Parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo «Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini»

(2009/C 276/02)

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

1. Il 10 giugno 2009 la Commissione ha adottato la comunicazione al Parlamento europeo e al Consiglio dal titolo «Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini» ([1]). Conformemente all'articolo 41 del regolamento (CE) n. 45/2001, il GEPD presenta il seguente parere.

2. Prima di adottare la comunicazione, la Commissione ha consultato in maniera informale il GEPD con lettera datata 19 maggio 2009. In risposta a tale richiesta, il 20 maggio 2009 il GEPD ha inviato osservazioni informarli intese a migliorare ulteriormente il testo della comunicazione e ha inoltre contribuito attivamente alla lettera del Gruppo «Polizia e giustizia», del 14 gennaio 2009, sul programma pluriennale per lo spazio di libertà, sicurezza e giustizia ([2]).

3. La comunicazione (punto 1) sottolinea che l'Unione «deve dotarsi di un nuovo programma pluriennale che, partendo dai progressi realizzati e traendo insegnamento dalle attuali carenze, si proietti nel futuro con ambizione. Il programma dovrà definire le priorità dei prossimi cinque anni». Questo programma pluriennale (già noto come «programma di Stoccolma») costituirà il seguito dei programmi di Tampere e dell'Aia, che hanno dato un forte impulso politico allo spazio di libertà, sicurezza e giustizia.

4. La comunicazione servirà da base per il nuovo programma pluriennale. Il GEPD rileva al riguardo che i programmi pluriennali, pur non essendo in quanto tali strumenti vincolanti, hanno un notevole impatto sulla politica che sarà attuata dalle istituzioni nel settore in questione, dato che molti degli interventi concreti, legislativi e non, trarranno origine dal programma.

5. La comunicazione stessa va vista in tale prospettiva. È il prossimo passo di un processo praticamente iniziato con le due relazioni presentate nel giugno 2008 dai cosiddetti «Gruppi sul futuro», istituiti dalla presidenza del Consiglio allo scopo di fornire idee: «Libertà, sicurezza, vita privata — Affari interni europei in un mondo aperto» ([3]) e «Soluzioni proposte per il futuro programma dell'UE nel settore della giustizia» ([4]).

II. CONTENUTO PRINCIPALE DEL PARERE

6. Il presente parere costituisce non solo una reazione alla comunicazione, ma anche un contributo del GEPD al dibattito più generale sul futuro dello spazio di libertà, sicurezza e giustizia che dovrà portare ad un nuovo programma di lavoro strategico («programma di Stoccolma»), come annunciato dalla presidenza svedese dell'UE ([5]). Il presente parere tratterà anche di alcune conseguenze dell'eventuale entrata in vigore del trattato di Lisbona.

7. Dopo la precisazione, nella terza parte, delle principali prospettive del parere, la quarta parte contiene una valutazione generale della comunicazione.

8. La quinta parte prende in esame la questione di come rispondere all'esigenza di un rispetto costante della tutela della vita privata e della protezione dei dati personali in un contesto di aumento dei relativi scambi. L'attenzione sarà focalizzata sul punto 2.3 della comunicazione, «Protezione dei dati personali e della vita privata» e, più in generale, sulla necessità di ulteriori interventi, di carattere legislativo e non, volti a migliorare il quadro per la protezione dei dati.

([1]) COM(2009) 262 definitivo («la comunicazione»).

([2]) Non pubblicato. Il Gruppo «Polizia e giustizia» (WPPJ) è stato istituito dalla conferenza europea dei commissari per la protezione dei dati affinché prepari le sue posizioni nel settore dell'applicazione della legge e agisca in suo nome in caso di questioni urgenti.

([3]) Documento del Consiglio n. 11657/08. Di seguito «relazione sugli affari interni».

([4]) Documento del Consiglio n. 11549/08 («relazione sulla giustizia»).

([5]) Programma di lavoro dell'UE stilato dal governo, www.regeringen.se

9. La sesta parte riguarda le esigenze e le possibilità di archiviazione, accesso e scambio di informazioni quali strumenti di contrasto ovvero, come dice la comunicazione, per «un'Europa della sicurezza». Il punto 4 della comunicazione contiene una serie di obiettivi sul flusso di informazioni e gli strumenti tecnologici, specie ai punti 4.1.2 (Gestione dell'informazione), 4.1.3 (Mobilitare gli strumenti tecnologici necessari) e 4.2.3.2 (I sistemi di informazione). La messa a punto di un modello europeo d'informazione (punto 4.1.2) può essere considerata la proposta più ambiziosa al riguardo. Nel suo parere il GEPD la analizza in modo approfondito.

10. La settima parte accenna brevemente ad un tema specifico, rilevante ai fini della protezione dei dati, nell'ambito dello spazio di libertà, sicurezza e giustizia, ossia l'accesso alla giustizia e la giustizia elettronica.

III. **PPOSPETTIVE DEL PARERE**

11. Il presente parere farà della necessità di tutelare i diritti fondamentali la prospettiva principale in cui analizzare la comunicazione e, più in generale, il futuro dello spazio di libertà, sicurezza e giustizia quale configurato in un nuovo programma pluriennale. Si baserà inoltre sui contributi forniti dal GEPD allo sviluppo della politica dell'UE in questo settore, specie nella sua veste di consulente. Ad oggi il GEPD ha adottato oltre trenta pareri e osservazioni su iniziative scaturite dal programma dell'Aia, tutti reperibili sul suo sito web.

12. Nel valutare la comunicazione, il GEPD terrà conto in particolare delle seguenti quattro prospettive, importanti per il futuro dello spazio di libertà, sicurezza e giustizia. Tutte e quattro hanno un ruolo chiave anche nella comunicazione.

13. La prima prospettiva è la crescita esponenziale delle informazioni digitali sui cittadini dovuta all'evoluzione delle tecnologie dell'informazione e della comunicazione ([6]). La società si sta trasformando in quella che è spesso definita una «società della sorveglianza», in cui ogni transazione e quasi ogni azione del cittadino possono generare una registrazione digitale. Il cosiddetto «Internet degli oggetti» e l'«intelligenza diffusa» si stanno già sviluppando rapidamente con l'uso delle etichette a radiofrequenza. Sempre più spesso si fa ricorso a caratteristiche digitalizzate del corpo umano (biometria). Ciò porta ad un mondo sempre più connesso in cui le organizzazioni addette alla sicurezza pubblica potranno avere accesso a grandi quantità di informazioni potenzialmente utili, con possibili ripercussioni dirette sulla vita degli interessati.

14. La seconda prospettiva è l'internazionalizzazione. Da un lato, nell'era digitale lo scambio di dati non è circoscritto dalle frontiere esterne dell'Unione europea mentre, dall'altro, vi è un bisogno crescente di cooperazione internazionale in tutte le diverse attività dell'UE nell'ambito dello spazio di libertà, sicurezza e giustizia, di cui la lotta al terrorismo, la cooperazione di polizia e giudiziaria, la giustizia civile e il controllo di frontiera sono solo alcuni esempi.

15. La terza prospettiva è l'utilizzo di dati ai fini dell'applicazione della legge: minacce recenti alla società, connesse o meno con il terrorismo, hanno avuto come conseguenza (la richiesta di) maggiori possibilità per le autorità incaricate dell'applicazione della legge di raccogliere, conservare e scambiare dati personali. In molti casi vengono attivamente coinvolti i privati, come mostrano tra l'altro la direttiva sulla conservazione dei dati ([7]) e i vari strumenti relativi al PNR ([8]).

16. La quarta prospettiva è la libera circolazione. La progressiva creazione di uno spazio di libertà, sicurezza e giustizia esige un'ulteriore rimozione delle frontiere interne e degli eventuali ostacoli alla libera circolazione al suo interno. In ogni caso, i nuovi strumenti che saranno applicati nel settore non dovrebbero reinstallare altri ostacoli. In questo contesto per «libera circolazione» si intende sia, da un lato, la libera circolazione delle persone che, dall'altro, la libera circolazione dei dati (personali).

17. Le suddette quattro prospettive dimostrano che il contesto in cui sono usate le informazioni sta rapidamente cambiando. In un tale contesto non possono sussistere dubbi sull'importanza di un meccanismo forte per la salvaguardia dei diritti fondamentali dei cittadini e soprattutto per la protezione dei dati e della vita privata. È per questi motivi che il GEPD sceglie la necessità di protezione come prospettiva principale della sua analisi, come indicato al punto 11.

([6]) Nella relazione sugli affari interni si parla addirittura a questo proposito di uno «tsunami digitale».

