collegati a specifiche minacce, essere soggetti a revisione e a clausole di durata massima. D'altra parte, le norme minime comuni riconosciute in uno strumento vincolante potrebbero facilitare eventuali ulteriori discussioni sul trasferimento di dati personali in relazione ad una specifica banca dati o a determinate operazioni di trattamento.

36. Il GEPD ritiene pertanto preferibile la definizione di una serie minima di criteri di protezione dei dati da completare caso per caso con disposizioni specifiche aggiuntive, come menzionato nella relazione del GCAL, all'alternativa di un accordo a sé stante. Tali disposizioni specifiche aggiuntive sono una condizione preliminare per permettere il trasferimento dei dati in casi particolari. Ciò incoraggerebbe un approccio armonizzato in termini di protezione dei dati.

Applicazione agli strumenti esistenti

37. Si dovrebbe altresì esaminare come un eventuale accordo generale si combinerebbe con gli accordi già esistenti conclusi tra l'UE e gli USA. Si noti che detti accordi non hanno la stessa natura vincolante: vanno menzionati in particolare l'accordo PNR (quello che presenta una maggiore certezza del diritto), gli accordi Europol e Eurojust o lo scambio di lettere con la SWIFT ([16]). Un nuovo quadro generale integrerebbe gli strumenti esistenti o, applicandosi soltanto agli altri futuri scambi di dati personali, li lascerebbe invariati? Secondo il GEPD, la coerenza giuridica richiederebbe una serie di norme armonizzate che si applicherebbe, integrandoli, agli accordi vincolanti, esistenti e futuri, in materia di trasferimento dei dati.

38. L'applicazione dell'accordo generale agli strumenti esistenti avrebbe come vantaggio il rafforzamento del loro carattere vincolante: ciò sarebbe particolarmente bene accolto per gli strumenti che non sono giuridicamente vincolanti, come lo scambio di lettere con la SWIFT, poiché imporrebbe almeno il rispetto di una serie di principi generali in materia di vita privata.

IV. **VALUTAZIONE GIURIDICA GENERALE**

39. La presente sezione intende prendere in esame come debba essere valutato il livello di protezione di un quadro o strumento specifico, inclusa la questione dei parametri da usare e dei requisiti di base necessari.

([16]) Cfr. nota in calce 2.

Livello di protezione adeguato

40. A parere del GEPD dovrebbe essere chiaro che uno dei principali risultati di un futuro strumento sarebbe che il trasferimento di dati personali verso gli Stati Uniti sia subordinato al fatto che le autorità statunitensi possono garantire un livello di protezione adeguato (e viceversa).

41. Il GEPD ritiene che soltanto una verifica dell'effettiva adeguatezza assicurerebbe garanzie sufficienti per quanto riguarda il livello di protezione dei dati personali. A suo avviso un accordo quadro generale con un campo di applicazione ampio come quello della relazione del GCAL avrebbe difficoltà a superare, in quanto tale, una verifica dell'effettiva adeguatezza. L'adeguatezza dell'accordo generale potrebbe essere riconosciuta soltanto se associata con l'adeguatezza degli accordi specifici conclusi caso per caso.

42. La valutazione del livello di protezione fornito da paesi terzi non è un esercizio insolito, in particolare per la Commissione europea: nell'ambito del primo pilastro l'adeguatezza è un requisito in materia di trasferimenti. È stata misurata in varie occasioni ai sensi dell'articolo 25 della direttiva 95/46/CE sulla base di criteri specifici e confermata da decisioni della Commissione europea ([17]). Nell'ambito del terzo pilastro tale sistema non è esplicitamente previsto: la stima dell'adeguatezza della protezione è prescritta soltanto nella situazione specifica degli articoli 11 e 13 della decisione quadro sulla protezione dei dati personali ([18]) — non ancora adottata — ed è lasciata agli Stati membri.

43. Nel caso presente la portata dell'esercizio concerne le finalità di contrasto: le discussioni sono condotte dalla Commissione sotto la supervisione del Consiglio. Il contesto è diverso dalla valutazione dei principi di approdo sicuro o dall'adeguatezza della legislazione canadese e si ricollega maggiormente ai recenti negoziati PNR con gli USA e l'Australia che si sono svolti in un quadro giuridico che rientra nel terzo pilastro. Tuttavia, i principi del GCAL sono stati menzionati anche nel contesto del Programma «Viaggio senza visto», che riguarda le frontiere e l'immigrazione e quindi questioni del primo pilastro.