([7]) Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, GU L 105 del 13.4.2006, pag. 54.

([8]) Cfr. ad es. l'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), GU L 204 del 4.8.2007, pag. 18, e la proposta di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione (Passenger Name Record, PNR) nelle attività di contrasto, COM(2007) 654 definitivo.

IV. **VALUTAZIONE GENERALE**

18. La comunicazione e il programma di Stoccolma si prefiggono di definire gli intenti dell'UE per i prossimi cinque anni, nonché le relative possibili ripercussioni anche a più lungo termine. Il GEPD rileva che la comunicazione è redatta in modo per così dire «neutrale rispetto al trattato di Lisbona». Pur comprendendo pienamente le ragioni di questo approccio da parte della Commissione, il GEPD si rammarica tuttavia che la comunicazione non abbia potuto trarre pieno vantaggio dalle possibilità supplementari offerte dal trattato di Lisbona. Nel presente parere si darà maggiore risalto alla prospettiva del trattato di Lisbona.

19. La comunicazione si basa sui risultati ottenuti negli ultimi anni con gli interventi dell'UE nel quadro dello spazio di libertà, sicurezza e giustizia. Detti risultati, che possono essere qualificati come «determinati dagli eventi», hanno posto l'accento su misure che estendono i poteri delle autorità di contrasto, ma sono invasive per il cittadino. È sicuramente il caso dei settori in cui i dati personali sono utilizzati e scambiati in modo intensivo, che sono quindi cruciali ai fini della protezione dei dati. I risultati sono determinati dagli eventi da quando eventi esterni, quali l'11 settembre e gli attentati di Madrid e Londra, hanno dato un forte impulso all'attività legislativa. Ad esempio, il trasferimento dei dati relativi ai passeggeri agli Stati Uniti può essere considerato una conseguenza dell'11 settembre ([9]), mentre gli attentati di Londra hanno portato all'adozione della direttiva 2006/24/CE sulla conservazione dei dati ([10]). L'accento è stato posto su misure più invasive in quanto il legislatore UE si è concentrato su misure che agevolano l'utilizzo e lo scambio di dati, mentre le misure volte a garantire la protezione dei dati personali sono state discusse con minore urgenza. La principale misura cautelare adottata è la decisione quadro 2008/977/GAI del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale ([11]), dopo tre anni di discussioni in sede di Consiglio. L'esito è stata una decisione quadro del Consiglio non pienamente soddisfacente (cfr. punti 29 e 30).

20. L'esperienza degli ultimi anni dimostra che, prima di adottare nuovi strumenti, è necessario riflettere sulle conseguenze per le autorità di contrasto e i cittadini europei. Tale riflessione dovrebbe tener debitamente conto, per mezzo di esami periodici, dei costi per la vita privata e dell'efficacia ai fini dell'applicazione della legge innanzi tutto all'atto della proposta e della discussione di nuovi strumenti, ma anche dopo in sede di attuazione. Tale riflessione è altrettanto fondamentale prima che un nuovo programma pluriennale stabilisca le principali iniziative per il prossimo futuro.

21. Il GEPD si rallegra che la comunicazione riconosca nella salvaguardia dei diritti fondamentali, e in particolare nella protezione dei dati personali, una delle questioni chiave per il futuro dello spazio di libertà, sicurezza e giustizia. Al punto 2 della comunicazione l'UE è definita uno spazio unico per la tutela dei diritti fondamentali basati su valori comuni. È positivo anche il fatto che l'adesione alla convenzione europea dei diritti dell'uomo sia menzionata tra gli orientamenti prioritari della comunicazione, anzi ne sia il primo. L'adesione è un passo avanti importante per garantire un sistema armonioso e coerente di salvaguardia dei diritti fondamentali. Ultima considerazione, ma non meno importante: la protezione dei dati ha avuto un posto di primo piano nella comunicazione.

22. L'accento posto dalla comunicazione su questo punto denota la ferma intenzione di garantire la salvaguardia dei diritti dei cittadini e, così facendo, di adottare un approccio più equilibrato. I governi necessitano di strumenti adeguati per garantire la sicurezza dei cittadini ma, nella nostra società europea, sono tenuti al pieno rispetto dei diritti fondamentali di questi ultimi. Per «servire i cittadini» ([12]) occorre un'Unione europea che mantenga tale equilibro.

23. Secondo il GEPD la comunicazione tiene conto molto bene della necessità di tale equilibrio, inclusa la necessità di protezione dei dati personali, e riconosce che occorre una diversa enfasi. Ciò è importante perché le politiche nell'ambito dello spazio di libertà, sicurezza e giustizia non dovrebbero favorire il graduale passaggio a una società della sorveglianza. Il GEPD si aspetta che il Consiglio adotti lo stesso approccio nel programma di Stoccolma, anche confermando gli orientamenti di cui al punto 25.

24. Ciò è tanto più importante in quanto lo spazio di libertà, sicurezza e giustizia è uno spazio che determina le circostanze della vita dei cittadini, in particolare lo spazio privato delle responsabilità personali e della sicurezza personale e sociale protetto dai diritti fondamentali, come ha recentissimamente sottolineato la Corte costituzionale tedesca nella sentenza del 30 giugno 2009 relativa al trattato di Lisbona ([13]).

([9]) L'accordo PNR del 2007, citato nella precedente nota, e i suoi predecessori.

([10]) Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, GU L 105 del 13.4.2006, pag. 54. Pur avendo come base giuridica l'articolo 95 del trattato CE, è stata una reazione immediata agli attentati di Londra.

([11]) 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, GU L 350 del 30.12.2008, pag. 60.

([12]) Cfr. il titolo della comunicazione.

([13]) Comunicato stampa n. 72/2009 della Corte costituzionale federale tedesca del 30 giugno 2009, punto 2 c).

25. Il GEPD sottolinea che in uno spazio siffatto:

— lo scambio di informazioni dovrebbe aver luogo tra le autorità degli Stati membri, nonché, se del caso, tra banche dati o organismi europei, in base a meccanismi adeguati ed efficaci che rispettino pienamente i diritti fondamentali dei cittadini e assicurino la fiducia reciproca,

— è necessaria a tal fine non solo la disponibilità di informazioni, unitamente al reciproco riconoscimento degli ordinamenti giuridici degli Stati membri (e dell'UE), ma anche l'armonizzazione delle norme in materia di protezione dell'informazione per mezzo, ad esempio ma non solo, di un quadro comune per la protezione dei dati,

— tali norme comuni non dovrebbero essere applicabili soltanto alle situazioni dalle dimensioni transnazionali. La fiducia reciproca può esistere solo se le norme sono forti e sempre rispettate, senza alcun rischio di non applicazione qualora la dimensione transnazionale non sia evidente o non lo sia più. A parte ciò, specie quando si tratta di uso dell'informazione, le differenze tra dati «interni» e «transnazionali» possono non funzionare nella pratica ([14]).

V. **STRUMENTI PER LA PROTEZIONE DEI DATI**

V.1. **Verso un regime globale di protezione dei dati**

26. Il GEPD approva l'approccio strategico di assegnare alla protezione dei dati una posizione di rilievo nella comunicazione. In effetti molte iniziative nell'ambito dello spazio di libertà, sicurezza e giustizia dipendono dall'utilizzo dei dati personali e perchè queste abbiano successo è essenziale una buona protezione dei dati. Il rispetto della protezione dei dati e della vita privata non è solo un obbligo legale sempre più riconosciuto a livello di UE, ma anche una questione cruciale per i cittadini europei, come indicano i risultati dell'Eurobarometro ([15]). Inoltre, limitare l'accesso ai dati personali è essenziale anche per garantire la fiducia da parte delle strutture di contrasto.

27. Al punto 2.3 della comunicazione si afferma che è necessario un regime completo di protezione dei dati che ricomprenda tutte le competenze dell'Unione ([16]). Il GEPD è del tutto favorevole a tale obiettivo, indipendentemente dall'entrata in vigore del trattato di Lisbona. Rileva altresì che un tale regime non implica necessariamente un solo quadro giuridico applicabile a qualsiasi trattamento. Conformemente ai trattati in vigore, le possibilità di adottare un solo quadro giuridico globale applicabile a qualsiasi trattamento sono limitate dalla struttura a pilastri e dal fatto che, almeno nel primo pilastro, la protezione dei dati trattati dalle istituzioni europee poggia su una base giuridica distinta (articolo 286 del trattato CE). Ciò nonostante, il GEPD rileva che si possono apportare alcuni miglioramenti sfruttando pienamente le possibilità offerte dai trattati in vigore, come già sottolineato dalla Commissione nella comunicazione dal titolo «Attuazione del programma dell'Aia: prospettive per il futuro» ([17]). Una volta entrato in vigore il trattato di Lisbona, l'articolo 16 del trattato sul funzionamento dell'Unione europea costituirà la base giuridica necessaria per un solo quadro giuridico globale applicabile a qualsiasi trattamento.

28. Il GEPD fa notare che è essenziale — in ogni caso — assicurare la coerenza interna del quadro giuridico per la protezione dei dati, eventualmente mediante l'armonizzazione e il consolidamento dei vari strumenti giuridici applicabili nello spazio di libertà, sicurezza e giustizia.

In virtù dei trattati in vigore

29. Un primo passo è stato fatto di recente con l'adozione della decisione quadro 2008/977/GAI del Consiglio ([18]). Non si tratta però di uno strumento giuridico qualificabile come «regime globale» sostanzialmente perché le sue disposizioni non hanno applicazione generale. Non si applicano alle situazioni interne, in cui i dati personali emanano dallo Stato membro che li utilizza. Tale limitazione non può che diminuire il valore aggiunto della decisione quadro del Consiglio, a meno che tutti gli Stati membri non decidano di includere le situazioni interne nella legislazione nazionale di attuazione, il che è improbabile.

30. Il secondo motivo per cui il GEPD ritiene che, a lungo termine, la decisione quadro 2008/977/GAI del Consiglio non contenga un quadro soddisfacente per la protezione dei dati in uno spazio di libertà, sicurezza e giustizia è che molte delle sue disposizioni essenziali non sono in linea con la direttiva 95/46/CE. Conformemente ai trattati in vigore, si potrebbe compiere un secondo passo ampliando il campo di applicazione e allineando la decisione quadro del Consiglio alla direttiva 95/46/CE.

31. Un altro impulso alla realizzazione di un regime globale di protezione dei dati potrebbe venire da una visione chiara e a lungo termine. Tale visione potrebbe prevedere un approccio globale e coerente per definire la raccolta e gli scambi di dati — nonché lo sfruttamento delle banche dati esistenti — e, al tempo stesso, le garanzie di protezione

([14]) Il GEPD ha sviluppato quest'ultimo punto nel parere del 19 dicembre 2005 sulla proposta di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale [COM(2005) 475 definitivo], GU C 47 del 25.2.2006, pag. 27, punti 30, 31 e 32.

([15]) «Data Protection in the European Union — Citizens' perceptions — Analytical report», La protezione dei dati nell'Unione europea — Le percezioni dei cittadini — Relazione analitica, Flash Eurobarometer Series 225, gennaio 2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) Cfr. anche gli orientamenti prioritari della comunicazione.

([17]) COM(2006) 331 definitivo del 28 giugno 2006.

([18]) Cfr. la nota in calce n. 11.

dei dati. Dovrebbe evitare inutili sovrapposizioni e doppioni degli strumenti (e quindi del trattamento dei dati personali). Dovrebbe inoltre favorire la coerenza delle politiche UE in questo settore, nonché la fiducia nel modo in cui le autorità pubbliche manipolano i dati dei cittadini. Il GEPD raccomanda al Consiglio di annunciare nel programma di Stoccolma la necessità di una visione chiara e a lungo termine.

32. Il GEPD raccomanda inoltre di valutare e porre in prospettiva le misure già adottate in questo settore, la loro attuazione concreta e la loro efficacia. Tale valutazione dovrebbe tenere debitamente conto dei costi per la vita privata e dell'efficacia ai fini dell'applicazione della legge. Se da tali valutazioni dovesse risultare che determinate misure non danno i risultati previsti o non sono proporzionate ai fini perseguiti, si dovrebbero prendere in considerazione le seguenti iniziative:

— in primo luogo, modificare o abrogare le misure qualora non sembrino sufficientemente giustificate dal punto di vista del valore aggiunto concreto che producono per le autorità di contrasto e i cittadini europei,

— in secondo luogo, valutare le possibilità di migliorare l'applicazione delle misure esistenti,

— soltanto in ultimo luogo, proporre nuove misure legislative se è probabile che siano necessarie per gli obiettivi previsti. L'adozione di nuovi strumenti dovrebbe essere limitata a quelli che apportano un chiaro e concreto valore aggiunto per le autorità di contrasto e i cittadini europei.

Il GEPD raccomanda di introdurre nel programma di Stoccolma un riferimento ad un sistema di valutazione delle misure esistenti.

33. Ultima ma non meno importante considerazione: bisognerebbe dare più importanza a una migliore applicazione delle garanzie esistenti conformemente alla comunicazione della Commissione sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati ([19]) e ai suggerimenti formulati dal GEPD nel parere relativo a tale comunicazione ([20]). Manca purtroppo alla Commissione, nel terzo pilastro, la possibilità di avviare procedure d'infrazione.

In virtù del trattato di Lisbona

34. Il trattato di Lisbona offre la possibilità di un vero quadro globale in materia di protezione dei dati. L'articolo 16, paragrafo 2 del trattato sul funzionamento dell'Unione europea esige che il Consiglio e il Parlamento europeo stabiliscano le norme relative alla protezione dei dati da parte di istituzioni, organismi, uffici ed agenzie dell'Unione, da parte degli Stati membri nello svolgimento delle attività che rientrano nell'ambito del diritto dell'Unione nonché da parte dei privati.

35. Il GEPD interpreta l'enfasi posta dalla comunicazione su un regime globale di protezione dei dati come un'ambizione della Commissione di proporre un quadro giuridico che si applichi a tutte le operazioni di trattamento. Approva pienamente tale ambizione in quanto rafforza la coerenza del sistema, assicura certezza del diritto e, così facendo, migliora la protezione. In particolare, eviterebbe in futuro la difficoltà di trovare una linea di demarcazione tra i pilastri nei casi in cui i dati raccolti nel settore privato a fini commerciali sono successivamente utilizzati a fini di contrasto. Detta linea di demarcazione tra i pilastri non riflette del tutto la realtà, come mostrano importanti sentenze della Corte di giustizia in materia di PNR ([21]) e di conservazione di dati ([22]).

36. Il GEPD suggerisce che il programma di Stoccolma ponga l'accento su questa motivazione per il regime globale di protezione dei dati, da cui risulta che un tale regime non è solo una semplice preferenza, bensì una necessità a causa delle prassi mutevoli in materia di utilizzo dei dati. Raccomanda di includere quale priorità nel programma di Stoccolma l'esigenza di un nuovo quadro legislativo, sostituendo tra l'altro la decisione quadro 2008/977/GAI del Consiglio.

37. Il GEPD sottolinea che il concetto di «regime globale di protezione dei dati» basato su un quadro giuridico generale non esclude l'adozione di norme supplementari per la protezione dei dati per la polizia e il settore giudiziario. Dette norme supplementari potrebbero tener conto delle necessità specifiche a fini di contrasto, come previsto dalla dichiarazione n. 21 allegata al trattato di Lisbona ([23]).

V.2. **Ribadire i principi della protezione dei dati**

38. La comunicazione rileva i cambiamenti tecnologici che trasformano la comunicazione tra individui e organizzazioni pubbliche e private. Occorre perciò ribadire, secondo la Commissione, una serie di principi fondamentali della protezione dei dati.

([19]) COM(2007) 87 definitivo del 7 marzo 2007.

([20]) Parere del 25 luglio 2007, GU C 255 del 27.10.2007, pag. 1, in particolare punto 30.

([21]) 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], pag. I-4721.

([22]) Sentenza della Corte del 10 febbraio 2009, Irlanda c/ Parlamento europeo e Consiglio dell'Unione europea, causa C-301/06, non ancora pubblicata.

([23]) Cfr. la dichiarazione n. 21 relativa alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, allegata all'atto finale della conferenza intergovernativa che ha adottato il trattato di Lisbona, GU C 115 del 9.5.2008, pag. 345.

39. Il GEPD si compiace delle intenzioni espresse nella comunicazione. Una valutazione dell'efficacia di tali principi nella prospettiva dei cambiamenti tecnologici è estremamente utile. In primo luogo, è importante rilevare che la conferma e la riaffermazione dei principi della protezione dei dati non devono sempre essere direttamente collegate agli sviluppi tecnologici. Potrebbero essere necessarie anche alla luce di altre prospettive, menzionate nella terza parte: l'internazionalizzazione, l'uso crescente dei dati a fini di contrasto e la libera circolazione.