44. Il GEPD raccomanda che qualsiasi constatazione dell'adeguatezza nell'ambito di un futuro strumento dovrebbe basarsi su esperienze in questi diversi settori. Raccomanda altresì l'ulteriore sviluppo della nozione di «adeguatezza» nel contesto di un futuro strumento, sulla base di

([17]) Le decisioni della Commissione sull'adeguatezza della protezione dei dati personali nei paesi terzi, inclusi Argentina, Canada, Svizzera, Stati Uniti, Guernsey, isola di Man e Jersey sono disponibili su http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

([18]) Limitata al trasferimento ad un paese terzo o a un organismo internazionale da parte di uno Stato membro dei dati ricevuti da un'autorità competente in un altro Stato membro.

criteri simili utilizzati in precedenti esercizi di determinazione dell'adeguatezza.

Reciproco riconoscimento — reciprocità

45. Un secondo elemento del livello di protezione si riferisce al riconoscimento reciproco dei sistemi dell'UE e degli USA. La relazione del GCAL menziona al riguardo che l'obiettivo sarebbe quello di ottenere il riconoscimento dell'efficacia dei rispettivi sistemi di protezione dei dati e di tutela della vita privata per i settori interessati da tali principi ([19]), e raggiungere un'applicazione equivalente e reciproca del diritto in materia di protezione dei dati personali e di tutela della vita privata.

46. Per il GEPD è ovvio che il reciproco riconoscimento (o la reciprocità) è possibile soltanto se viene garantito un livello di protezione adeguato. In altre parole, il futuro strumento dovrebbe armonizzare il livello minimo di protezione (tramite una constatazione dell'adeguatezza, tenendo conto della necessità di accordi specifici caso per caso). Soltanto in base a questa condizione preliminare potrebbe essere riconosciuta la reciprocità.

47. Il primo elemento da considerare è la reciprocità delle disposizioni sostanziali sulla protezione dei dati. Secondo il GEPD un accordo dovrebbe contemplare il concetto della reciprocità delle disposizioni sostanziali sulla protezione dei dati in maniera da assicurare, da una parte, che il trattamento dei dati all'interno del territorio dell'UE (e degli USA) rispetti pienamente le leggi nazionali sulla protezione dei dati e, dall'altra, che il trattamento al di fuori del paese di origine dei dati che rientra nel campo di applicazione dell'accordo rispetti i principi della protezione dei dati previsti nell'accordo.

48. Il secondo elemento è la reciprocità dei meccanismi di riparazione. Si dovrebbe garantire che i cittadini europei abbiano mezzi di riparazione adeguati quando i dati che li riguardano sono trattati negli Stati Uniti (indipendentemente dal diritto applicabile al trattamento), ma anche che l'Unione europea ed i suoi Stati membri garantiscano diritti equivalenti ai cittadini statunitensi.

49. Il terzo elemento è la reciprocità dell'accesso ai dati personali da parte delle autorità di contrasto. Se uno strumento permette alle autorità degli Stati Uniti di accedere a dati che provengono dall'Unione europea, la reciprocità implicherebbe che lo stesso accesso dovrebbe essere fornito alle autorità dell'UE per quanto riguarda i dati provenienti dagli USA. La reciprocità non deve danneggiare l'efficacia della protezione degli interessati. È una condizione preliminare per consentire l'accesso «transatlantico» da parte delle autorità di contrasto. Questo significa, in termini concreti, che:

— l'accesso diretto ai dati all'interno del territorio dell'UE da parte delle autorità statunitensi (e viceversa) non dovrebbe essere permesso. L'accesso dovrebbe essere consentito soltanto su base indiretta nell'ambito di un sistema «push»;

— tale accesso dovrebbe avvenire sotto il controllo delle autorità preposte alla protezione dei dati e delle autorità giudiziarie nel paese in cui ha luogo il trattamento dei dati;

— l'accesso da parte delle autorità statunitensi alle banche dati situate all'interno dell'UE dovrebbe rispettare le disposizioni sostanziali in materia di protezione dei dati (vedi sopra) ed assicurare la piena riparazione per gli interessati.