40. Secondo il GEPD, inoltre, tale valutazione può essere inclusa nella consultazione pubblica annunciata dalla Commissione nella conferenza «Dati personali — maggior uso, maggiore protezione?» del 19 e 20 maggio 2009, da cui potrebbero derivare preziosi contributi ([24]). Il GEPD suggerisce che il Consiglio, nel testo del programma di Stoccolma, e la Commissione, nelle dichiarazioni pubbliche sulla consultazione, mettano in evidenza il nesso tra le intenzioni di cui al punto 2.3 della comunicazione e la consultazione pubblica sul futuro della protezione dei dati.

41. Al fine di illustrare ciò che dovrebbe essere oggetto della valutazione si menzionano i seguenti punti:

— nello spazio di libertà, sicurezza e giustizia è probabile che i dati personali siano di carattere particolarmente sensibile, ad esempio i dati relativi alle condanne penali, i dati di polizia e i dati biometrici quali impronte digitali e profili di DNA,

— il loro trattamento può comportare conseguenze negative per gli interessati, specie se si considerano i poteri coercitivi delle autorità di contrasto. Inoltre, il monitoraggio e l'analisi dei dati sono sempre più automatizzati, molto spesso senza alcun intervento umano. La tecnologia consente l'utilizzo di banche dati contenenti dati personali per ricerche generali (estrapolazione di dati, creazione di profili di dati, ecc.). Si dovrebbero definire chiaramente gli obblighi legali su cui è basato il trattamento dati,

— una pietra miliare della normativa sulla protezione dei dati è il vincolo che i dati personali siano raccolti a fini specifici e non siano utilizzati in modo con essi incompatibile. L'uso a fini incompatibili dovrebbe essere consentito soltanto se stabilito per legge e se necessario per interessi pubblici specifici, quali quelli definiti dall'articolo 8, paragrafo 2 della CEDU,

— l'esigenza di rispettare il principio di limitazione delle finalità potrebbe avere conseguenze sulle attuali tendenze nell'uso dei dati. A fini di contrasto si utilizzano dati raccolti da società private a fini commerciali nelle telecomunicazioni, nei trasporti e nel settore finanziario. Vengono inoltre istituiti sistemi di informazione su vasta scala, ad esempio nei settori dell'immigrazione e del controllo delle frontiere. Sono anche consentiti l'accesso alle banche dati e l'interconnessione tra le medesime, ampliando così le finalità originarie della raccolta di dati personali. È necessario riflettere sulle tendenze in atto nonché, se del caso, su possibili adeguamenti e/o garanzie supplementari,

— oltre ai principi della protezione dei dati menzionati nella comunicazione, la valutazione dovrebbe prestare attenzione alla necessità di assicurare la trasparenza del trattamento, consentendo all'interessato di esercitare i propri diritti. La trasparenza è una questione particolarmente spinosa nel settore delle attività di contrasto, soprattutto perché andrebbe valutata in rapporto ai rischi per le indagini,

— bisognerebbe trovare soluzioni per gli scambi con i paesi terzi.

42. La valutazione dovrebbe inoltre incentrarsi sulle possibilità di rendere più efficace l'applicazione dei principi della protezione dei dati. Potrebbe essere utile al riguardo concentrarsi sugli strumenti che possono rafforzare le competenze dei responsabili del trattamento dei dati. Tali strumenti devono consentire che della gestione dei dati rispondano interamente i suddetti responsabili del trattamento. È utile a questo proposito il concetto di «governance dei dati», in cui rientrano tutti i mezzi legali, tecnici ed organizzativi con cui le organizzazioni assicurano la piena responsabilità delle modalità di gestione dei dati, quali pianificazione e controllo, utilizzo di tecnologie corrette, adeguata formazione del personale, controlli di conformità, ecc.

V.3. **Tecnologie rispettose della vita privata**

43. Il GEPD si rallegra che al punto 2.3 la comunicazione menzioni una certificazione del rispetto della vita privata. Oltre a questo, si potrebbe prevedere anche un riferimento al principio della «tutela della vita privata fin dalla progettazione» («privacy by design») e alla necessità di individuare le «migliori tecniche disponibili» conformi al quadro normativo dell'UE per la protezione dei dati.

44. Il GEPD ritiene che la «tutela della vita privata fin dalla progettazione» e le tecnologie rispettose della vita privata possano essere strumenti utili ai fini di una maggiore protezione e per un uso più efficace dell'informazione. Suggerisce due modi di procedere, che non si escludono a vicenda:

— un regime di certificazione per la protezione della vita privata e dei dati ([25]) quale opzione per i creatori e gli utenti dei sistemi di informazione, eventualmente sostenuto da finanziamenti o legislazione dell'UE,

([24]) Il Gruppo dell'articolo 29 per la protezione dei dati, al quale partecipa il GEPD, ha deciso di lavorare intensamente al proprio contributo alla consultazione pubblica.

([25]) Ne costituisce un esempio il marchio di certificazione europeo della tutela della privacy (EuroPriSe).

— l'obbligo giuridico per i creatori e gli utenti dei sistemi di informazione di utilizzare sistemi che siano conformi al principio della «tutela della vita privata fin dalla progettazione». Ciò potrebbe richiedere un ampliamento dell'attuale campo di applicazione della normativa sulla protezione dei dati, per rendere i creatori responsabili dei sistemi di informazione che sviluppano ([26]).

Il GEPD suggerisce di menzionare nel programma di Stoccolma questi possibili modi di procedere.

V.4. **Aspetti esterni**

45. Un altro argomento menzionato nella comunicazione è lo sviluppo e la promozione di norme internazionali in materia di protezione dei dati. Attualmente si svolgono numerose attività in vista della definizione di norme possibili da applicare su scala mondiale, ad esempio da parte della conferenza internazionale dei commissari in materia di protezione dei dati e della vita privata. In un prossimo futuro ciò potrebbe sfociare in un accordo internazionale. Il GEPD suggerisce che il programma di Stoccolma appoggi tali attività.

46. La comunicazione fa inoltre riferimento alla conclusione di accordi bilaterali sulla base di progressi già realizzati con gli Stati Uniti. Il GEPD condivide la necessità di un quadro giuridico chiaro per il trasferimento di dati a paesi terzi e si compiace quindi del lavoro congiunto delle autorità UE e USA in sede di Gruppo di contatto ad alto livello in merito ad un possibile strumento transatlantico sulla protezione dei dati, ma chiede maggiore chiarezza e attenzione su aspetti specifici ([27]). In tale prospettiva è inoltre interessante notare le idee contenute nella relazione sugli affari interni riguardo ad un'area di cooperazione euroatlantica nel settore della libertà, della sicurezza e della giustizia su cui, secondo la relazione, l'UE dovrebbe prendere una decisione entro il 2014. Tale area non sarebbe possibile senza adeguate garanzie in materia di protezione dei dati.

47. Il GEPD ritiene che le norme europee per la protezione dei dati, basate sulla convenzione 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale ([28]) e sulla giurisprudenza della Corte di giustizia europea e della Corte europea dei diritti dell'uomo, debbano determinare il livello di protezione in un accordo generale con gli Stati Uniti in materia di protezione e scambio dei dati. Un tale accordo generale potrebbe servire da base per disposizioni specifiche sullo scambio di dati personali. Ciò è tanto più importante alla luce dell'intenzione di cui al punto 4.2.1 della comunicazione, secondo cui l'Unione europea deve concludere accordi in materia di cooperazione di polizia ogniqualvolta necessario.

48. Il GEPD capisce perfettamente l'esigenza di rafforzare la cooperazione internazionale, talvolta anche con paesi che non tutelano i diritti fondamentali. È tuttavia ([29]) essenziale tener conto che la cooperazione internazionale produrrà probabilmente un notevole aumento della raccolta e del trasferimento internazionale di dati. È quindi essenziale che i principi dell'equità e legittimità del trattamento, e in generale quelli relativi al giusto processo, si applichino alla raccolta e al trasferimento di dati personali oltre le frontiere dell'Unione, e che i dati personali siano trasferiti a paesi terzi o ad organismi internazionali solo se i paesi terzi in questione assicurano un adeguato livello di protezione o altre garanzie appropriate.