Precisione dello strumento

50. La specificazione delle condizioni della valutazione (adeguatezza, equivalenza, riconoscimento reciproco) è essenziale poiché determina il contenuto, in termini di precisione, certezza del diritto ed efficacia della protezione. Il contenuto di un futuro strumento deve essere preciso ed accurato.

51. Inoltre, dovrebbe essere chiaro che qualsiasi accordo specifico concluso in una fase ulteriore dovrà pur sempre prevedere garanzie di protezione dei dati dettagliate e complete in relazione all'interessato dello scambio di dati previsto. Soltanto un tale doppio livello di principi concreti di protezione dei dati assicurerebbe la perfetta corrispondenza necessaria tra l'accordo generale e gli accordi specifici, come già osservato ai punti 35 e 36 del presente parere.

Sviluppo di un modello per gli altri paesi terzi

52. La misura in cui un accordo con gli USA potrebbe essere un modello per gli altri paesi terzi merita particolare attenzione. Il GEPD rileva che, oltre agli USA, la suddetta relazione del «Gruppo del futuro» indica anche la Russia quale partner strategico dell'UE. Nella misura in cui i principi sono neutri e conformi alle fondamentali garanzie dell'UE, possono costituire un utile precedente. Tuttavia, le specificità inerenti per es. al quadro giuridico del paese destinatario o allo scopo del trasferimento impedirebbe il semplice recepimento dell'accordo. Ugualmente decisiva sarà la situazione democratica dei paesi terzi: si dovrebbe assicurare che i principi concordati siano effettivamente garantiti e attuati nel paese destinatario.

Quali parametri per valutare il livello di protezione?

53. Un'adeguatezza implicita o esplicita dovrebbe comunque conformarsi al quadro giuridico europeo ed internazionale

([19]) Capitolo A. Accordo internazionale vincolante, pag. 8.

e specialmente alle garanzie di protezione dei dati comunemente convenute. Queste sono sancite nelle linee guida delle Nazioni Unite, nella convenzione 108 del Consiglio d'Europa e nel relativo protocollo addizionale, nelle linee guida dell'OCSE e nel progetto di decisione quadro sulla protezione dei dati personali, nonché, per gli aspetti del primo pilastro, nella direttiva 95/46/CE ([20]). Tutti questi strumenti contengono principi simili che sono più ampiamente riconosciuti come l'essenza stessa della protezione dei dati personali.

54. È ancora più importante che i principi succitati siano debitamente tenuti in conto considerato l'impatto di un potenziale accordo come quello previsto dalla relazione del GCAL. Uno strumento che tratti tutto il settore dell'*applicazione* di un paese terzo sarebbe in effetti una situazione senza precedenti. Le decisioni in materia di adeguatezza esistenti nel primo pilastro, e gli accordi conclusi con i paesi terzi nell'ambito del terzo pilastro dell'UE (Europol, Eurojust) sono sempre stati collegati con uno specifico trasferimento di dati, mentre in questo caso potrebbero essere resi possibili trasferimenti con un campo di applicazione molto più ampio, considerati l'ampio scopo perseguito (la lotta ai reati, la sicurezza nazionale e pubblica, l'esecuzione alle frontiere) e il numero sconosciuto di banche dati interessate.

Requisiti fondamentali

55. Le condizioni da soddisfare nel contesto del trasferimento di dati personali verso paesi terzi sono state sviluppate in un documento di lavoro del Gruppo dell'articolo 29 ([21]). Qualsiasi accordo su principi minimi in materia di vita privata dovrebbe soddisfare una verifica di conformità che assicuri l'efficacia delle garanzie di protezione dei dati.

— Per quanto riguarda la sostanza, i principi in materia di protezione dei dati dovrebbero prevedere un elevato livello di protezione e soddisfare standard in linea con i principi UE. I 12 principi inclusi nella relazione del GCAL saranno ulteriormente analizzati in questa prospettiva nel capitolo V del presente parere.

— Per quanto riguarda la specificità, a seconda della natura dell'accordo, e specialmente se esso costituisce un accordo internazionale ufficiale, le norme e le procedure dovrebbero essere sufficientemente dettagliate, in modo da permettere un'attuazione efficace.