49. Per concludere, il GEPD raccomanda di dare risalto nel programma di Stoccolma all'importanza di concludere accordi generali con gli Stati Uniti e altri paesi terzi in materia di protezione e scambio dei dati, basati sul livello di protezione garantito nel territorio dell'UE. In una più ampia prospettiva il GEPD segnala l'importanza di promuovere attivamente il rispetto dei diritti fondamentali, in particolare della protezione dei dati, nelle relazioni con paesi terzi e organizzazioni internazionali ([30]). Inoltre, il programma di Stoccolma potrebbe menzionare l'idea generale che lo scambio di dati personali con i paesi terzi richiede un livello adeguato di protezione o altre garanzie appropriate in tali paesi.

VI. **L'UTILIZZO DELLE INFORMAZIONI**

VI.1. **Verso un modello europeo di informazione**

50. Un migliore scambio delle informazioni rappresenta un obiettivo politico essenziale per l'Unione europea nell'ambito dello spazio di libertà, sicurezza e giustizia. Il punto 4.1.2 della comunicazione sottolinea che la sicurezza all'interno dell'Unione dipende dall'efficacia dei dispositivi di scambio delle informazioni tra le autorità nazionali e altri attori europei. Tale enfasi sullo scambio di informazioni è logica, in assenza di una forza di polizia europea, di un sistema europeo di giustizia penale e di un controllo

([26]) Gli utenti dell'informazione sono tutelati dalla normativa sulla protezione dei dati, alla stessa stregua dei responsabili o degli incaricati del trattamento.

([27]) Cfr. il parere del GEPD dell'11 novembre 2008 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, GU C 128 del 6.6.2009, pag. 1.

([28]) ETS 108 del 28.1.1981.

([29]) Cfr. la lettera del GEPD del 28 novembre 2005 riguardante la comunicazione della Commissione sulla dimensione esterna dello spazio di libertà, sicurezza e giustizia, disponibile sul sito web del GEPD.

([30]) La recente giurisprudenza sugli elenchi di terroristi conferma che le garanzie sono necessarie — anche in relazione alle Nazioni Unite — per garantire che le misure antiterrorismo siano conformi alle norme UE in materia di diritti fondamentali (cause riunite C-402/05 P e C-415/05 P, Kadi and Al Barakaat Foundation c/Consiglio, sentenza del 3 settembre 2008, non ancora pubblicata).

delle frontiere a livello europeo. Le misure relative alle informazioni costituiscono pertanto contributi essenziali dell'Unione europea, che consentono alle autorità degli Stati membri di affrontare efficacemente la criminalità transfrontaliera e di proteggere validamente le frontiere esterne. Tuttavia, queste misure non contribuiscono soltanto alla sicurezza dei cittadini ma anche alla loro libertà — era stato accennato in precedenza alla libera circolazione delle persone come prospettiva del presente parere — e alla giustizia.

51. È precisamente per questi motivi che il principio della disponibilità è stato introdotto nel programma dell'Aia. In virtù di tale principio le informazioni necessarie per combattere la criminalità dovrebbero poter attraversare liberamente le frontiere interne dell'UE. Le esperienze recenti mostrano la difficoltà di attuare questo principio nelle misure legislative. La proposta della Commissione del 12 ottobre 2005 relativa alla decisione quadro del Consiglio sullo scambio di informazioni in virtù del principio di disponibilità ([31]) non è stata accolta dal Consiglio. Gli Stati membri non erano disposti ad accettare le conseguenze del principio di disponibilità nella misura più ampia possibile. Sono stati invece adottati strumenti più limitati ([32]) quali la decisione 2008/615/GAI del Consiglio, del 23 giugno 2008, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera («decisione di Prüm») ([33]).

52. Mentre il principio di disponibilità era un elemento centrale del programma dell'Aia, attualmente sembra che la Commissione adotti un'impostazione più modesta. Essa prevede di incentivare ulteriormente lo scambio di informazioni tra le autorità degli Stati membri introducendo il modello europeo di informazione. La presidenza svedese dell'UE condivide tale ottica ([34]). Essa presenterà una proposta di strategia per lo scambio di informazioni. Il Consiglio ha già avviato i lavori su questo progetto ambizioso di strategia di gestione delle informazioni a livello di Unione europea, che è strettamente collegato al modello europeo di informazione. Il GEPD prende atto con grande interesse di questi sviluppi e sottolinea che, nell'ambito di tali progetti, dovrebbe essere prestata attenzione agli elementi relativi alla protezione dei dati.

Il modello europeo di informazione e la protezione dei dati

53. In primo luogo, è opportuno sottolineare che il futuro dello spazio di libertà, sicurezza e giustizia non dovrebbe essere orientato dalla tecnologia, nel senso che le quasi illimitate opportunità offerte dalle nuove tecnologie dovrebbero essere sempre verificate alla luce dei pertinenti principi in materia di protezione dei dati e utilizzate unicamente nella misura in cui siano conformi a tali principi.

54. Il GEPD rileva che la comunicazione presenta il modello di informazione non come un semplice modello tecnico, ma come uno comportante una capacità di analisi strategica potenziata e un sistema migliorato per la raccolta e il trattamento delle informazioni operative. Essa riconosce inoltre che si dovrebbe tener conto degli aspetti di carattere politico, come i criteri di raccolta, condivisione e trattamento delle informazioni, nel rispetto dei principi della protezione dei dati.

55. La tecnologia dell'informazione e le condizioni giuridiche sono — e continueranno a essere — entrambe essenziali. Il GEPD accoglie favorevolmente la comunicazione la quale parte dall'assunto che un modello europeo di informazione non può essere concepito sulla base di considerazioni tecniche. È essenziale che le informazioni siano raccolte, condivise e trattate unicamente sulla base di esigenze concrete di sicurezza e tenendo conto dei principi in materia di protezione dei dati. Inoltre il GEPD sottoscrive pienamente l'esigenza di definire un meccanismo di follow up per valutare il funzionamento dello scambio di informazioni. Egli suggerisce che il Consiglio elabori ulteriormente questi elementi nel programma di Stoccolma.

56. In tale contesto, il GEPD sottolinea che la protezione dei dati, volta a tutelare il cittadino, non dovrebbe essere considerata un ostacolo a un'efficace gestione dei dati. Essa fornisce strumenti importanti per migliorare l'archiviazione, l'accesso e lo scambio di informazioni. I diritti dell'interessato di venire a conoscenza delle informazioni in corso di trattamento che lo riguardano nonché di rettificare le informazioni inesatte possono anche rafforzare la precisione dei dati contenuti nei sistemi di gestione dei dati.

57. La normativa sulla protezione dei dati ha sostanzialmente le seguenti conseguenze: se i dati sono necessari per una finalità specifica e legittima possono essere utilizzati; se non sono necessari per una finalità ben determinata, i dati personali non dovrebbero essere utilizzati. Nel primo caso, potrebbero essere necessarie misure aggiuntive per fornire garanzie adeguate.

58. Il GEPD è tuttavia critico nella misura in cui la comunicazione accenna all'individuazione di esigenze future nell'ambito del modello di informazione. Egli sottolinea che anche in futuro il principio di limitazione delle finalità dovrà orientare la creazione dei sistemi di informazione ([35]). Si tratta di una delle garanzie essenziali che il sistema di protezione dei dati offre al cittadino: egli deve essere in grado di sapere in anticipo per quale finalità sono raccolti i dati che lo riguardano e che detti dati saranno utilizzati solo per tale finalità, segnatamente in futuro. Questa garanzia è anche sancita dall'articolo 8 della Carta dei diritti fondamentali dell'Unione. Il principio di limitazione delle finalità consente eccezioni — che sono particolarmente rilevanti nell'ambito dello spazio di libertà, sicurezza e giustizia — ma tali eccezioni non dovrebbero determinare la creazione di un sistema.

([31]) COM(2005) 490 definitivo.

([32]) Nella prospettiva della disponibilità; la decisione di Prüm contiene disposizioni di vasta portata per l'utilizzo dei dati biometrici (DNA e impronte digitali).

([33]) GU L 210 del 6.8.2008, pag. 1.

([34]) Cfr. il programma di lavoro dell'UE stilato dal governo, citato nella nota 5 alla pagina 23.

([35]) Cfr. anche il punto 41.

Scegliere la giusta architettura

59. Scegliere la giusta architettura per lo scambio di informazioni è il punto di partenza dell'intero processo. Nella comunicazione si riconosce l'importanza di adeguate architetture informative (punto 4.1.3) ma purtroppo solo in relazione all'interoperabilità.