— Per quanto riguarda la sorveglianza, per assicurare la conformità con le norme convenute, dovrebbero essere attuati specifici meccanismi di controllo, a livello sia interno (audit) sia esterno (revisioni). Questi meccanismi devono essere ugualmente disponibili per entrambe le parti dell'accordo. La sorveglianza include meccanismi per assicurare la conformità a livello generale come i meccanismi congiunti di revisione, nonché la conformità a livello particolare, come i ricorsi individuali.

56. Oltre a questi tre requisiti di base, dovrebbe essere attribuita particolare attenzione alle specificità collegate con il trattamento dei dati personali in un contesto di applicazione della legge. Questo è in effetti un settore in cui i diritti fondamentali possono subire talune restrizioni. Dovrebbero pertanto essere adottate garanzie per compensare la restrizione dei diritti della persona, specialmente riguardo agli aspetti seguenti, a motivo dell'impatto sulla persona:

— Trasparenza: le informazioni e l'accesso ai dati personali potrebbero essere limitati in un contesto di attività di contrasto, a causa ad esempio delle esigenze connesse ad indagini discrete. Mentre all'interno dell'UE sono tradizionalmente attuati meccanismi aggiuntivi per compensare questa limitazione dei diritti fondamentali (spesso coinvolgendo autorità per la protezione dei dati indipendenti), occorre assicurare che meccanismi di compensazione simili saranno disponibili dopo il trasferimento delle informazioni ad un paese terzo.

— Ricorso: per i motivi succitati, le persone dovrebbero beneficiare di possibilità alternative di difesa dei propri diritti, in particolare tramite un'autorità di controllo indipendente e dinanzi a un organo giurisdizionale.

— Conservazione dei dati: la motivazione per il periodo di conservazione potrebbe non essere trasparente. Devono essere prese misure intese affinché ciò non osti a un effettivo esercizio dei diritti da parte delle persone interessate o delle autorità di controllo.

([20]) — Linee guida delle Nazioni Unite per la regolamentazione degli archivi informatici contenenti dati personali, adottate dall'Assemblea Generale il 14 dicembre 1990, disponibili su www.unhchr.ch/html/menu3/b/71.htm
— convenzione sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale del Consiglio d'Europa, del 28 gennaio 1981, disponibile su www.conventions.coe.int/treaty/en/Treaties/html/108.htm
— linee guida dell'OCSE sulla protezione della vita privata e dei flussi transfrontalieri di dati personali, adottate il 23 settembre 1980, disponibili su www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, disponibile su http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=it&DosId=193371
— direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. GU L 281 del 23.11.1995, pag. 31.

([21]) Documento di lavoro del 24 luglio 1998 sui trasferimenti di dati personali a paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati; WP 12.

— Responsabilità delle autorità di contrasto: se manca un'effettiva trasparenza, i meccanismi di controllo da parte dei soggetti interessati a livello individuale o istituzionale non possono in alcun modo essere esaurienti. In considerazione della sensibilità dei dati e delle misure vincolanti che possono essere prese contro i singoli in base al trattamento dei dati, sarebbe ancora fondamentale che tali controlli poggiassero su una base stabile. La responsabilità è un elemento decisivo nell'ambito meccanismi di controllo nazionale del paese destinatario, ma anche in considerazione delle possibilità di revisione da parte del paese o della regione di origine dei dati. Tali meccanismi di revisione sono previsti in accordi specifici quali l'accordo PNR, e il GEPD raccomanda insistentemente di includerli anche in uno strumento generale.

V. **ANALISI DEI PRINCIPI**

Introduzione

57. La presente sezione analizza i 12 principi riportati nel documento del GCAL nella prospettiva seguente:

— Si constata che gli USA e l'UE hanno alcuni approcci comuni a livello dei principi, poiché si possono riscontrare analogie con i principi della convenzione 108.

— Un accordo a livello dei principi non è tuttavia sufficiente. Uno strumento giuridico dovrebbe essere abbastanza incisivo da assicurare l'osservanza.

— Il GEPD deplora che i principi non siano corredati di un promemoria esplicativo.

— Prima di soffermarsi sulla descrizione dei principi dovrebbe risultare chiaro che entrambe le parti interpretano allo stesso modo i termini usati, per esempio per quanto riguarda la nozione di informazione personale o di persone protette. Sarebbero auspicabili definizioni in tal senso.