60. Il GEPD sottolinea un altro aspetto: nell'ambito del modello europeo di informazione, i requisiti in materia di protezione dei dati dovrebbero essere parte integrante di tutto lo sviluppo del sistema e non dovrebbero essere considerati semplicemente una condizione necessaria per la legittimità di un sistema ([36]). Ci si dovrebbe basare sul concetto della «tutela della vita privata fin dalla progettazione» e sull'esigenza di individuare «le migliori tecniche disponibili» ([37]), come indicato al punto 43. Il modello europeo di informazione dovrebbe fondarsi su questi concetti. Ciò significa più concretamente che i sistemi di informazione progettati per finalità di sicurezza pubblica dovrebbero sempre essere costruiti conformemente al principio della «tutela della vita privata fin alla progettazione». Il GEPD raccomanda al Consiglio di includere questi elementi nel programma di Stoccolma.

Interoperabilità dei sistemi

61. Il GEPD sottolinea che l'interoperabilità non è una questione puramente tecnica ma ha ripercussioni anche sulla protezione del cittadino, in particolare per quanto riguarda la protezione dei dati. Dalla prospettiva della protezione dei dati, l'interoperabilità dei sistemi, se realizzata correttamente, presenta chiari vantaggi nell'evitare una doppia archiviazione. Tuttavia, è altresì ovvio che rendere tecnicamente fattibile l'accesso ai dati o il loro scambio diventa, in molti casi, un potente incentivo per l'accesso o lo scambio «de facto» di tali dati. In altre parole, l'interoperabilità presenta rischi particolari di interconnessione tra banche dati aventi finalità differenti ([38]). Essa può incidere sulle rigorose limitazioni relative alla finalità delle banche dati.

62. In breve, il semplice fatto che sia tecnicamente possibile scambiare informazioni digitali tra banche dati interoperabili o accorpare queste banche dati non giustifica un'eccezione al principio di limitazione delle finalità. L'interoperabilità dovrebbe nei casi concreti basarsi su scelte politiche chiare e oculate. Il GEPD suggerisce di precisare tale nozione nel programma di Stoccolma.

VI.2. **L'utilizzo delle informazioni raccolte per altre finalità**

63. La comunicazione non affronta esplicitamente una delle più importanti tendenze degli ultimi anni, precisamente l'utilizzo ai fini dell'applicazione della legge di dati raccolti nel settore privato per finalità commerciali. Questa tendenza non solo si riferisce ai dati relativi al traffico delle comunicazioni elettroniche e ai dati relativi ai passeggeri aerei che si recano in (taluni) paesi terzi ([39]) ma riguarda anche il settore finanziario. Un esempio è costituito dalla direttiva 2005/60/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo ([40]). Un altro esempio ben noto e molto dibattuto riguarda il trattamento, da parte della «Society for Worldwide Interbank Financial Telecommunication» (SWIFT) ([41]), dei dati personali che sono necessari per le finalità del programma di controllo delle transazioni finanziarie dei terroristi del Dipartimento del Tesoro statunitense.

64. Il GEPD ritiene che queste tendenze richiedano un'attenzione specifica nel programma di Stoccolma. Esse possono essere considerate quali deroghe al principio di limitazione delle finalità e sono spesso molto invasive della vita privata, dal momento che l'utilizzo di questi dati può rivelare molto sul comportamento delle persone. Ogni volta che sono proposte misure siffatte, devono sussistere prove molto solide della loro necessità. Se sono fornite tali prove, si deve assicurare il pieno rispetto dei diritti delle persone.

65. Secondo il GEPD l'utilizzo ai fini dell'applicazione della legge di dati personali raccolti per finalità commerciali dovrebbe essere consentito unicamente nel rispetto di condizioni rigorose, quali:

— i dati sono utilizzati soltanto per finalità specificamente definite, quali la lotta al terrorismo o alle forme gravi di criminalità, da determinarsi caso per caso,

— i dati sono trasferiti tramite un sistema «push» invece che «pull» ([42]),

([36]) Cfr. «Guidelines and criteria for the development, implementation and use of Privacy Enhancing Security Technologies» (Orientamenti e criteri per lo sviluppo, l'attuazione e l'utilizzo delle tecnologie di sicurezza che migliorano la protezione della vita privata) elaborati nel progetto PRISE (www.prise.oeaw.ac.at).

([37]) Per «migliori tecniche disponibili» si intende la fase più efficace e avanzata dello sviluppo delle attività e dei loro metodi di funzionamento, che indichi l'attitudine pratica di particolari tecniche a costituire in linea di principio la base per applicazioni e sistemi ITS che rispettino i requisiti del quadro normativo dell'UE in materia di vita privata, protezione dei dati e sicurezza.

([38]) Cfr. le osservazioni del GEPD sulla comunicazione della Commissione sull'interoperabilità tra le banche dati europee, 10 marzo 2006, disponibile all'indirizzo: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

([39]) Cfr. ad esempio il punto 15.

([40]) GU L 309 del 25.11.2005, pag. 15.

([41]) Cfr. il parere 10/2006 del Gruppo dell'articolo 29 sul trattamento dei dati personali da parte della Society for Worldwide Interbank Financial Telecommunication (SWIFT).

([42]) Nel sistema «push» il responsabile del trattamento trasmette i dati su richiesta («pushes») all'autorità di contrasto. Nel sistema «pull» l'autorità di contrasto ha accesso alla banca dati del responsabile ed estrae («pulls») le informazioni dalla stessa banca dati. Nel sistema «pull» risulta più difficoltoso per il responsabile del trattamento assumere nuovamente la propria responsabilità.

— le richieste di dati dovrebbero essere proporzionate, strettamente mirate e basate in linea di principio su sospetti relativi a persone specifiche,

— dovrebbero essere evitati le ricerche di routine, l'estrapolazione di dati e l'elaborazione di profili di dati,

— tutti gli utilizzi dei dati ai fini dell'applicazione della legge dovrebbero essere registrati per consentire un controllo efficace sull'utilizzo, da parte dell'interessato nell'esercizio dei propri diritti, delle autorità garanti della protezione dei dati e delle autorità giudiziarie.

VI.3. **Sistemi di informazione e organi dell'UE**

Sistemi di informazione con o senza archiviazione centralizzata ([43])

66. Negli ultimi anni, il numero dei sistemi di informazione basati sulla normativa dell'UE è considerevolmente aumentato nell'ambito dello spazio di libertà, sicurezza e giustizia. A volte sono prese decisioni per istituire un sistema che comporta l'archiviazione centralizzata dei dati a livello europeo, in altri casi la legge prevede unicamente lo scambio di informazioni tra le banche dati nazionali. Il sistema di informazione Schengen è probabilmente il migliore esempio di sistema con archiviazione centralizzata. La decisione 2008/615/GAI del Consiglio (decisione di Prüm) ([44]) è dalla prospettiva della protezione dei dati l'esempio più significativo di un sistema senza archiviazione centralizzata in quanto prevede uno scambio massiccio di dati biometrici tra le autorità degli Stati membri.

67. La comunicazione illustra che questa tendenza di creare nuovi sistemi continuerà. Un primo esempio, tratto dal punto 4.2.2, è un sistema di informazione che espande il Sistema europeo di informazione sui casellari giudiziari (ECRIS) per contemplare i cittadini di paesi non appartenenti all'UE. La Commissione ha già commissionato uno studio su uno schedario europeo per i cittadini di paesi terzi che abbiano subito una condanna (EICTCN), che porterà forse alla creazione di una banca dati centralizzata. Un secondo esempio è lo scambio di informazioni sulle persone iscritte nei registri di insolvenza di altri Stati membri, nell'ambito della giustizia elettronica (punto 3.4.1 della comunicazione), senza archiviazione centralizzata.

68. Un sistema decentrato offrirebbe alcuni vantaggi dal punto di vista della protezione dei dati. Esso evita la doppia archiviazione dei dati da parte dell'autorità dello Stato membro e da parte del sistema centralizzato, la responsabilità dei dati è chiara in quanto l'autorità dello Stato membro sarà il responsabile del trattamento, mentre il controllo da parte dell'autorità giudiziaria e da parte delle autorità incaricate della protezione dei dati può avvenire a livello di Stati membri. Ma questo sistema presenta anche delle carenze quando i dati sono scambiati con altre giurisdizioni, per esempio quando si tratta di garantire che le informazioni siano tenute aggiornate tanto nel paese di origine quanto nel paese di destinazione e circa le modalità per assicurare un controllo efficace da entrambe le parti. Risulta ancora più complicato garantire la responsabilità del sistema tecnico per lo scambio. Tali carenze possono essere superate optando per un sistema centralizzato la cui responsabilità ricada sugli organi europei almeno per parti del sistema stesso (come l'infrastruttura tecnica).