1. Definizione della finalità

58. In base al primo principio elencato nell'allegato della relazione del GCAL le informazioni personali sono trattate a fini legittimi di contrasto. Come indicato sopra ciò si riferisce, per l'Unione europea, alla prevenzione, all'accertamento, all'investigazione e al perseguimento dei reati. Tuttavia per gli USA l'interpretazione delle attività di contrasto va oltre i reati penali e include «finalità di esecuzione alle frontiere, sicurezza pubblica e sicurezza nazionale». Le conseguenze di questo divario tra le finalità dichiarate dall'UE e dagli USA non sono chiare. Se la relazione indica che in pratica le finalità possono in ampia misura coincidere, rimane decisivo sapere precisamente in quale misura essi *non* coincidono. Nell'ambito delle attività di contrasto, in considerazione delle conseguenze delle misure adottate per i singoli, il principio della limitazione della finalità deve essere rigorosamente rispettato e le finalità devono essere chiare e circoscritte. Tenendo conto della reciprocità prevista nella relazione, sembra essenziale anche il ravvicinamento di tali finalità. In sintesi, è necessario chiarire in che modo va inteso tale principio.

2. Integrità/qualità dei dati

59. Il GEPD si compiace della disposizione secondo cui ai fini di un trattamento legittimo sono necessarie informazioni personali precise, pertinenti, tempestive e complete. Questo principio è un presupposto fondamentale per un efficace trattamento dei dati.

3. Necessità/proporzionalità

60. Il principio crea un chiaro collegamento tra le informazioni raccolte e la necessità di tali informazioni per rispondere a una finalità di contrasto prevista dalla legge. Questo requisito di una base legislativa è un elemento positivo per accertare la legittimità del trattamento. Il GEPD rileva tuttavia che, benché in tal modo sia rafforzata la certezza giuridica del trattamento, la base giuridica di tale trattamento consiste nella legge di un paese terzo. La legge di un paese terzo non può di per sé costituire una base legittima per un trasferimento di dati personali ([22]). Nel contesto della relazione del GCAL sembra scontato che la legittimità della normativa di un paese terzo, ossia degli Stati Uniti, è riconosciuta in linea di massima. Si dovrebbe tenere presente che, se tale ragionamento è giustificato in questo contesto, dato che gli Stati Uniti sono uno paese democratico, lo stesso sistema non sarebbe valido e non potrebbe essere trasposto alle relazioni con altri paesi terzi.

61. Qualsiasi trasferimento di dati personali deve essere pertinente, necessario e appropriato conformemente all'allegato alla relazione del GCAL. Il GEPD sottolinea che per essere proporzionato, il trattamento non deve essere indebitamente intrusivo e le modalità del trattamento devono essere equilibrate, tenendo conto dei diritti e degli interessi delle persone interessate.

62. Per tale motivo l'accesso alle informazioni dovrebbe avvenire caso per caso, in funzione delle esigenze pratiche nel contesto di indagini specifiche. Un accesso permanente da parte di autorità di contrasto di paesi terzi alle basi dati situate nell'UE sarebbe considerato sproporzionato e insufficientemente giustificato. Il GEPD ricorda che anche nel contesto degli accordi esistenti in materia di scambio di dati, ad esempio nel caso dell'accordo PNR, lo

([22]) Cfr. in particolare l'articolo 7, lettere c) ed e) della direttiva 95/46/CE. Nel suo parere 6/2002 del 24 ottobre 2002 sulla trasmissione di informazioni APIS e di altri dati dalle linee aeree agli Stati Uniti, il gruppo «Articolo 29» ha dichiarato che non sembra accettabile che una decisione unilaterale presa da un paese terzo per motivi inerenti al suo interesse pubblico debba portare al trasferimento di routine e massiccio di dati protetti in virtù della direttiva.

scambio di dati si basa su circostanze specifiche ed è previsto per un periodo di tempo limitato ([23]).

63. Seguendo la stessa logica, il periodo di conservazione dei dati dovrebbe essere disciplinato: i dati dovrebbero essere conservati solo fintantoché sono necessari in considerazione della finalità specifica perseguita. Se non sono più pertinenti in relazione alla finalità definita, dovrebbero essere soppressi. Il GEPD si oppone fermamente alla costituzione di «depositi di dati» in cui sarebbero conservate informazioni su individui non sospettati in previsione di eventuali esigenze future.

4. Sicurezza dell'informazione

64. Nei principi sono indicate le misure e procedure per salvaguardare i dati dagli abusi, dall'alterazione e da altri rischi, assieme a una disposizione che limita l'accesso alle persone autorizzate. Il GEPD ritiene che ciò sia soddisfacente.

65. Il principio potrebbe inoltre essere integrato da una disposizione secondo cui dovrebbero essere conservate le registrazioni sulle persone che accedono ai dati. Ciò rafforzerebbe l'efficacia delle garanzie intese a limitare l'accesso e impedire l'abuso dei dati.

66. Dovrebbe inoltre essere prevista l'informazione reciproca in caso di violazione della sicurezza: i destinatari negli USA e nell'UE sarebbero responsabili per l'informazione delle rispettive controparti in caso di divulgazione illecita dei dati. Ciò contribuirebbe a una maggiore responsabilità in vista di un trattamento sicuro dei dati.

5. Categorie particolari di informazioni personali

67. La portata del principio che vieta il trattamento di dati sensibili è secondo il GEPD considerevolmente limitata dall'eccezione che consente qualsiasi trattamento di dati sensibili per i quali la legge nazionale prevede «garanzie appropriate». Proprio a causa del carattere sensibile dei dati, qualsiasi deroga al principio del divieto deve essere motivata adeguatamente e precisamente, con un elenco di finalità e circostanze in cui un tipo determinato di dati sensibili può essere trattato, nonché con un'indicazione della qualità dei responsabili autorizzati a trattare detti tipi di dati. Tra le garanzie da adottare, il GEPD ritiene che i dati sensibili non dovrebbero in quanto tali costituire un elemento che può determinare un'indagine. Potrebbero essere disponibili in circostanze specifiche, ma solo quale informazione aggiuntiva per quanto riguarda una persona interessata oggetto di indagini. Queste garanzie e condizioni devono essere enumerate in modo limitativo nel testo che descrive il principio.

6. Responsabilità

68. Come illustrato nei punti 55-56 del presente parere, la responsabilità degli enti pubblici che trattano dati personali deve essere assicurata in modo efficace e nell'accordo devono essere fornite garanzie sul modo in cui sarà assicurata tale responsabilità. Ciò è tanto più importante in considerazione della mancanza di trasparenza tradizionalmente associata al trattamento dei dati personali nell'ambito delle attività di contrasto. In questo contesto il fatto di menzionare — come avviene nell'allegato — che gli enti pubblici sono responsabili senza fornire altre spiegazioni sulle modalità e conseguenze di tale responsabilità, non è una garanzia soddisfacente. Il GEPD raccomanda che tale spiegazione sia fornita nel testo dello strumento.

7. Vigilanza indipendente ed efficace

69. Il GEPD sostiene appieno l'inserimento di una disposizione che garantisca una vigilanza indipendente ed efficace, da parte di una o più autorità di supervisione. Ritiene che occorra precisare come va interpretata l'indipendenza, indicando in particolare da chi sono indipendenti dette autorità e a chi devono riferire. A tal fine sono necessari criteri che dovrebbero tener conto dell'indipendenza istituzionale e funzionale in relazione agli organismi esecutivi e legislativi. Il GEPD ricorda che si tratta di un elemento essenziale per assicurare l'effettivo rispetto dei principi concordati. Anche i poteri di intervento e contrasto di tali autorità sono fondamentali riguardo alla questione della responsabilità degli enti pubblici che trattano dati personali, come indicato sopra. La loro esistenza e le loro competenze dovrebbero essere rese chiaramente visibili ai soggetti interessati affinché siano in grado di esercitare i propri diritti, in particolare se sono competenti varie autorità in funzione del contesto del trattamento.

70. Il GEPD raccomanda inoltre che un futuro accordo preveda anche meccanismi di cooperazione tra le autorità di contrasto.