69. In questo contesto, sarebbe utile elaborare criteri basilari per la scelta tra sistemi centralizzati e decentrati, garantendo scelte politiche chiare e oculate nei casi concreti. Tali criteri possono contribuire al funzionamento dei sistemi stessi, nonché alla protezione dei dati riguardanti il cittadino. Il GEPD suggerisce di includere nel programma di Stoccolma l'intenzione di elaborare tali criteri.

Sistemi di informazione su vasta scala

70. Il punto 4.2.3.2 della comunicazione tratta brevemente del futuro dei sistemi di informazione su vasta scala con enfasi sul sistema d'Informazione Schengen (SIS) e sul sistema di informazione visti (VIS).

71. Il punto 4.2.3.2 cita inoltre la creazione di un sistema elettronico di registrazione ingressi/uscite dal territorio degli Stati membri dell'Unione europea oltre ai programmi di viaggiatori registrati. Questo sistema era stato annunciato in precedenza dalla Commissione quale parte del «pacchetto frontiere» su iniziativa del vicepresidente Frattini ([45]). Nelle sue osservazioni preliminari ([46]), il GEPD era stato piuttosto critico nei confronti di questa proposta poiché l'esigenza di tale sistema invasivo, in aggiunta ai sistemi su vasta scala esistenti, non era sufficientemente dimostrata. Il GEPD non constata alcuna prova ulteriore dell'esigenza di tale sistema e suggerisce pertanto al Consiglio di non accennare a tale idea nel programma di Stoccolma.

72. In questo contesto, il GEPD desidera rinviare ai suoi pareri su varie iniziative nel settore dello scambio di informazioni a livello di UE ([47]), in cui ha formulato vari suggerimenti e osservazioni sulle implicazioni in materia di protezione dei dati derivanti dall'utilizzo di vaste banche dati a livello di UE. Tra le altre questioni, ha prestato particolare attenzione

([43]) L'archiviazione centralizzata è in questo contesto intesa come archiviazione a livello centrale europeo, mentre per archiviazione decentrata si intende l'archiviazione a livello degli Stati membri.

([44]) Cfr. la nota 33.

([45]) Comunicazione della Commissione «Preparare le prossime fasi della gestione delle frontiere nell'Unione europea», del 13 febbraio 2008, COM(2008) 69.

([46]) Osservazioni preliminari del GEPD su tre comunicazioni della Commissione sulla gestione delle frontiere [COM(2008) 69, COM(2008) 68 e COM(2008) 67], del 3 marzo 2008. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

([47]) In particolare: parere del 23 marzo 2005 sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata, GU C 181 del 23.7.2005, pag. 13 e parere del 19 ottobre 2005 su tre proposte sul sistema d'Informazione Schengen di seconda generazione (SIS II), GU C 91 del 19.4.2006, pag. 38.

all'esigenza di attuare garanzie forti e mirate nonché alla proporzionalità e alla necessità delle valutazioni d'impatto prima che eventuali misure siano proposte o intraprese in questo settore. Il GEPD ha sempre invocato un equilibrio giusto e rispettoso della protezione dei dati tra i requisiti di sicurezza e la protezione della vita privata delle persone soggette ai sistemi. Egli ha assunto la stessa posizione agendo da garante delle parti centrali dei sistemi.

73. Inoltre, il GEPD coglie questa opportunità per sottolineare l'esigenza di un approccio coerente verso lo scambio di informazioni a livello di UE nel complesso, in termini di coerenza giuridica, tecnica e di controllo tra i sistemi già in atto e quelli ancora in corso di elaborazione. Oggi più di prima sussiste di fatto una chiara esigenza di una visione coraggiosa e complessiva sulla struttura del sistema per lo scambio di informazioni a livello di UE e del futuro sistema di informazione su vasta scala. Solo sulla base di tale visione, un sistema elettronico di registrazione ingressi/uscite dal territorio degli Stati membri potrebbe essere eventualmente riconsiderato.

74. Il GEPD suggerisce di fare riferimento nel programma di Stoccolma all'intenzione di sviluppare tale visione, il che dovrebbe includere una riflessione sull'eventuale entrata in vigore del trattato di Lisbona e le relative implicazioni sui sistemi la cui base giuridica risiede nel primo e terzo pilastro.

75. Infine, la comunicazione accenna all'istituzione di una nuova agenzia che secondo la comunicazione stessa dovrebbe essere competente anche per il sistema elettronico di registrazione ingressi/uscite. Nel frattempo, la Commissione ha adottato una proposta per l'istituzione di tale agenzia ([48]). Il GEPD sostiene in linea di massima questa proposta in quanto può rendere più efficace il funzionamento di tali sistemi, inclusa la protezione dei dati. Presenterà a tempo debito un parere su tale proposta.

Europol ed Eurojust

76. Il ruolo di Europol è citato a più riprese nella comunicazione in cui si sottolinea tra le questioni prioritarie il fatto che Europol è chiamato a svolgere un ruolo centrale in materia di coordinamento, scambio di informazioni e formazione degli operatori. Ugualmente, il punto 4.2.2 della comunicazione rinvia alle recenti modifiche apportate al quadro normativo della cooperazione tra Eurojust ed Europol e annuncia il proseguimento dei lavori sul rafforzamento di Eurojust, in particolare per quanto riguarda il potere di indagine in materia di criminalità organizzata transfrontaliera. Il GEPD sostiene pienamente questi obiettivi, a condizione che le garanzie per la protezione dei dati siano opportunamente rispettate.

77. In questo contesto, il GEPD accoglie favorevolmente il nuovo progetto di accordo recentemente raggiunto tra Europol ed Eurojust ([49]), volto a migliorare e rafforzare la cooperazione reciproca tra i due organi e a prevedere un efficace scambio di informazioni tra gli stessi. Questo è un lavoro in cui un'efficiente ed efficace protezione dei dati svolge un ruolo essenziale.

VI.4. **L'utilizzo dei dati biometrici**

78. Il GEPD rileva che la comunicazione non affronta la questione dell'utilizzo crescente dei dati biometrici nei differenti strumenti giuridici dell'Unione europea relativi all'utilizzo dello scambio di informazioni, compresi gli strumenti che istituiscono i sistemi di informazione su vasta scala. Questo è deplorevole considerato che si tratta di una questione di particolare importanza e sensibilità dal punto di vista della protezione dei dati e della vita privata.

79. Pur riconoscendo i vantaggi generali dell'utilizzo di elementi biometrici, il GEPD ha sottolineato costantemente il grande impatto che l'utilizzo di tali dati ha sui diritti delle persone e ha suggerito di inserire rigorose garanzie per l'utilizzo di elementi biometrici in ogni singolo sistema. La recente sentenza della Corte europea dei diritti dell'uomo in *S. and Marper c. Regno Unito* ([50]) fornisce indicazioni utili in questo contesto, in particolare sulla giustificazione e sui limiti dell'utilizzo dei dati biometrici. In particolare l'utilizzo di informazioni sul DNA può rivelare informazioni sensibili sulle persone, anche perché le possibilità tecniche di estrarre informazioni dal DNA continuano a crescere. Nel caso di utilizzo su vasta scala dei dati biometrici nei sistemi di informazione, sussiste anche un problema dovuto alle inesattezze insite nella raccolta e nel confronto dei dati biometrici. Per questi motivi, il legislatore dell'UE dovrebbe assumere un atteggiamento moderato sull'utilizzo di questi dati.

80. Un'altra questione ricorrente degli ultimi anni è stato l'utilizzo delle impronte digitali dei minori e degli anziani, a causa delle imperfezioni insite nei sistemi biometrici per questi gruppi di età. Il GEPD ha chiesto uno studio approfondito al fine di accertare l'esattezza dei sistemi ([51]). Egli ha proposto un limite di età di 14 anni per i minori, a meno che questo studio non pervenga a risultati diversi. Il GEPD raccomanda di menzionare la questione nel programma di Stoccolma.

([48]) Proposta della Commissione del 24 giugno 2009 di un regolamento del Parlamento europeo e del Consiglio che istituisce un'agenzia per la gestione operativa del sistema d'Informazione Schengen (SIS II), del sistema d'informazione visti (VIS), di EURODAC e di altri sistemi di tecnologia dell'informazione su larga scala del settore della libertà, della sicurezza e della giustizia [COM(2009) 293/2].