8. Accesso e rettifica a livello individuale

71. Sono necessarie garanzie specifiche per quanto riguarda l'accesso e la rettifica nel contesto delle attività di contrasto. In tal senso il GEPD si compiace del principio secondo cui alle persone deve/dovrebbe essere offerto l'accesso e la possibilità di chiedere «la rettifica e/o la cancellazione delle loro informazioni personali». Rimangono tuttavia alcune incertezze per quanto riguarda la definizione di persone (dovrebbero essere protette tutte le persone interessate e non solo i cittadini del paese interessato) e sulle condizioni in cui le persone possono essere autorizzate a opporsi al trattamento delle loro informazioni. Sono necessarie precisazioni sui «casi appropriati» in cui è possibile o

([23]) L'accordo scadrà e cesserà di avere effetto sette anni dopo la data della firma, a meno che le parti non convengano reciprocamente di sostituirlo.

non è possibile opporsi. Per le persone interessate dovrebbe essere chiaro in quali circostanze — in funzione, per esempio, del tipo di autorità, del tipo di investigazione o altri criteri — avranno la facoltà di esercitare i loro diritti.

72. Inoltre, se vi sono motivi giustificati per non concedere la possibilità diretta di opporsi a un trattamento, dovrebbe essere disponibile una verifica indiretta, tramite l'autorità indipendente responsabile della vigilanza sul trattamento.

9. Trasparenza e segnalazione

73. Il GEPD torna a sottolineare l'importanza di un'effettiva trasparenza, affinché le persone possano esercitare i propri diritti e contribuire alla responsabilità generale delle autorità pubbliche che trattano dati personali. Sostiene i principi quali sono stati formulati e insiste in particolare sulla necessità di una segnalazione generale e individuale alla persona interessata. Ciò è rispecchiato nel principio formulato al punto 9 dell'allegato.

74. Tuttavia la relazione nel relativo capitolo 2, parte A. B («Principi convenuti») indica che negli USA la trasparenza può includere singolarmente o in combinazione, la pubblicazione nel registro federale, la segnalazione individuale e la divulgazione nei procedimenti giudiziari. Va chiarito che la pubblicazione in una gazzetta ufficiale non è di per sé sufficiente a garantire l'appropriata informazione del soggetto interessato. Oltre alla necessità di una segnalazione individuale, il GEPD ricorda che tutte le informazioni devono essere fornite in un linguaggio facilmente comprensibile per la persona interessata.

10. Procedure di ricorso

75. Per garantire l'effettivo esercizio dei propri diritti, le persone devono poter presentare un reclamo dinanzi a un'autorità indipendente preposta alla protezione dei dati, nonché un ricorso dinanzi a un giudice imparziale. Entrambe le possibilità di ricorso dovrebbero essere ugualmente disponibili.

76. L'accesso a un'autorità indipendente preposta alla protezione dei dati è necessario in quanto offre un'assistenza flessibile e meno costosa in un contesto — le attività di contrasto — piuttosto opaco per i cittadini. Le autorità preposte alla protezione dei dati possono altresì prestare assistenza nell'esercitare diritti di accesso a nome di persone interessate in caso di eccezioni che impediscono a queste ultime di accedere direttamente ai loro dati personali.

77. L'accesso al sistema giudiziario è una garanzia addizionale e indispensabile che le persone interessate possano presentare ricorso dinanzi a un'autorità appartenente a un settore del sistema democratico distinto dalle istituzioni pubbliche che trattano effettivamente i loro dati. L'esistenza di un siffatto rimedio effettivo dinanzi a un giudice è stata ritenuta dalla Corte di giustizia europea [24] «essenziale per assicurare al singolo la tutela effettiva del suo diritto. (...) [Essa] costituisce espressione di un principio generale di diritto comunitario su cui sono basate le tradizioni costituzionali comuni agli Stati membri e che è stato sancito dagli articoli 6 e 13 della Convenzione europea dei diritti dell'uomo.» L'esistenza di un ricorso giurisdizionale è altresì prevista esplicitamente dall'articolo 47 della Carta dei diritti fondamentali dell'Unione europea e dall'articolo 22 della direttiva 95/46/CE, fatta salva la possibilità di un ricorso amministrativo.

11. Decisioni individuali automatizzate

78. Il GEPD si compiace della disposizione che prevede garanzie appropriate in caso di trattamento automatizzato delle informazioni personali. Rileva che un'interpretazione comune della nozione di «azione che comporti un danno significativo nei confronti dei pertinenti interessi del singolo» chiarirebbe le condizioni di applicazione di questo principio.