([49]) Progetto di accordo, approvato dal Consiglio che deve ancora essere firmato da entrambe le parti. Cfr. il registro del Consiglio: http://register.consilium.europa.eu/pdf/en/09/st10/st10019.en09.pdf http://register.consilium.europa.eu/pdf/en/09/st10/st10107.en09.pdf

([50]) Domande riunite 30562/04 e 30566/04, S. and Marper v. United Kingdom, sentenza del 4 dicembre 2008 della CEDU, non ancora pubblicata.

([51]) Parere del 26 marzo 2008 sulla proposta di regolamento che modifica il regolamento (CE) n. 2252/2004 del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri, GU C 200 del 6.8.2008, pag. 1.

81. Ciò detto, il GEPD suggerisce che sarebbe utile elaborare criteri sostanziali per l'utilizzo dei dati biometrici. Questi criteri dovrebbero garantire che i dati saranno utilizzati solo se necessari, adeguati e proporzionati, e se il legislatore ne avrà dimostrato una finalità esplicita, specifica e legittima. Per essere più precisi, non si dovrebbe ricorrere ai dati biometrici e in particolare ai dati relativi al DNA se lo stesso risultato può essere raggiunto utilizzando altre informazioni meno sensibili.

VII. **ACCESSO ALLA GIUSTIZIA E ALLA GIUSTIZIA ELETTRONICA**

82. La tecnologia sarà inoltre utilizzata quale strumento per una migliore cooperazione giudiziaria. Al punto 3.4.1 della comunicazione, la giustizia elettronica è presentata come strumento che agevola l'accesso alla giustizia per i cittadini. Comprende un portale con informazioni e videoconferenze come parte della procedura legale. Essa consente inoltre di accedere a procedure giuridiche on line e prevede l'interconnessione dei registri nazionali, come i registri di insolvenza. Il GEPD rileva che la comunicazione non cita nuove iniziative sulla giustizia elettronica ma consolida le azioni già in corso. Il GEPD è interessato ad alcune di queste azioni, come follow up del parere pubblicato il 19 dicembre 2008 sulla comunicazione della Commissione «Verso una strategia europea in materia di giustizia elettronica» ([52]).

83. La giustizia elettronica è un progetto ambizioso che ha bisogno di pieno sostegno. Essa può migliorare effettivamente il sistema giudiziario in Europa e la tutela giudiziaria del cittadino. Rappresenta un passo significativo verso uno spazio europeo di giustizia. Tenendo presente questo apprezzamento positivo, possono essere formulate alcune osservazioni:

— i sistemi tecnologici di giustizia elettronica dovrebbero essere costruiti secondo il principio della «privacy by design»; come affermato in precedenza, in relazione al modello europeo di informazioni, il punto di partenza per tutto è scegliere la giusta architettura,

— l'interconnessione e l'interoperabilità dei sistemi dovrebbero rispettare il principio di limitazione delle finalità,

— le responsabilità dei differenti attori dovrebbero essere definite con precisione,

— le conseguenze per le persone dell'interconnessione dei registri nazionali contenenti dati personali delicati, come i registri di insolvenza, dovrebbero essere analizzate in anticipo.

VIII. **CONCLUSIONI**

84. Il GEPD approva nella comunicazione l'enfasi data alla protezione dei diritti fondamentali, e in particolare alla protezione dei dati personali, una delle questioni chiave per il futuro dello spazio di libertà, sicurezza e giustizia. Secondo il GEPD, la comunicazione promuove giustamente un equilibrio tra le esigenze di strumenti adeguati per garantire la sicurezza dei cittadini e la protezione dei loro diritti fondamentali. Essa riconosce che maggior risalto dovrebbe essere dato alla protezione dei dati personali.

85. Il GEPD sostiene pienamente il punto 2.3 della comunicazione in cui si chiede di istituire un regime completo di protezione dei dati che contempli tutti i settori di competenza dell'UE, indipendentemente dall'entrata in vigore del trattato di Lisbona. Egli raccomanda in questo contesto di:

— annunciare nel programma di Stoccolma l'esigenza di una visone chiara e a lungo termine relativa a tale regime completo,

— valutare le misure che sono state adottate in questo settore, nonché la loro attuazione concreta e la loro efficacia, alla luce dei costi per la vita privata e dell'efficacia per l'applicazione della legge,

— includere quale priorità nel programma di Stoccolma, l'esigenza di un nuovo quadro normativo, sostituendo tra l'altro la decisione quadro 2008/977/GAI del Consiglio.

86. Il GEPD accoglie favorevolmente l'intenzione della Commissione di riaffermare i principi in materia di protezione dei dati, che devono essere collegati alla consultazione pubblica annunciata dalla Commissione nella conferenza *Personal data — more use, more protection?* del 19 e 20 maggio 2009. Quanto al merito, il GEPD sottolinea l'importanza del principio di limitazione delle finalità quale pietra miliare della normativa in materia di protezione dei dati nonché del fatto di concentrasi sulle possibilità di migliorare l'efficacia dell'applicazione dei principi in materia di protezione dei dati tramite strumenti che possano rafforzare le competenze dei responsabili del trattamento.

87. Le tecnologie della «privacy by design» e «rispettose della vita privata» potrebbero essere promosse tramite:

— un regime di certificazione per la protezione della vita privata e dei dati quale opzione per ideatori e utenti dei sistemi di informazione,

— l'obbligo giuridico per gli ideatori e gli utenti dei sistemi di informazione di utilizzare sistemi che siano conformi al principio della «privacy by design».

88. Per quanto riguarda gli aspetti esterni della protezione dei dati, il GEPD raccomanda di:

— sottolineare nel programma di Stoccolma l'importanza di accordi generali con gli Stati Uniti e altri paesi terzi in materia di protezione dei dati e di scambio di dati,

([52]) Parere del GEPD del 19 dicembre 2008 sulla comunicazione della Commissione «Verso una strategia europea in materia di giustizia elettronica», GU C 128 del 6.6.2009, pag. 13.

— promuovere attivamente il rispetto dei diritti fondamentali, e in particolare della protezione dei dati, in relazione ai paesi terzi e alle organizzazioni internazionali,

— menzionare nel programma di Stoccolma che lo scambio di dati personali con i paesi terzi richiede un livello adeguato di protezione o altre garanzie appropriate in quei paesi terzi.

89. Il GEPD prende atto con grande interesse degli sviluppi verso una strategia di gestione delle informazioni a livello di Unione europea e verso un modello europeo di informazione e mette in risalto l'attenzione che dovrebbe essere prestata in tali progetti agli elementi di protezione dei dati, che dovranno essere ulteriormente elaborati nel programma di Stoccolma. L'architettura per lo scambio di informazioni dovrebbe essere basata sulla «privacy by design» e sulle «migliori tecniche disponibili».

90. Il semplice fatto che sia tecnicamente possibile scambiare informazioni digitali tra banche dati interoperabili o accorpare queste banche dati non giustifica un'eccezione al principio di limitazione delle finalità. L'interoperabilità dovrebbe nei casi concreti basarsi su scelte politiche chiare e attente. Il GEPD suggerisce di precisare tale nozione nel programma di Stoccolma.

91. L'utilizzo ai fini dell'applicazione della legge di dati raccolti per finalità commerciali dovrebbe, secondo il GEPD, essere unicamente consentito nel rispetto di condizioni rigorose, precisate al punto 65 del presente parere.

92. Altri suggerimenti riguardo all'utilizzo delle informazioni personali includono:

— l'elaborazione di criteri sostanziali per la scelta tra sistema centralizzato e decentrato, e includere l'intenzione di elaborare tali criteri nel programma di Stoccolma,

— l'istituzione di un sistema elettronico di registrazione ingressi/uscite dal territorio degli Stati membri dell'Unione europea oltre ai programmi di viaggiatori registrati non dovrebbero essere citati nel programma di Stoccolma,

— il sostegno per il rafforzamento di Europol ed Eurojust e per il nuovo accordo recentemente elaborato tra Europol ed Eurojust,

— l'elaborazione di criteri sostanziali per l'utilizzo dei dati biometrici, garantendo che i dati siano utilizzati unicamente se necessari, adeguati e proporzionati, e se è stata dimostrata una finalità esplicita, specifica e legittima da parte del legislatore; i dati relativi al DNA non dovrebbero essere utilizzati se può essere raggiunto lo stesso effetto ricorrendo ad altre informazioni meno sensibili.

93. Il GEPD sostiene la giustizia elettronica e ha formulato alcune osservazioni sulle modalità per migliorare il progetto (cfr. punto 83).

Fatto a Bruxelles, addì 10 luglio 2009.

Peter HUSTINX

Garante europeo della protezione dei dati