12. Trasferimenti successivi

79. Le condizioni previste per i trasferimenti successivi sono talvolta poco chiare. In particolare, qualora il trasferimento successivo debba avvenire nel rispetto di accordi e intese internazionali tra il paese di invio e i paesi destinatari, dovrebbe essere precisato se si tratta di accordi tra i due paesi che hanno posto in atto il primo trasferimento o tra i due paesi coinvolti nel trasferimento successivo. Secondo il GEPD sono comunque necessari accordi tra i due paesi che hanno posto in atto il primo trasferimento.

80. Il GEPD constata anche una definizione molto ampia della nozione di «legittimi interessi pubblici» che consentono un trasferimento successivo. La portata della sicurezza pubblica rimane poco chiara e il prolungamento della possibilità di effettuare trasferimenti in caso di violazioni della deontologia o delle condizioni applicabili alle professioni regolamentate sembra ingiustificato ed eccessivo nel contesto delle attività di contrasto.

VI. **CONCLUSIONE**

81. Il GEPD si compiace dei lavori congiunti svolti dalle autorità dell'UE e degli USA nell'ambito delle attività di contrasto in cui la protezione dei dati riveste un'importanza fondamentale. Insiste tuttavia sul fatto che la tematica è complessa, in particolare per quanto riguarda la sua portata e natura precise, e che richiede pertanto un'analisi accurata e approfondita. L'impatto di uno strumento transatlantico

[24] Causa 222/84 *Johnston* [1986] Racc. 1651; Causa 222/86 *Heylens* [1987] Racc. 4097; Causa C-97/91 *Borelli* [1992] Racc. I-6313.

sulla protezione dei dati dovrebbe essere esaminato attentamente in relazione al quadro giuridico vigente e alle conseguenze per i cittadini.

82. Il GEPD chiede maggiore chiarezza e disposizioni concrete in particolare sugli aspetti seguenti:

— precisazioni in merito alla natura dello strumento, che dovrebbe essere giuridicamente vincolante per garantire una sufficiente sicurezza giuridica;

— una valutazione approfondita dell'adeguatezza, basata su requisiti essenziali incentrati sugli aspetti del sistema attinenti al contenuto, al carattere specifico e alla vigilanza. Il GEPD ritiene che l'adeguatezza dello strumento generale potrebbe essere riconosciuta soltanto se combinata con adeguati accordi specifici conclusi caso per caso;

— un campo d'applicazione circoscritto, con una chiara definizione comune delle finalità di contrasto pertinenti;

— precisazioni circa le modalità secondo le quali gli organismi privati possono essere coinvolti nei sistemi di trasferimento dei dati;

— rispetto del principio di proporzionalità, il che comporta lo scambio di dati caso per caso in presenza di una necessità concreta;

— efficaci meccanismi di vigilanza e meccanismi di ricorso disponibili ai soggetti interessati, compresi mezzi di ricorso amministrativi e giudiziari;

— efficaci misure che garantiscano l'esercizio dei propri diritti a tutte le persone interessate, a prescindere dalla loro nazionalità;

— coinvolgimento di autorità indipendenti preposte alla protezione dei dati, in particolare per quanto riguarda la vigilanza e l'assistenza ai soggetti interessati.

83. Il GEPD insiste sul fatto che nell'elaborazione dei principi occorrerebbe evitare un modo di procedere affrettato che produrrebbe solo soluzioni insoddisfacenti, con effetti contrari a quelli ricercati in termini di protezione dei dati. A questo punto la migliore via da seguire sarebbe pertanto la messa a punto di una tabella di marcia in vista di un eventuale accordo in una fase successiva.

84. Il GEPD invita inoltre a introdurre una maggiore trasparenza per quanto riguarda il processo di elaborazione dei principi per la protezione dei dati. Solo con la partecipazione di tutti i soggetti interessati, compreso il Parlamento europeo, lo strumento potrà beneficiare di un dibattito democratico e ottenere il necessario sostegno e riconoscimento.

Fatto a Bruxelles, 11 novembre 2008

Peter HUSTINX

Garante europeo della protezione dei dati